

Jahresausgabe

**Schönherr  
Datenschutzmonitor  
Jahresausgabe 2025**

Erscheinungsdatum: 30.01.2026

## contacts



**János Böszörményi**  
Rechtsanwalt  
Schönherr Rechtsanwälte GmbH  
+43 664 800 60 3211  
[j.boeszormentyi@schoenherr.eu](mailto:j.boeszormentyi@schoenherr.eu)



**Denise Stahleder**  
Rechtsanwaltsanwärtlerin  
Schönherr Rechtsanwälte GmbH  
+43 664 80060 3912  
[de.stahleder@schoenherr.eu](mailto:de.stahleder@schoenherr.eu)



**Florian Terharen**  
Rechtsanwalt  
Schönherr Rechtsanwälte GmbH  
+43 664 80060 3625  
[fl.terharen@schoenherr.eu](mailto:fl.terharen@schoenherr.eu)



**Daniela Birnbauer**  
Rechtsanwaltsanwältin  
Schönherr Rechtsanwälte GmbH  
+43 1 53437



**Christian Kracher**  
Rechtsanwaltsanwärtler  
Schönherr Rechtsanwälte GmbH  
+43 1 534 37 50053  
[ch.kracher@schoenherr.eu](mailto:ch.kracher@schoenherr.eu)



**Gamze Turan**  
Paralegal  
Schönherr Rechtsanwälte GmbH



**Anna Maria Gidwani**  
Paralegal  
Schönherr Rechtsanwälte GmbH

Für die ausgezeichnete Unterstützung bedanken wir uns bei Philipp John, Christopher Drolz, Nora Perchthaler, Léa Depart, Barbara Gatterbauer, Alexander Fechter, Katharina Falkner, Lisa Duranik, Linda Bräuer, Nelson Hsieh und Sarah Ocsenás.



**Registrieren Sie sich**, um wöchentliche Updates  
in Ihr E-Mail-Postfach zu erhalten!

# Vorwort

Der **Schönherr Datenschutzmonitor** ist ein **wöchentlich erscheinender Newsletter**, der seit seiner Erstausgabe am **10.01.2024** einen **Überblick** über die **datenschutzrechtlichen Entwicklungen** der jeweils **vergangenen Woche** bietet. In der Anfangsphase wurde die **österreichische und europäische Rechtsprechung** zum Datenschutzrecht berücksichtigt. Seitdem ist der Datenschutzmonitor stetig weiterentwickelt worden.

Mittlerweile informieren wir auch über andere Rechtsgebiete, wie Entwicklungen bei der **Regulierung künstlicher Intelligenz**. Der Datenschutzmonitor deckt zudem neben der Rechtsprechung auch für das Datenschutz- und Digitalisierungsrecht relevante **Rechtsakte auf österreichischer und europäischer Ebene** sowie Leitlinien des Europäischen Datenschutzausschusses (**EDSA**) und der Europäischen Kommission (**EK**) ab. Da der Beobachtungsfokus zunehmend auf das Digitalisierungsrecht ausgedehnt wurde, wird der Datenschutzmonitor ab dem **Jahr 2026** in **Schönherr Digitalrechtsmonitor** umbenannt.

Die bedeutendste Erweiterung des Schönherr Datenschutzmonitors im Jahr 2025 war der **Digital Law Monitor**, der dieser Jahresausgabe als Anhang beigelegt ist. Der Digital Law Monitor erscheint quartalsmäßig auf Englisch und deckt neben der EU-Ebene den gesamten **CEE-Raum** ab.

Diese Jahresausgabe wird weiters durch ein **Abkürzungsverzeichnis** und ein **Begriffslexikon** angereichert, die den wöchentlichen Ausgaben des Datenschutzmonitors **vorangestellt** sind. Den wöchentlichen Ausgaben **nachgestellt** haben wir mehrere Übersichten. In der ersten Übersicht fassen wir **ausgewählte Rechtsprechungslinien** zusammen. In den darauf folgenden **Übersichtstabellen** werden einerseits die **Rechtsprechung** der österreichischen und europäischen Höchstgerichte und der DSB sowie ausgewählte Rechtsprechungen anderer Gerichte, insb des BVwG, für die Jahre 2024 und 2025 aufgelistet. Weiters werden die **nationalen und europäischen Rechtsakte** sowie **Leitlinien** des EDSA und der EK aus den Jahren 2024 und 2025 angeführt.

Das Abkürzungsverzeichnis, das Begriffslexikon und die Übersichten können auch über unsere **Webseite** unter "Weiterführende Informationen" (rechts unten) aufgerufen werden.

Wir **bedanken uns herzlich** bei unseren Leser:innen und freuen uns, wenn wir Sie mit unserem Newsletter auch künftig unterstützen dürfen.

*János Böszörményi*

# Inhaltsverzeichnis

|   |            |
|---|------------|
| <b>VORWORT</b> .....                                    | <b>3</b>   |
| <b>INHALTSVERZEICHNIS</b> .....                         | <b>4</b>   |
| <b>ABKÜRZUNGSVERZEICHNIS</b> .....                      | <b>5</b>   |
| <b>BEGRIFFSLEXIKON</b> .....                            | <b>7</b>   |
| <b>DATENSCHUTZMONITOR. 01/2025 VOM 08.01.2025</b> ..... | <b>9</b>   |
| <b>DATENSCHUTZMONITOR. 02/2025 VOM 15.01.2025</b> ..... | <b>12</b>  |
| <b>DATENSCHUTZMONITOR. 03/2025 VOM 22.01.2025</b> ..... | <b>19</b>  |
| <b>DATENSCHUTZMONITOR. 04/2025 VOM 29.01.2025</b> ..... | <b>24</b>  |
| <b>DATENSCHUTZMONITOR. 05/2025 VOM 06.02.2025</b> ..... | <b>29</b>  |
| <b>DATENSCHUTZMONITOR. 06/2025 VOM 12.02.2025</b> ..... | <b>34</b>  |
| <b>DATENSCHUTZMONITOR. 07/2025 VOM 19.02.2025</b> ..... | <b>42</b>  |
| <b>DATENSCHUTZMONITOR. 08/2025 VOM 26.02.2025</b> ..... | <b>47</b>  |
| <b>DATENSCHUTZMONITOR. 09/2025 VOM 05.03.2025</b> ..... | <b>54</b>  |
| <b>DATENSCHUTZMONITOR. 10/2025 VOM 12.03.2025</b> ..... | <b>59</b>  |
| <b>DATENSCHUTZMONITOR. 11/2025 VOM 19.03.2025</b> ..... | <b>63</b>  |
| <b>DATENSCHUTZMONITOR. 12/2025 VOM 26.03.2025</b> ..... | <b>68</b>  |
| <b>DATENSCHUTZMONITOR. 13/2025 VOM 03.04.2025</b> ..... | <b>74</b>  |
| <b>DATENSCHUTZMONITOR. 14/2025 VOM 09.04.2025</b> ..... | <b>81</b>  |
| <b>DATENSCHUTZMONITOR. 15/2025 VOM 16.04.2025</b> ..... | <b>88</b>  |
| <b>DATENSCHUTZMONITOR. 16/2025 VOM 24.04.2025</b> ..... | <b>93</b>  |
| <b>DATENSCHUTZMONITOR. 17/2025 VOM 30.04.2025</b> ..... | <b>99</b>  |
| <b>DATENSCHUTZMONITOR. 18/2025 VOM 07.05.2025</b> ..... | <b>106</b> |
| <b>DATENSCHUTZMONITOR. 19/2025 VOM 14.05.2025</b> ..... | <b>110</b> |
| <b>DATENSCHUTZMONITOR. 20/2025 VOM 21.05.2025</b> ..... | <b>114</b> |
| <b>DATENSCHUTZMONITOR. 21/2025 VOM 28.05.2025</b> ..... | <b>121</b> |
| <b>DATENSCHUTZMONITOR. 22/2025 VOM 04.06.2025</b> ..... | <b>126</b> |
| <b>DATENSCHUTZMONITOR. 23/2025 VOM 11.06.2025</b> ..... | <b>134</b> |
| <b>DATENSCHUTZMONITOR. 24/2025 VOM 18.06.2025</b> ..... | <b>141</b> |
| <b>DATENSCHUTZMONITOR. 25/2025 VOM 25.06.2025</b> ..... | <b>147</b> |
| <b>DATENSCHUTZMONITOR. 26/2025 VOM 02.07.2025</b> ..... | <b>151</b> |
| <b>DATENSCHUTZMONITOR. 27/2025 VOM 09.07.2025</b> ..... | <b>157</b> |
| <b>DATENSCHUTZMONITOR. 28/2025 VOM 16.07.2025</b> ..... | <b>165</b> |
| <b>DATENSCHUTZMONITOR. 29/2025 VOM 23.07.2025</b> ..... | <b>172</b> |
| <b>DATENSCHUTZMONITOR. 30/2025 VOM 30.07.2025</b> ..... | <b>178</b> |
| <b>DATENSCHUTZMONITOR. 31/2025 VOM 06.08.2025</b> ..... | <b>183</b> |
| <b>DATENSCHUTZMONITOR. 32/2025 VOM 13.08.2025</b> ..... | <b>188</b> |
| <b>DATENSCHUTZMONITOR. 33/2025 VOM 20.08.2025</b> ..... | <b>193</b> |
| <b>DATENSCHUTZMONITOR. 34/2025 VOM 27.08.2025</b> ..... | <b>200</b> |
| <b>DATENSCHUTZMONITOR. 35/2025 VOM 03.09.2025</b> ..... | <b>206</b> |
| <b>DATENSCHUTZMONITOR. 36/2025 VOM 10.09.2025</b> ..... | <b>213</b> |
| <b>DATENSCHUTZMONITOR. 37/2025 VOM 17.09.2025</b> ..... | <b>220</b> |
| <b>DATENSCHUTZMONITOR. 38/2025 VOM 24.09.2025</b> ..... | <b>227</b> |
| <b>DATENSCHUTZMONITOR. 39/2025 VOM 01.10.2025</b> ..... | <b>233</b> |
| <b>DATENSCHUTZMONITOR. 40/2025 VOM 08.10.2025</b> ..... | <b>238</b> |
| <b>DATENSCHUTZMONITOR. 41/2025 VOM 15.10.2025</b> ..... | <b>243</b> |
| <b>DATENSCHUTZMONITOR. 42/2025 VOM 23.10.2025</b> ..... | <b>249</b> |
| <b>DATENSCHUTZMONITOR. 43/2025 VOM 29.10.2025</b> ..... | <b>256</b> |
| <b>DATENSCHUTZMONITOR. 44/2025 VOM 05.11.2025</b> ..... | <b>261</b> |
| <b>DATENSCHUTZMONITOR. 45/2025 VOM 12.11.2025</b> ..... | <b>267</b> |
| <b>DATENSCHUTZMONITOR. 46/2025 VOM 19.11.2025</b> ..... | <b>271</b> |
| <b>DATENSCHUTZMONITOR. 47/2025 VOM 26.11.2025</b> ..... | <b>278</b> |
| <b>DATENSCHUTZMONITOR. 48/2025 VOM 03.12.2025</b> ..... | <b>285</b> |
| <b>DATENSCHUTZMONITOR. 49/2025 VOM 11.12.2025</b> ..... | <b>292</b> |
| <b>DATENSCHUTZMONITOR. 50/2025 VOM 17.12.2025</b> ..... | <b>300</b> |
| <b>DATENSCHUTZMONITOR. 51/2025 VOM 29.12.2025</b> ..... | <b>306</b> |
| <b>DATENSCHUTZMONITOR. 52/2025 VOM 02.01.2026</b> ..... | <b>313</b> |
| <b>RECHTSPRECHUNGSLINIEN</b> .....                      | <b>319</b> |
| <b>RECHTSPRECHUNGSÜBERSICHT 2024</b> .....              | <b>323</b> |
| <b>RECHTSAKTE UND LEITLINIEN 2024</b> .....             | <b>340</b> |
| <b>RECHTSPRECHUNGSÜBERSICHT 2025</b> .....              | <b>345</b> |
| <b>RECHTSAKTE UND LEITLINIEN 2025</b> .....             | <b>378</b> |
| <b>DIGITAL LAW MONITOR – CONTACTS</b> .....             | <b>393</b> |
| <b>DIGITAL LAW MONITOR. 1/2025</b> .....                | <b>394</b> |
| <b>DIGITAL LAW MONITOR. 2/2025</b> .....                | <b>401</b> |
| <b>DIGITAL LAW MONITOR. 3/2025</b> .....                | <b>414</b> |
| <b>DIGITAL LAW MONITOR. 4/2025</b> .....                | <b>430</b> |

# Abkürzungsverzeichnis

| <b>Abkürzung</b> | <b>Begriff</b>  |
|------------------|---|
| <b>AEUV</b>      | Vertrag über die Arbeitsweise der Europäischen Union  |
| <b>AußStrG</b>   | Außerstreitgesetz   |
| <b>AVG</b>       | Allgemeines Verwaltungsverfahrensgesetz   |
| <b>BAO</b>       | Bundesabgabenordnung  |
| <b>BDB</b>       | Bundesdisziplinarbehörde  |
| <b>BFG</b>       | Bundesfinanzgericht   |
| <b>BVwG</b>      | Bundesverwaltungsgericht  |
| <b>COFAG</b>     | COVID-19-Finanzierungsagentur des Bundes  |
| <b>DSB</b>       | Datenschutzbehörde  |
| <b>DSG</b>       | Datenschutzgesetz   |
| <b>DSGVO</b>     | Datenschutz-Grundverordnung (VO (EU) 2016/679)  |
| <b>DSRL-PJ</b>   | Datenschutzrichtlinie für Polizei und Justiz (RL (EU) 2016/680)                                   |
| <b>EAA</b>       | Europäische Ermittlungsanordnung  |
| <b>EDSA</b>      | Europäischer Datenschutzausschuss   |
| <b>EGMR</b>      | Europäischer Gerichtshof für Menschenrechte   |
| <b>EK</b>        | Europäische Kommission  |
| <b>EKEK</b>      | Europäischer Kodex für die elektronische Kommunikation  |
| <b>EMRK</b>      | Europäische Menschenrechtskonvention  |
| <b>ErwGr</b>     | Erwägungsgrund (einem Rechtsakt der Europäischen Union, zB RL oder VO, vorangestellte Erwägungen) |

|                |  |
|----------------|--|
| <b>EuG</b>     | Gericht der Europäischen Union   |
| <b>EuGH</b>    | Europäischer Gerichtshof   |
| <b>EUV</b>     | Vertrag über die Europäische Union                                       |
| <b>FinStrG</b> | Finanzstrafgesetz  |
| <b>GEREK</b>   | Gremium Europäischer Regulierungsstellen für elektronische Kommunikation |
| <b>IFG</b>     | Informationsfreiheitsgesetz  |
| <b>LVwG</b>    | Landesverwaltungsgericht/e   |
| <b>OGH</b>     | Oberster Gerichtshof   |
| <b>OLG</b>     | Oberlandesgericht/e  |
| <b>PoI-W-G</b> | Politische-Werbung-Gesetz  |
| <b>RKEG</b>    | Resilienz kritischer Einrichtungen-Gesetz                                |
| <b>RL</b>      | Richtlinie der Europäischen Union  |
| <b>SA</b>      | Schlussanträge der Generalanwälte (EuGH)                                 |
| <b>StPO</b>    | Strafprozeßordnung   |
| <b>V</b>       | Verordnung nach österreichischem Recht                                   |
| <b>VfGH</b>    | Verfassungsgerichtshof   |
| <b>VO</b>      | Verordnung der Europäischen Union  |
| <b>VStG</b>    | Verwaltungsstrafgesetz   |
| <b>VwGH</b>    | Verwaltungsgerichtshof   |
| <b>ZPO</b>     | Zivilprozessordnung  |

# Begriffslexikon

| Begriff                          | Erklärung   |
|----------------------------------|---|
| <b>Amtswegiges Prüfverfahren</b> | Ein von der DSB von Amts ( <i>ex officio</i> ) wegen eingeleitetes Verfahren, das nach dem AVG durchgeführt wird.   |
| <b>Ausgangsbescheid</b>          | Erstbescheid in einem Verfahren, in dem auch eine Beschwerdeentscheidung als Zweitbescheid erlassen wird.   |
| <b>Auskunftsersuchen</b>         | Den Begriff Auskunftsersuchen verwenden wir stets für das Ersuchen um Auskunft iSd Art 15 DSGVO oder § 1 Abs 3 Z 1 DSG im Verhältnis zwischen Betroffenen und Verantwortlichen.   |
| <b>Auskunftsverfahren</b>        | Das Verfahren, in dem eine Verletzung im Recht auf Auskunft gemäß Art 15 DSGVO geltend gemacht wird.  |
| <b>Aussetzungsbescheid</b>       | Bescheid, mit dem die DSB ein bei ihr anhängiges Verfahren aussetzt.  |
| <b>Aussetzungsbeschluss</b>      | Entscheidung, mit der das BVwG, die ordentlichen Gerichte sowie die Höchstgerichte ein anhängiges Verfahren aussetzen.  |
| <b>Berichtigungsersuchen</b>     | Den Begriff Berichtigungsersuchen verwenden wir stets für das Ersuchen um Berichtigung iSd Art 16 DSGVO oder § 1 Abs 3 Z 2 DSG im Verhältnis zwischen Betroffenen und Verantwortlichen.   |
| <b>Berufungsgericht</b>          | Die Berufungsgerichte sind regelmäßig die OLG, weil datenschutzrechtliche Angelegenheiten auf dem Zivilrechtsweg in die Zuständigkeit der Landesgerichte fallen. Entscheidet in erster Instanz ein Bezirksgericht, wird das Landesgericht zum Berufungsgericht. |
| <b>Betroffene/r</b>              | Die/der Betroffene ist die betroffene Person.   |
| <b>Beschreibbeschwerde</b>       | Die Beschwerde, die gegen den Bescheid einer Verwaltungsbehörde (1. Instanz) an ein Verwaltungsgericht (2. Instanz) erhoben wird. In datenschutzrechtlichen Angelegenheiten richtet   |

|                                      |  |
|--------------------------------------|--|
|                                      | sich die Bescheidbeschwerde gegen den Bescheid der DSB an das BVwG.  |
| <b>Datenschutzbeschwerde</b>         | Die DSB kann Verfahren von Amts wegen oder auf Antrag einer Partei einleiten. Als Datenschutzbeschwerde bezeichnen wir jenen Antrag, mit dem ein Verfahren bei der DSB auf Partei-antrag eingeleitet wird. |
| <b>Erkenntnisbeschwerde</b>          | Beschwerde an den VfGH gegen das Erkenntnis eines Verwaltungsgerichts.   |
| <b>Erstgericht</b>                   | Bezirks- oder Landesgericht. In datenschutzrechtlichen Angelegenheiten ist das Erstgericht idR ein Landesgericht.  |
| <b>Geheimhaltungsverfahren</b>       | Das Verfahren, in dem eine Verletzung im Recht auf Geheimhaltung gemäß § 1 DSG geltend gemacht wird.   |
| <b>Lösch- oder Löschungsersuchen</b> | Den Begriff Löschungsersuchen verwenden wir stets für das Ersuchen um Löschung iSd Art 17 DSGVO oder § 1 Abs 3 Z 2 DSG im Verhältnis zwischen Betroffenen und Verantwortlichen.                            |
| <b>Löschungsverfahren</b>            | Das Verfahren, in dem eine Verletzung im Recht auf Löschung gemäß Art 17 DSGVO geltend gemacht wird.   |





to the point

# Datenschutzmonitor. 01/2025 vom 08.01.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Wir wünschen ein frohes neues Jahr und freuen uns, Sie auch im Jahr 2025 beim Datenschutzmonitor begrüßen zu dürfen.

Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des VfGH**

VfGH 09.03.2023, E2097/2021 (Finanzdatenaustausch, Besteuerung, GMSG)

- **Rechtsprechung des BVwG**

BVwG 22.11.2024, W211 2272744-1; 18.11.2024, W137 2272120-1 (Betroffenheit, Mitwirkungspflicht)

- **EU-Rechtsakte**

VO (EU) 2024/3228 über die Einstellung der Europäischen Plattform für Online-Streitbeilegung

RL (EU) 2024/3237 zum Informationsaustausch über die Straßenverkehrssicherheit

## To the Point:

### Rechtsprechung des VfGH

VfGH 09.03.2023, E2097/2021

#### **Finanzdatenaustausch, Besteuerung, GMSG**

- Ein Österreicher mit einem deutschen Bankkonto erachtete sich in seinem Grundrecht auf Datenschutz verletzt, weil der **Bundesminister für Finanzen (BMF)** personenbezogene Daten vom deutschen Bundeszentralamt für Steuern erhielt, verarbeitete und an die zuständige Abgabenbehörde weiterleitete. Die Datenverarbeitung beruhte auf § 113 **Gemeinsamer Meldestandard-Gesetz (GMSG)** und der Richtlinie 2011/16/EU über die Zusammenarbeit der Verwaltungsbehörden im Bereich der Besteuerung. Die DSB wies die Datenschutzbeschwerde ab. Das BVwG wies die Bescheidbeschwerde ab. Der VfGH wies die **Erkenntnisbeschwerde** ab und trat sie an den VfGH zur Entscheidung darüber ab, ob der Österreicher durch das angefochtene Erkenntnis in einem sonstigen Recht verletzt wurde.

Der VfGH hat erwogen: §§ 112 und 113 GMSG setzen den **automatischen Austausch von Finanzdaten** gemäß Art 8 Abs 3a der Richtlinie über die Zusammenarbeit der Verwaltungsbehörden im Bereich der Besteuerung deckungsgleich um. Der VfGH kann die Verfassungsmäßigkeit der §§ 112 und 113 GMSG daher nur dann prüfen, wenn der EuGH zuvor Art 8 Abs 3a der Richtlinie für ungültig erklärt. Der VfGH hat jedoch auch keine Bedenken ob der Vereinbarkeit des Art 8 Abs 3a der Richtlinie mit Art 7 und 8 GRC.

**Einschränkungen** der Rechte auf Achtung des Privat- und Familienlebens, der Wohnung sowie Kommunikation und des Rechts auf Schutz personenbezogener Daten sind gemäß **Art 52 GRC** zulässig, wenn sie gesetzlich vorgesehen sind und den Wesensgehalt dieser Rechte wahren. Die Einschränkungen müssen verhältnismäßig und notwendig sein und im Einklang mit dem Gemeinwohl dienenden Zielsetzungen oder dem Schutz der Rechte und Freiheiten Dritter stehen.

Bei Eingriffen in das Datenschutzrecht muss das **öffentliche Interesse** an der Datenerhebung gegen den Schutz des Privatlebens abgewogen werden. Besonders schützenswert sind Daten, die für die spätere automatische Datenverarbeitung gesammelt werden. Es ist sicherzustellen, dass nur **relevante Daten** erhoben werden und diese nicht länger aufbewahrt werden, als dies für die Erreichung der Ziele erforderlich ist. Auch **Schutzmaßnahmen gegen Datenmissbrauch** sind zu treffen. Der BMF und alle am Informationsaustausch beteiligten Behörden sind an die Vorgaben der DSGVO gebunden,

um den erforderlichen Sicherheitsanforderungen für die Verarbeitung zu entsprechen.

Die Weitergabe von **Finanzdaten** gemäß der Richtlinie über die Zusammenarbeit der Verwaltungsbehörden im Bereich der Besteuerung und somit gemäß §§ 112 f GMSG soll **Steuerbetrug und -hinterziehung** verhindern, die Wirksamkeit und Effizienz der Steuererhebung fördern und aggressive Steuerplanung eindämmen. Diese Ziele liegen alle im öffentlichen Interesse. Der **automatische Informationsaustausch** geht nicht über das Maß hinaus, das notwendig und erforderlich ist, um diese Ziele zu erreichen.

Die Rechtsprechung des EuGH zur **Verhältnismäßigkeit** der **Vorratsdatenspeicherung** sind auf die Regelungen der Richtlinie über die Zusammenarbeit der Verwaltungsbehörden im Bereich der **Besteuerung** nicht übertragbar, weil sich die Regelungen in ihren Zielsetzungen unterscheiden und die verarbeiteten Finanzdaten nicht den **Kernbereich des Privatlebens** betreffen. Auch anderen EuGH-Urteilen kann nicht entnommen werden, dass Art 8 Abs 3a der Richtlinie über die Zusammenarbeit der Verwaltungsbehörden im Bereich der Besteuerung gegen Art 8 GRC verstoßen würde.

### Rechtsprechung des BVwG

Aus der Rechtsprechung des BVwG:

- Eine Verletzung des Rechts auf Geheimhaltung kann nur dann vorliegen, wenn **tatsächlich Daten des Betroffenen verarbeitet wurden**. Den Betroffenen trifft eine **Mitwirkungspflicht**, den **Nachweis** der Verarbeitung zu erbringen. Es besteht eine erhöhte Mitwirkungspflicht, wenn es um Umstände geht, die in der persönlichen Sphäre der Parteien liegen ([BVwG 22.11.2024, W211 2272744-1](#); [18.11.2024, W137 2272120-1](#)).

### EU-Rechtsakte

- Am **30.12.2024** ist die "*VO (EU) 2024/3228 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 zur Aufhebung der Verordnung (EU) Nr. 524/2013 und zur Änderung der Verordnungen (EU) 2017/2394 und (EU) 2018/1724 im Hinblick auf die Einstellung der Europäischen Plattform für Online-Streitbeilegung*", [ABI L 2024/3228, 1](#), kundgemacht worden. Mit dieser Verordnung wird die **Europäische Plattform für Online-Streitbeilegung eingestellt**.
- Am **30.12.2024** ist die "*RL (EU) 2024/3237 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 zur Änderung der Richtlinie (EU) 2015/413 zur Erleichterung des grenzüberschreitenden Austauschs von Informationen über die*

*Straßenverkehrssicherheit gefährdende Verkehrsdelikte*", [ABI L 2024/3237, 1](#), kundgemacht worden. Geregelt werden ua der **Austausch von Fahrzeugzulassungsdaten** und die **Amts- und Rechtshilfe** betreffend **Verkehrsdelikte**.

to the point

# Datenschutzmonitor. 02/2025 vom 15.01.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH 09.01.2025, C-394/23, *Mousse* (Anrede, Vertragserfüllung, berechtigtes Interesse)

EuGH 09.01.2025, C-416/23, *Österreichische Datenschutzbehörde* (Exzess, Wahlrecht der Aufsichtsbehörde)

- **Rechtsprechung des EuG**

EuG 08.01.2025, T-354/22, *Bindl/Kommission* (IP-Adresse, Datentransfer, Schadenersatz)

- **Rechtsprechung des VwGH**

VwGH 26.11.2024, Ra 2024/04/0408 (Zurückweisung, Abweichung von bisheriger Rechtsprechung)

- **Rechtsprechung des BVwG**

BVwG 25.11.2024, W252 2282050-1 (Dark Patterns, Cookie-Banner, Widerruf)

BVwG 18.11.2024, W274 2284469-1 (Entschiedene Sache, Exekutionsverfahren)

BVwG 18.11.2024, W137 2297057-1 (Auskunftsrecht, Rechte von Dritten, Öffnungsklausel)

BVwG 25.11.2024, W214 2273462-1 (Bürgermeister, staatliche Behörde)

BVwG 04.12.2024, W603 2303734-1; 03.12.2024, I406 2300562-1 (Zuständigkeit, ORF-Beitrag)

- **Rechtsprechung der DSB**

DSB 27.06.2024, 2024-0.028.256 (Anzeige, Akteneinsicht, Interessenabwägung)

- **EU-Rechtsakte**

VO (EU) 2025/12 über die Übermittlung von Fluggastdaten für den Außengrenzschutz

VO (EU) 2025/13 über die Übermittlung von Fluggastdaten zur Bekämpfung von schwerer Kriminalität und Terrorismus

RL (EU) 2025/25 über digitale Werkzeuge im Gesellschaftsrecht

Berichtigung der VO (EU) 2022/1925 (Gesetz über digitale Märkte; DMA)

UN-Regelung Nr. 155 für die Genehmigung von Fahrzeugen hinsichtlich Cybersicherheit

## To the Point:

### Rechtsprechung des EuGH

EuGH 09.01.2025, C-394/23, Mousse

#### **Anrede, Vertragserfüllung, berechtigtes Interesse**

- Ein Transportunternehmen verlangte bei der Online-Buchung von Fahrscheinen die Angabe der Anrede "Herr" oder "Frau". Der Verband "Mousse" erhob Klage, weil diese Datenverarbeitung weder auf einer Rechtsgrundlage gemäß Art 6 Abs 1 DSGVO beruhe noch dem Grundsatz der Datenminimierung entspreche. Zudem seien Transparenz- und Informationspflichten gemäß Art 13 DSGVO verletzt. Die Vorlagefrage des vorlegenden Gerichts betraf die in Art 6 Abs 1 lit b (Vertragserfüllung) und lit f (berechtigtes Interesse) DSGVO genannten Rechtfertigungsgründe.

Der EuGH hat erwogen: Eine **geschlechtsspezifische Personalisierung** der geschäftlichen Kommunikation ist weder objektiv unerlässlich noch wesentlich, um die ordnungsgemäße **Erfüllung des Vertrags** zu ermöglichen. Die Datenverarbeitung kann daher nicht auf Art 6 Abs 1 lit b DSGVO gestützt werden. Weniger einschneidend wären allgemeine und **inklusive Höflichkeitsformen**, die von der Geschlechtsidentität unabhängig sind.

Die Verarbeitung personenbezogener Daten ist gemäß Art 6 Abs 1 lit f DSGVO rechtmäßig, wenn (i) ein **berechtigtes Interesse** des Verantwortlichen oder eines Dritten wahrgenommen wird; (ii) die Datenverarbeitung zur Verwirklichung des berechtigten Interesses erforderlich ist und (iii) die Interessen oder Grundrechte und Grundfreiheiten der Betroffenen gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen.

**Kommerzielle Direktwerbung** und deren Personalisierung können ein berechtigtes Interesse sein. Gemäß Art 13 Abs 1 DSGVO ist den Betroffenen **zum Zeitpunkt der Datenerhebung** das verfolgte berechtigte Interesse aber **mitzuteilen**. Andernfalls kann die Erhebung nicht auf Art 6 Abs 1 lit f DSGVO gestützt werden.

Die Abfrage einer Anrede und/oder Geschlechtsidentität erscheint im Licht des **Grundsatzes der Datenminimierung** nicht erforderlich. Für die Personalisierung reichen Name und Vorname der Kunden aus. Art 6 Abs 1 lit f DSGVO sieht bei der Beurteilung der **Erforderlichkeit** einer Datenverarbeitung keine Berücksichtigung der **Gepflogenheiten** und **gesellschaftlichen Konventionen** vor.

Im Fall der Gefahr einer Beeinträchtigung der Grundrechte und Grundfreiheiten der Betroffenen kann das berechtigte Interesse an

kommerzieller Direktwerbung nicht überwiegen. Das vorlegende Gericht hat insbesondere zu prüfen, ob die Gefahr einer **Diskriminierung** aufgrund der Geschlechtsidentität besteht. Dies vor allem im Licht der RL (EU) 2004/113, mit der der Grundsatz der Gleichbehandlung von Männern und Frauen beim Zugang zu und bei der Versorgung mit Gütern und Dienstleistungen verwirklicht wird. Diese Richtlinie gilt auch für Diskriminierungen, die ihre Ursache in der Änderung der Geschlechtsidentität einer Person haben.

EuGH 09.01.2025, C-416/23, Österreichische Datenschutzbehörde

#### **Exzess, Wahlrecht der Aufsichtsbehörde**

- Innerhalb von etwa 20 Monaten brachte eine Betroffene 77 ähnliche Datenschutzbeschwerden bei der DSB ein. Die DSB lehnte die Behandlung einer der Datenschutzbeschwerden ab, weil sie exzessiv sei. Das BVwG behob den Bescheid der DSB, woraufhin diese Amtsrevision an den VwGH erhob. Der VwGH ersuchte den EuGH um Vorabentscheidung, ob (i) der Begriff der "Anfrage" iSd Art 57 Abs 4 DSGVO auch Beschwerden nach Art 77 Abs 1 DSGVO erfasse, (ii) ob ein Exzess allein an der Anzahl von Beschwerden, die eine Person an eine Aufsichtsbehörde stellt, festzumachen sei, und (iii) ob eine Aufsichtsbehörde frei wählen könne, eine angemessene Gebühr zu verlangen oder die Behandlung der Beschwerde zu verweigern.

Der EuGH hat erwogen: Für die Verfolgung des Ziels, ein gleichmäßiges und hohes Schutzniveau für natürliche Personen in der Union sicherzustellen, ist das **ordnungsgemäße Funktionieren der Aufsichtsbehörden** unentbehrlich. Art 57 Abs 4 DSGVO soll der Verfolgung dieses Ziels dienen, indem verhindert wird, dass Aufsichtsbehörden durch offenkundig unbegründete oder exzessive Beschwerden behindert werden.

Eine Auslegung dahingehend, dass der Begriff "**Anfrage**" nur Anfragen nach Art 57 Abs 1 lit e DSGVO und nicht auch Beschwerden nach Art 77 Abs 1 DSGVO umfasse, würde Art 57 Abs 4 DSGVO eines großen Teils seiner praktischen Wirksamkeit berauben und – im Ergebnis – den wirksamen Schutz der durch diese Verordnung garantierten Rechte untergraben. Der in Art 57 Abs 4 DSGVO enthaltene Begriff der "Anfrage" umfasst daher auch **Beschwerden an Aufsichtsbehörden**.

Die – alleinige – Häufung von Beschwerden von einer Person kann ein Indiz **für exzessive Anfragen** sein, wenn sich herausstellt, dass die Beschwerden nicht objektiv durch Erwägungen gerechtfertigt sind, die sich auf den Schutz der Rechte beziehen, die die DSGVO dieser Person verleiht. Dies kann

etwa dann der Fall sein, wenn eine Person eine große Zahl von Beschwerden bei einer Aufsichtsbehörde einreicht, die eine Vielzahl von Verantwortlichen betreffen, zu denen sie nicht unbedingt einen Bezug hat und diese übermäßige Inanspruchnahme des Beschwerderechts in Verbindung mit anderen Gesichtspunkten, wie dem Inhalt der Beschwerden, die Absicht der Person erkennen lässt, die Behörde lahmzulegen, indem sie sie mit Anfragen **überflutet**. Eine isolierte Betrachtung der Zahl der Beschwerden könnte zu einer **willkürlichen Beeinträchtigung** der Rechte der betroffenen Person aus der DSGVO führen. Die Feststellung, dass exzessive Anfragen iSd Art 57 Abs 4 DSGVO vorliegen, setzt aus diesen Überlegungen den **Nachweis einer Missbrauchsabsicht** der Person voraus, die solche Beschwerden einreicht.

Die beiden in Art 57 Abs 4 DSGVO für den Fall exzessiver Anfragen vorgesehenen Optionen, nämlich (i) eine angemessene Gebühr auf der Grundlage der Verwaltungskosten zu verlangen, oder (ii) sich zu weigern, aufgrund solcher Anfragen tätig zu werden, sind nebeneinander aufgeführt und durch die nebenordnende Konjunktion "**oder**" getrennt. Dieser Wortinterpretation Rechnung tragend darf die Aufsichtsbehörde bei exzessiven Anfragen durch eine mit Gründen versehene Entscheidung darüber **wählen**, ob sie eine **angemessene Gebühr** auf der Grundlage der Verwaltungskosten verlangt oder **sich weigert**, aufgrund der Anfrage tätig zu werden. Die Aufsichtsbehörde hat dabei jedoch alle relevanten Umstände zu berücksichtigen und muss sich vergewissern, dass die gewählte Option geeignet, erforderlich und verhältnismäßig ist.

### Rechtsprechung des EuG

EuG 08.01.2025, T-354/22, Bindl/Kommission

#### **IP-Adresse, Datentransfer, Schadenersatz**

- Ein Bürger besuchte eine Website der EU, für die die Europäische Kommission ("**Kommission**") datenschutzrechtliche Verantwortliche war. Er meldete sich für eine Veranstaltung über "**EU Login**" mittels "**Sign in with Facebook**" an. Der Bürger ersuchte die Kommission nach der Anmeldung zwei Mal um Datenauskunft bzgl der dadurch verarbeiteten Daten. Ihm wurde auf seine erste Anfrage mitgeteilt, dass seine Daten nicht an Drittländer übermittelt und nur innerhalb Europas gespeichert und verarbeitet werden. Auf seine (präzisierte) zweite Anfrage, die konkrete Fragen zur Datenübermittlung an Meta in den USA aufgrund der Anmeldung enthielt, reagierte die Kommission nicht innerhalb der vorgesehenen Frist, weshalb der Bürger eine Klage an das EuG erhob. Das EuG gab der Klage teilweise statt und sprach dem Bürger auch Schadenersatz zu.

Das EuG hat erwogen: Die beantragte Nichtigerklärung der Übermittlungen der personenbezogenen Daten an Drittländer ohne angemessenes Schutzniveau ist abzuweisen, weil sich ein solcher Antrag nur auf Rechtsakte beziehen kann. Die **Datenübermittlung** ist dagegen ein **Realakt**, der einer Nichtigerklärung nicht zugänglich ist.

Die Datenübermittlung an die USA bei der Anmeldung für die Veranstaltung ist der Kommission zuzurechnen. Diese hat als Verantwortliche der Website mit dem Hyperlink "Sign in with Facebook" die **Voraussetzungen für die Übermittlung** der IP-Adresse des Bürgers an Facebook (= Meta) geschaffen. Da – zum Zeitpunkt der Datenübermittlung – **kein Angemessenheitsbeschluss** vorlag und die Kommission auch keine **geeigneten Garantien (Standarddatenschutz- oder Vertragsklauseln)** nachweisen konnte, galten nur die Nutzungsbedingungen von Facebook. Die Kommission hat somit gegen die Voraussetzungen für die Übermittlung personenbezogener Daten an ein Drittland durch ein Organ der Union verstoßen.

Durch die Datenübermittlung wurde der Bürger in eine Lage gebracht, in der er nicht sicher ist, wie die ihn betreffenden personenbezogenen Daten, insbesondere seine **IP-Adresse**, verarbeitet werden. Daher hat er einen **immateriellen Schaden** erlitten. Für die unrechtmäßige Datenübermittlung ist eine Entschädigung iHv **EUR 400** angemessen. **Anm: Gegen diese Entscheidung könnte ein Rechtsmittel an den EuGH erhoben werden.**

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Das BVwG hat mit Erkenntnis vom 27.06.2024, W176 2248629-1, ausgesprochen, dass die Übermittlung eines MRT-Befundes zur Behandlung im Gesundheitsbereich auf der Grundlage des MTD-Gesetzes zulässig ist. Die gegen dieses Erkenntnis gerichtete außerordentliche Revision wurde vom VwGH aus formalen Gründen zurückgewiesen. Ein Revisionswerber, der eine **Abweichung** des angefochtenen Erkenntnisses von der **Rechtsprechung des Verwaltungsgerichtshofs** behauptet, hat konkret darzulegen, dass der der gegenständlich angefochtenen Entscheidung zugrundeliegende Sachverhalt einer der von ihm ins Treffen geführten Entscheidung gleicht, das Verwaltungsgericht im revisionsgegenständlichen Fall jedoch anders entschieden hat und es damit von der ständigen Rechtsprechung des Verwaltungsgerichtshofs abgewichen ist. Eine **bloße Wiedergabe von Rechtssätzen**, die **bloße Zitierung aus Literaturfundstellen** oder **Geschäftszahlen** ohne Eingehen auf die behaupteten inhaltlichen

Abweichungen reicht zur Darlegung des Abweichens von der Rechtsprechung des Verwaltungsgerichtshofs nicht aus ([VwGH 26.11.2024, Ra 2024/04/0408](#)). **Anm: Die Zusammenfassung des Erkenntnisses des BVwG vom 27.06.2024, W176 2248629-1, können Sie im Schönherr Datenschutzmonitor vom 28.08.2024 nachlesen.**

### **Rechtsprechung des BVwG**

BVwG 25.11.2024, W252 2282050-1

#### **Dark Patterns, Cookie-Banner, Widerruf**

- Ein Websitenutzer brachte wegen behaupteter Mangelhaftigkeit eines Cookie-Banners einer von ihm besuchten Website Datenschutzbeschwerde bei der DSB ein. Im Cookie-Banner war die Option zur Einwilligung farblich kontrastreich und groß gestaltet, die Möglichkeit zur Ablehnung war mit geringem Kontrast und kleinerer Schrift gestaltet. Durch die Gestaltung wurde der Websitenutzer zu einer Einwilligung und damit zu einer Handlung gegen sein Interesse verleitet (**Dark Patterns**). In der Datenschutzbeschwerde machte der Websitenutzer die Verletzung in den Rechten auf Geheimhaltung und Löschung seiner Daten geltend. Die DSB wies die Datenschutzbeschwerde hinsichtlich des Rechts auf Geheimhaltung ab, gab ihr betreffend die Verletzung im Recht auf Löschung aber statt und trug dem Websitebetreiber eine Änderung des Cookie-Banners auf. Die Websitebetreiberin erhob Bescheidbeschwerde an das BVwG, insbesondere weil die DSGVO keine Gleichwertigkeit von Einwilligungs- und Ablehnungsoptionen vorschreibe. Das BVwG wies die Bescheidbeschwerde ab.

Das BVwG hat erwogen: Durch die **Verknüpfung** von **Zeichenfolgen** mit zusätzlichen Daten, zB der IP-Adresse oder einer anderen Kennung, kann die **Identifizierung** eines **Websitenutzers ermöglicht werden**. Es handelt sich dann um ein **personenbezogenes Datum** im Sinne von Art 4 Z 1 DSGVO. Eine **Unique-ID** ist auch dann ein **personenbezogenes Datum**, wenn der Websitebetreiber **nicht selbst** die Möglichkeit hat, diese mit einer gespeicherten oder unmittelbar von Dritten erhaltenen **IP-Adresse** zu **kombinieren**. Die Weiterverarbeitung von in Cookies gespeicherten oder weitergegebenen Daten fällt in den Anwendungsbereich der DSGVO.

Ein Verantwortlicher hat **personenbezogene Daten**, die **unrechtmäßig verarbeitet** wurden, unverzüglich gemäß Art 17 Abs 1 lit d DSGVO **zu löschen**. Dies trifft auch dann zu, wenn eine **Einwilligung widerrufen** wurde und eine **andere Rechtsgrundlage** für die Verarbeitung **fehlt**.

Eine **Einwilligung** muss in **informierter Weise**, **unmissverständlich** und

**eindeutig** abgegeben werden. Eine **versehentliche Einwilligung** durch Betroffene soll durch die Bedingungen für die Einwilligung in Art 7 Abs 2 DSGVO und auch dem Transparenzgrundsatz in Art 5 Abs 1 lit a DSGVO **verhindert werden**.

Ist ein **Einwilligungsbutton** durch Größe, Kontrast und Platzierung **auffällig gestaltet**, die **Widerspruchsmöglichkeit** aber **im Vergleich** dazu **unauffälliger**, kann **mangels Transparenz nicht von** einer eindeutigen **Einwilligung** ausgegangen werden.

Ein Anspruch auf Ausgestaltung der **Widerrufsmöglichkeit** in Form eines "schwebenden" Symbols besteht jedoch nicht.

BVwG 18.11.2024, W274 2284469-1

#### **Entschiedene Sache, Exekutionsverfahren**

- Der Betroffene stellte ein Auskunftersuchen an einen gerichtlich bestellten Gutachter, der im Rahmen eines Verfahrens vor dem Zivilgericht ein Gutachten mit Bezug zum Betroffenen erstellte. Dabei verlangte er ausdrücklich auch Auskunft über die **Herkunft der Daten** gemäß Art 15 Abs 1 lit g DSGVO. Der Betroffene behauptete, der Gutachter habe eine falsche Diagnose gestellt, ohne seine Krankengeschichte zu kennen. Nachdem der Gutachter dem Auskunftersuchen nicht nachkam, brachte der Betroffene eine (erfolgreiche) Datenschutzbeschwerde bei der DSB wegen Verletzung im Recht auf Auskunft ein. Der Gutachter kam dem Ersuchen trotz zweimaligem Hinweis durch die DSB nicht nach, woraufhin die DSB eine Verletzung des Rechts auf Auskunft feststellte und dem Gutachter auftrag, innerhalb von vier Wochen dem Antrag des Betroffenen zu entsprechen. Der Gutachter übermittelte nach ergangenem Bescheid eine Auskunft zur Diagnose des Betroffenen und verwies auf eine frühere Diagnose eines anderen Arztes. Der Betroffene hielt die Diagnose für falsch und verlangte deren Korrektur. Nachdem der Gutachter an seiner Diagnose festhielt, forderte der Betroffene detailliertere Auskunft über die Herkunft der Daten. Der Gutachter verwies hierzu auf den Gerichtsakt. Der Betroffene erachtete diese Auskunft als unzureichend und reichte erneut eine Datenschutzbeschwerde bei der DSB ein, welche die DSB abwies, weil der Gutachter dem Betroffenen bereits Auskunft erteilt habe. Daraufhin erhob der Betroffene eine (erfolgreiche) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die **materielle Rechtskraft** eines Bescheids steht einer **weiteren Entscheidung** in derselben Rechtssache entgegen. Eine Änderung entscheidungsrelevanter Fakten führt dazu, dass die Sache ihre ursprüngliche Identität verliert, womit eine andere Sache vorliegt, über die bescheidmäßig abgesprochen

werden kann oder muss. Bei der Beurteilung der Identität der Sache ist festzustellen, ob an den entscheidungsrelevanten Fakten eine wesentliche Änderung eingetreten ist.

Die Behörde hat die **Identität der Sache** im Vergleich mit dem im **Vorbescheid** angenommenen Sachverhalt zu beurteilen und zu prüfen, ob sich an diesem Sachverhalt oder an seiner rechtlichen Beurteilung eine wesentliche Änderung ergeben hat. Dem Vorbescheid lag eine Datenschutzbeschwerde zugrunde, der einen Antrag auf Feststellung der Rechtsverletzung durch den Gutachter sowie einen Leistungsauftrag zur Entsprechung des Auskunftersuchens umfasste. Die zweite Datenschutzbeschwerde des Betroffenen bezog sich erneut auf die Herkunft der Daten. Die beantragte Auskunft über die Herkunft der Daten war bereits Gegenstand des Leistungsauftrags des ersten Bescheids. Die zweite Datenschutzbeschwerde war daher wegen **entschiedener Sache** zurückzuweisen.

Sollte der Betroffene mit den bisherigen Auskünften nicht zufrieden sein, ist er auf ein allfälliges **Exekutionsverfahren** zu verweisen. Zudem ist darauf hinzuweisen, dass die Fragen des Betroffenen typischerweise bei der Erörterung von Gutachten im Zivilverfahren zu klären sind.

BVwG 18.11.2024, W137 2297057-1

### **Auskunftsrecht, Rechte von Dritten, Öffnungsklausel**

- Ein Mann war über acht Jahre mit der Pflege und Erziehung eines minderjährigen Kindes betraut. Nach einem behördlich eingeleiteten Überprüfungsverfahren wurde das Kind aufgrund von Bedenken hinsichtlich des Kindeswohls anderweitig untergebracht. Die Obsorge ging auf den Kinder- und Jugendhilfeträger über. Dieser verarbeitete personenbezogene Daten des ehemaligen Pflegevaters in mehreren elektronischen Akten. Neben dessen Papierakt lag ein weiterer Akt über das Kind vor, der auch personenbezogene Daten des ehemaligen Pflegevaters enthielt. Dieser stellte ein Auskunftersuchen gemäß Art 15 DSGVO, um Informationen über die Verarbeitung seiner personenbezogenen Daten zu erhalten. Weiters beantragte der ehemalige Pflegevater die Herausgabe seiner Daten in Papierform und forderte eine ungekürzte Übermittlung der beantragten Informationen samt Unterlagen. Die anschließend erteilte Auskunft hielt er für unvollständig. Die DSB wies die Datenschutzbeschwerde ab. Daraufhin erhob der Mann (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Eine Betroffene soll durch die Auskunft in die Lage versetzt werden, sich der Verarbeitung ihrer personenbezogenen Daten bewusst zu sein und deren

Rechtmäßigkeit überprüfen zu können. **Art 15 DSGVO** gewährt jedoch **nur das Recht, die eigenen Daten zu erhalten**. Dementsprechend kann sich der ehemalige Pflegevater in Bezug auf die Daten des Kindes nicht auf Art 15 DSGVO stützen.

Weiters könnte er das Kind im Verfahren nur dann vertreten, wenn dies dessen **Interesse im Rahmen des Kindeswohls** entspräche. Da die Kinder- und Jugendhilfe ein höchst sensibler Bereich ist, können einzelne Informationen gemäß **§ 12 Abs 4 Wiener Kinder- und Jugendhilfegesetz (WKJHG)** unter Berücksichtigung des Kindeswohls unter Umständen nicht erteilt oder Kopien nur eingeschränkt übermittelt werden.

Darüber hinaus darf gemäß Art 15 Abs 4 DSGVO das **Recht auf Erhalt einer Kopie** die **Rechte und Freiheiten anderer Personen** nicht beeinträchtigen. Weiters enthalten die nach der **Öffnungsklausel** des Art 23 DSGVO zulässigen Bestimmungen, ua im WKJHG, **Beschränkungen des Auskunftsrechts aufgrund von Kindeswohlerwägungen**. Diese ähneln den Regelungen des § 4 Abs 6 DSG, die sich auf Geschäfts- und Betriebsgeheimnisse beziehen.

Da dem ehemaligen Pflegevater die **Obsorge entzogen** wurde, ist nicht anzunehmen, dass die **Einsicht in den Papierakt** seines ehemaligen Pflegekindes dem **Kindeswohl dient**. Dementsprechend ist die Zurverfügungstellung des noch nicht beauskunfteten Papierakts bzw der Aktenanteile vor dem Hintergrund des Kindeswohls bzw der sonstigen Einschränkungen des Auskunftsrechts nach dem WKJHG nicht geboten.

Das **Auskunftsrecht** nach der DSGVO unterscheidet sich von den Rechten einer Verfahrenspartei im Rahmen eines Rechtsstreits. Es ist aber nicht dazu gedacht, allfällige **Ausnahmen** von einer **Akteneinsicht auszuhebeln**.

### Aus der Rechtsprechung des BVwG:

- Der **Bürgermeister** einer Stadt ist eine **staatliche Behörde** iSd § 1 Abs 2 DSG. Denn der Begriff "Behörde" ist im **funktionalen Sinn** zu verstehen, davon sind auch **Selbstverwaltungskörper** und alle Stellen der Hoheitsverwaltung erfasst. Eingriffe staatlicher Behörden sind nur aufgrund von **Gesetzen** zulässig, die ausreichend **präzise**, also für **jedermann vorhersehbar**, regeln, unter welchen Voraussetzungen die Verwendung personenbezogener Daten für die **Wahrnehmung konkreter Verwaltungsaufgaben** erlaubt ist (BVwG 25.11.2024, W214 2273462-1).
- Die Verarbeitung bestimmter personenbezogener Daten zum Zweck der Erhebung des **ORF-Beitrags** sowie der Ermittlung der Beitragsschuldner und zur Prüfung, ob eine



Befreiung vorliegt, ist notwendig. Die Regelungen des mit "**Datenübermittlung**" titulierte § 13 ORF-Beitrags-Gesetz (**OBG**) erscheinen **sachgerecht** und sind auf das notwendige bzw verhältnismäßige Maß beschränkt. Ein unzulässiger und unverhältnismäßiger Eingriff in das **Grundrecht auf Datenschutz** durch das OBG ist nicht zu erblicken (BVwG [04.12.2024, W603 2303734-1](#); [03.12.2024, I406 2300562-1](#)).

### **Rechtsprechung der DSB**

[DSB 27.06.2024, 2024-0.028.256](#)

### **Anzeige, Akteneinsicht, Interessenabwägung**

- Der Betroffene machte eine Eingabe bei der Bauabteilung eines Gemeindeamts, in welcher er darauf hinwies, dass die Brandschutzsicherungsmaßnahmen sowie der Schallschutz eines Wohnbaus eines Grundstückseigentümers nicht in Ordnung seien und überprüft werden müssten. Dabei sei ihm nicht klar gewesen, dass es sich bei seiner Eingabe um eine Anzeige handle. Nachdem der Grundstückseigentümer Kenntnis von der Anzeige erlangte, nahm er Akteneinsicht und kontaktierte den Betroffenen telefonisch, wobei auch Beschimpfungen und Drohungen gefallen sein sollen. Das Gemeindeamt legte dem Grundstückseigentümer den Vor- und Nachnamen des Betroffenen offen, nicht aber dessen Telefonnummer. Daraufhin brachte der Betroffene eine (erfolgreiche) Datenschutzbeschwerde gegen das Gemeindeamt bei der DSB ein, weil er sich durch die Weitergabe seiner Daten an den Grundstückseigentümer in seinem Grundrecht auf Geheimhaltung verletzt sah. Die DSB hat erwogen: Gemäß § 1 Abs 1 DSGVO hat Jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Es spielt keine Rolle, auf welche Weise Daten verarbeitet werden, auch eine mündliche Mitteilung kann eine Verletzung sein. Der offengelegte Vor- und Nachname des Betroffenen fällt in den sachlichen Schutzbereich des § 1 DSGVO.

Die Offenlegung durch das Gemeindeamt erfolgte zwar auf Basis einer qualifizierten rechtlichen Grundlage, weil der Grundstückseigentümer sein **Recht auf Akteneinsicht** nach § 17 AVG wahrnahm. Grundsätzlich erstreckt sich die Akteneinsicht auf alle Unterlagen, die sich auf die Sache beziehen. § 17 Abs 3 AVG nimmt jedoch Aktenbestandteile davon aus, wenn der Einsichtnahme legitime Interessen entgegenstehen. Das Gemeindeamt hätte eine **Interessenabwägung** zwischen dem Recht auf Akteneinsicht des Grundstückseigentümers und dem Grundrecht auf Geheimhaltung des Betroffenen vornehmen müssen. Das Interesse des Grundstückseigentümers an vollständiger

Information wäre dabei geringer zu gewichten als das Interesse an Geheimhaltung seitens des Betroffenen. Die Offenlegung der Identität des Betroffenen war zur Gewährleistung des Rechts auf Akteneinsicht nicht notwendig, weshalb eine Verletzung des **Grundsatzes der Datenminimierung** verwirklicht wurde.

### **EU-Rechtsakte**

- Am **08.01.2025** ist die "*VO (EU) 2025/12 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über die Erhebung und Übermittlung vorab übermittelter Fluggastdaten zur Verbesserung und Erleichterung der Kontrollen an den Außengrenzen, zur Änderung der Verordnungen (EU) 2018/1726 und (EU) 2019/817 sowie zur Aufhebung der Richtlinie 2004/82/EG des Rates*", [ABI L 2025/12, 1](#), kundgemacht worden. Mit dieser VO wird den **Fluggesellschaften** die Pflicht auferlegt, bei Flügen **in die Union** sogenannte **API-Daten** (vorab übermittelte Fluggastdaten) zu erheben und diese verschlüsselt an die zuständigen **Grenzbehörden** zu übermitteln. Die API-Daten umfassen Identifizierungs-, Flugzeug- und Gepäckdaten.
- Am **08.01.2025** ist die "*VO (EU) 2025/13 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über die Erhebung und Übermittlung vorab übermittelter Fluggastdaten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität und zur Änderung der Verordnung (EU) 2019/818*", [ABI L 2025/13, 1](#), kundgemacht worden. Mit dieser VO wird den **Fluggesellschaften** die Pflicht auferlegt, zur Bekämpfung der länderübergreifenden **schweren und organisierten Kriminalität** sowie des **Terrorismus** an die sogenannten **PNR-Zentralstellen** verschlüsselte **API-Daten** und **sonstige PNR-Daten** (sonstige Fluggastdatensatzdaten) zu übermitteln.
- Am **10.01.2025** ist die "*RL (EU) 2025/25 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 zur Änderung der Richtlinien 2009/102/EG und (EU) 2017/1132 zur Ausweitung und Optimierung des Einsatzes digitaler Werkzeuge und Verfahren im Gesellschaftsrecht*", [ABI L 2025/25, 1](#), kundgemacht worden. Ziel dieser RL ist es, durch die **Vernetzung von Unternehmensregistern** und die Schaffung von **digitalen Werkzeugen**, die grenzüberschreitende **Gründung von Kapitalgesellschaften, Eintragung von Zweigniederlassungen und Einreichung von Dokumenten und Informationen** bei den **Unternehmensregistern** zu erleichtern.

- Am **10.01.2025** ist eine **Berichtigung** der "VO (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte; **DMA**)", [ABI L 2025/90024, 1](#), kundgemacht worden. Berichtigt wird ein redaktionelles Versehen und die Berichtigung betrifft nur einen Verweis auf die Befugnisse der Europäischen Kommission.
- Am **10.01.2025** ist die "UN-Regelung Nr. 155 – Einheitliche Bedingungen für die **Genehmigung von Fahrzeugen** hinsichtlich der **Cybersicherheit** und des **Cybersicherheitsmanagementsystems**" im Amtsblatt der EU, [ABL L 2025/5, 1](#), kundgemacht worden. Verbindlich ist jedoch die von der UN verabschiedete Originalfassung.

to the point

# Datenschutzmonitor. 03/2025 vom 22.01.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

In der vergangenen Woche wurden die nachstehenden Entscheidungen, Leitlinien und Rechtsakte veröffentlicht:

- **Rechtsprechung des VfGH**

VfGH 02.12.2024, E1380/2024; 02.12.2024, E1379/2024 (Nationalrat, Auskunftsrecht)

- **Rechtsprechung des OGH**

OGH 11.12.2024, 6Ob147/24x (Zentrales Testamentsregister, Erbe, Notar)

- **Rechtsprechung des BVwG**

BVwG 06.11.2024, L532 2300411-1 (Gesetzesprüfungsantrag, Handyauswertung)

BVwG 18.10.2024, W256 2248161-1 (Verarbeitung, Informationspflicht, Ausnahme)

BVwG 30.10.2024, W256 2247276-1 (Präklusion)

BVwG 27.11.2024, W256 2246546-1 (konkrete Rechtsverletzung, kein Recht auf Strafverfahren)

BVwG 10.12.2024, W211 2272735-1 (Verstorbener, Verlust der Parteistellung)

- **Leitlinien**

EDSA Leitlinien 01/2025 über Pseudonymisierung (Pseudonymisierung, Personenbezug, Weiterverarbeitung)

Erklärung zum Zusammenspiel von Datenschutz- und Wettbewerbsrecht (Markt- und Wettbewerbsfaktoren, Datenschutzpraktiken, Regulierungsbehörden)

- **EU-Rechtsakte**

VO (EU) 2025/37 über verwaltete Sicherheitsdienste

CybersolidaritätsVO (EU) 2025/38

## To the Point:

### Rechtsprechung des VfGH

VfGH 02.12.2024, E1380/2024; 02.12.2024, E1379/2024

#### **Nationalrat, Auskunftsrecht**

- Ein Abgeordneter zum Nationalrat stellte zur Vorbereitung seiner parlamentarischen Tätigkeit Auskunftsersuchen zu Korruptionsvorwürfen an den Bundesminister für Bildung, Wissenschaft und Forschung (E1379/2024) und an den Bundesminister für Finanzen (E1380/2024), die er auf das AuskunftspflichtG stützte. Nachdem ihm die Auskünfte verweigert wurden, erhob er Beschwerdebeschwerden an das BVwG, das diese abwies. Begründet wurde dies damit, dass der Abgeordnete das Auskunftsbegehren als Abgeordneter zum Nationalrat gestellt habe. In dieser Funktion komme ihm gemäß Art 52 B-VG (Interpellationsrecht) ein besonderes Auskunftsrecht zu. Aufgrund dieses spezielleren Auskunftsrechts sei eine Auskunft gemäß § 6 AuskunftspflichtG ausgeschlossen. Dagegen erhob er **Erkenntnisbeschwerden** gemäß Art 144 B-VG wegen Verletzung in verfassungsgesetzlich gewährleisteten Rechten an den VfGH, der diesen stattgab und feststellte, dass der Abgeordnete im Recht auf Gleichheit aller Staatsbürger vor dem Gesetz gemäß Art 2 StGG und Art 7 B-VG verletzt wurde.

Der VfGH hat erwogen: Das BVwG begründet seine Entscheidung ausschließlich damit, dass das Auskunftsbegehren in der Funktion eines **Abgeordneten zum Nationalrat** und damit als **Organ der Gesetzgebung** gestellt wurde. Das **Interpellationsrecht** ist in Art 52 B-VG sowie den §§ 90 ff GOG-NR geregelt und unterliegt strengen Formalvoraussetzungen.

**Anfragen von Abgeordneten** sind nur dann eine der Gesetzgebung zuzuzählende Tätigkeit eines gesetzgebenden Organs, wenn sie in der vorgesehenen Weise gestellt wurden. Das Verhalten eines Abgeordneten ist nicht schlechthin immer schon dann der Gesetzgebung zuzuzählen, wenn der Abgeordnete als solcher auftritt. Auch ein Verweis auf die Vorbereitung der parlamentarischen Tätigkeit in den Auskunftsersuchen ändert daran nichts. Auch ein Abgeordneter muss wie **jedermann** das Recht haben, ein Auskunftsbegehren nach dem AuskunftspflichtG zu stellen.

### Rechtsprechung des OGH

Aus der Rechtsprechung des OGH:

#### **Zentrales Testamentsregister, Erbe, Notar**

- Der quotenmäßige Erbe eines Verstorbenen hat kein Recht auf Einsicht in das von der Österreichischen Notariatskammer geführte

**Österreichische Zentrale Testamentsregister** ("ÖZTR"). Auf die Datenverarbeitungen zur Führung des ÖZTR sowie die sich aus dem Recht auf Auskunft, Richtigstellung und Löschung nach § 1 DSG ergebenden Rechte und Pflichten sind die **Notariatsordnung** ("NO") und die nach § 140a Abs 2 Z 8 NO erlassenen Richtlinien ("RL") anzuwenden. § 140c Abs 3 NO sieht eine Übermittlung der registrierten Daten (nur) an die (i) **Verlassenschaftsgerichte** und (ii) öffentlichen **Notare** als Gerichtskommissäre in Verlassenschaftssachen sowie (iii) zu **Kontrollzwecken** an die Gerichte, Notare und Rechtsanwälte vor. Hingegen ist ein Erbe weder in der NO noch in den RL genannt ([OGH 11.12.2024, 6Ob147/24x](#)).

### Rechtsprechung des BVwG

BVwG 06.11.2024, L532 2300411-1

#### **Gesetzesprüfungsantrag, Handyauswertung**

- Im Verfahren vor dem Bundesamt für Fremdenwesen und Asyl zielen die **§§ 35a, 39, 39a BFA-VG** darauf ab, die Reiseroute und Identität eines **Asylwerbers** zu ermitteln. Dazu erlauben sie die Sicherstellung und – aufgrund behördlicher Anordnung – die Auswertung von Datenträgern. Die Auswertung eines Datenträgers setzt lediglich voraus, dass ein Antrag auf internationalen Schutz gestellt wurde, eine Feststellung der Identität nicht möglich ist und eine Auswertung nicht bereits durch die Erstaufnahmestelle erfolgt ist.

In einem **Maßnahmenbeschwerdeverfahren** wurde die Verfassungskonformität dieser Bestimmungen in Frage gestellt, weil sie weitreichende Eingriffsbefugnisse ohne angemessenen Rechtsschutz und Garantien für die Betroffenen vorsehen würden. Erst kürzlich habe der VfGH entschieden, dass die Abnahme und Sicherstellung von Mobiltelefonen im strafrechtlichen Ermittlungsverfahren ohne richterliche Bewilligung gegen das Grundrecht auf Datenschutz und das Recht auf Privatleben verstoße und daher verfassungswidrig sei.

Die Maßnahmen im BFA-VG böten bei **gleicher Eingriffsintensität** schwächere Garantien zum Schutz der Geheimhaltungsinteressen der Betroffenen als die für verfassungswidrig erklärten Regelungen der StPO. Der Grundrechtseingriff könne im Rahmen einer Maßnahmenbeschwerde nicht vollständig angefochten werden, sodass der gesetzlich vorgesehene **Rechtsschutz** gegen die Sicherstellung und Auswertung eines Datenträgers unzureichend sei.

Das BVwG teilt diese Bedenken, setzte das Maßnahmenbeschwerdeverfahren aus und stellte einen **Gesetzesprüfungsantrag** an

den VfGH auf Aufhebung einzelner Bestimmungen des BFA-VG.

Das BVwG hat erwogen: Es bestehen erhebliche Bedenken an der Verfassungskonformität der **§§ 35a, 39, 39a BFA-VG** und des **§ 38 Abs 2 BFA-VG**. Zwar wurde die Verfassungsmäßigkeit von § 38 Abs 2 BFA-VG nicht in Zweifel gezogen, doch darf diese Bestimmung bei einer Aufhebung der übrigen Bestimmungen nicht bestehen bleiben.

Dem Gesetzgeber steht es frei, für verschiedene Regelungsregime wie Strafprozessrecht und fremdenrechtliches Verfahrensrecht unterschiedliche Anordnungen zu treffen. Es ist jedoch nicht nachvollziehbar, warum **gravierende unterschiedliche Anforderungen** gelten sollten, die zu **unsachlichen Schlechterstellungen** führen.

Ein gangbarer gesetzgeberischer Weg wäre, die Anordnungsbefugnis zur Datenträgersicherung unverändert im Rechtsbestand zu belassen, die Anordnung zur Datenträgerauswertung jedoch von einer bekämpfbaren Entscheidung des BVwG abhängig zu machen, sodass die **Rechtsschutzmöglichkeiten** von betroffenen Fremden bei gleichzeitiger Sicherstellung effektiver verwaltungsbehördlicher Verfahrensführung gewahrt blieben.

BVwG 18.10.2024, W256 2248161-1

#### **Verarbeitung, Informationspflicht, Ausnahme**

- Ein Wahlberechtigter abonnierte über die Website einer politischen Partei deren Newsletter unter Angabe seiner E-Mail-Adresse. Diese enthielten Informationen über politische Themen und Aktivitäten in Form von Texten, die von Regierungsmitgliedern verfasst und unterzeichnet wurden. Der Versand erfolgte über das technische Netzwerk der Partei und in deren eigener Verantwortung.

Der Wahlberechtigte stellte ein Auskunftsersuchen nach Art 15 DSGVO. Die darauf erteilte Auskunft hielt er für unzureichend. Zudem vertrat er die Ansicht, dass eine Offenlegung seiner personenbezogenen Daten an Dritte erfolgt sei. Weiters monierte er eine Verletzung der Informationspflicht gemäß Art 14 DSGVO wegen der Verarbeitung seiner Daten aus der Wählerevidenz. Die DSB stellte zwar fest, dass die Partei sein Recht auf Auskunft verletzt hatte, jedoch sei keine Offenlegung an Dritte erfolgt. Weiters wurde die Datenschutzbeschwerde hinsichtlich der Verletzung der Informationspflicht abgewiesen. Daraufhin erhob der Wahlberechtigte (erfolglose) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Der Spruch enthält keine explizite Abweisung in Bezug auf die vom Wahlberechtigten aufgezeigte

Unvollständigkeit der Auskunft. **Fehlt es dem Spruch an der gebotenen Deutlichkeit**, so ist die **Bescheidbegründung zu seiner Auslegung** heranzuziehen. Unter Berücksichtigung der Bescheidbegründung kann kein Zweifel daran bestehen, dass die Datenschutzbeschwerde in dieser Hinsicht abgewiesen wurde.

Nach Art 4 Z 2 DSGVO fällt nicht nur die Offenlegung durch Übermittlung, sondern bereits **jede "andere Form der Bereitstellung"** unter den Begriff einer Verarbeitung. Damit wird der Charakter der Offenlegung als "Zugänglichmachen" verdeutlicht. Jedoch räumte man den jeweiligen Regierungsmitgliedern in keiner Weise eine Einblicksmöglichkeit in die Daten des Wahlberechtigten ein. Es wurden lediglich von diesen bereitgestellte Texte in die Newsletter kopiert und in weiterer Folge unter Verwendung der Daten des Wahlberechtigten an diesen versendet.

Gemäß Art 14 DSGVO hat der Verantwortliche der Betroffenen bestimmte Informationen zur Verfügung zu stellen. Nach **Art 14 Abs 5 lit c DSGVO entfallen die Informationspflichten**, wenn und soweit eine **Rechtsvorschrift** die Erhebung oder (zweckändernde) Offenlegung bestimmter Daten **ausdrücklich regelt**.

Die Daten des Wahlberechtigten wurden aufgrund der Bestimmung des **§ 4 Abs 2 Wählerevidenzgesetz** aus der Wählerevidenz der Gemeinde erhoben. Die **Ausnahmeregelung** des Art 14 Abs 5 lit c DSGVO greift hier zwar nicht, weil die Partei nicht verpflichtet war, die Daten zu erheben, sondern die **Erhebung freiwillig erfolgte**. Die Partei hatte aber bereits im Zeitpunkt der Datenerhebung in ihrer **Datenschutzerklärung** über die Datenverarbeitung informiert. Die **zusätzliche Nennung** der bereits im Gesetz ausreichend klar und präzise geregelten Informationen gemäß Art 14 DSGVO ist in einem solchen Fall nicht erforderlich. Schon allein der Hinweis auf die tatsächliche Datenverarbeitung versetzt die betroffene Person in die Lage, sich **anhand der Rechtsvorschrift** einen hinreichenden Überblick über die konkrete Datenverwendung zu verschaffen.

Da die gegenständliche Datenerhebung zum Zweck der **Kommunikation** erfolgt ist, bestehen im Hinblick auf die **Ausnahmeregelung** des **Art 14 Abs 3 lit b DSGVO** auch keine Bedenken daran, dass die Informationserteilung der Partei rechtzeitig erfolgt ist.

BVwG 30.10.2024, W256 2247276-1

#### **Präklusion**

- In einem Rechtsstreit vor Gericht übermittelte die beklagte Klinik Gesundheitsdaten auf deren Ansuchen an die dem Rechtsstreit beigetretene Nebenintervenientin. Von der

Datenübermittlung erfuhr der klagende Patient von der Klinik im Mai 2019 aufgrund eines Auskunftersuchens. Der Patient fühlte sich durch diese Vorgehensweise in seinem Recht auf Geheimhaltung verletzt, weil die Übermittlung der Gesundheitsdaten zur Verteidigung von Rechtsansprüchen nicht notwendig gewesen sei und brachte im Juni 2020 Datenschutzbeschwerde bei der DSB ein. Die DSB wies die Datenschutzbeschwerde ab. Dagegen erhob der Patient Bescheidbeschwerde an das BVwG. Das BVwG wies die Bescheidbeschwerde wegen bereits eingetretener Präklusion gemäß § 24 Abs 4 DSG zurück.

Das BVwG hat erwogen: Die Verjährungsregelung des § 24 Abs 4 DSG ist eine **Präklusivfrist**, die von Amts wegen wahrzunehmen ist und die Lebensdauer eines Rechts nicht verlängerbar begrenzt. Da die DSGVO keine Vorschriften oder Fristen für die Rechtsverfolgung enthält, ist es Sache jedes einzelnen Mitgliedstaats, das Verfahren für die Rechtsverfolgung und auch die Präklusion von Rechten in seiner innerstaatlichen Rechtsordnung unter Wahrung der Grundsätze der **Äquivalenz** und **Effektivität** auszugestalten.

Das Grundrecht auf Datenschutz darf nur unter Einhaltung strenger Bedingungen eingeschränkt werden. Zulässige Einschränkungen müssen dabei gesetzlich vorgesehen sein, den Wesensgehalt des betreffenden Rechts beachten sowie unter Wahrung des Grundsatzes der **Verhältnismäßigkeit** erforderlich sein und dem von der EU anerkannten Gemeinwohl entsprechen. Die Präklusion und somit die Einschränkung des Grundrechts auf Datenschutz ist in § 24 Abs 4 DSG gesetzlich vorgesehen.

Die **einjährige Präklusivfrist** des § 24 Abs 4 DSG beginnt mit Kenntnis der Betroffenen vom "beschwerenden Ereignis" zu laufen. Der Patient war nach der Beantwortung des Auskunftersuchens im Mai 2019 in der Lage, das zur Begründung seines Anspruchs erforderliche Sachvorbringen in Form einer Datenschutzbeschwerde konkret zu erstatten. Die einjährige **subjektive Frist** des § 24 Abs 4 DSG begann daher ab diesem Zeitpunkt zu laufen und war bei Beschwerdeerhebung schon verstrichen.

#### Aus der weiteren Rechtsprechung des BVwG:

- Die Behörden und Gerichte dürfen nur darüber absprechen, was beantragt wurde. Sie sind an den Inhalt der Datenschutzbeschwerde gebunden. Gegenstand des Verfahrens ist daher ausschließlich die zugrundeliegende Datenschutzbeschwerde und die darin **konkret geltend gemachte Rechtsverletzung**. Weder die DSB noch das BVwG haben im Falle einer behaupteten Verletzung im Recht auf Auskunft jegliche Rechtsverletzung zu überprüfen. Ein **subjektives Recht**

auf **Einleitung eines Strafverfahrens** besteht **nicht**. Darüber hinaus gilt nach § 25 Abs 1 VStG das **Prinzip der Amtswegigkeit**. Die Behörde hat sowohl bei der Einleitung als auch bei der Durchführung des Verwaltungsstrafverfahrens von Amts wegen vorzugehen. Der Betroffene hat keinen Anspruch auf Einleitung eines Verwaltungsstrafverfahrens ([BVwG 27.11.2024, W256 2246546-1](#)).

- Stirbt der Betroffene, hat das BVwG den angefochtenen Bescheid ersatzlos aufzuheben. Das Datenschutzrecht ist ein **höchstpersönliches Recht**, das mit dem **Tod** des Betroffenen untergeht und nicht auf einen etwaigen Rechtsnachfolger übergehen kann. Mit dem **Verlust der Parteistellung** fällt die Berechtigung weg, eine Datenschutzbeschwerde zu erheben. Damit einhergehend fällt die Berechtigung der DSB weg, über die Datenschutzbeschwerde zu entscheiden ([BVwG 10.12.2024, W211 2272735-1](#)).

#### **Neues vom EDSA**

EDSA Leitlinien 01/2025 über Pseudonymisierung (2025)

#### **Pseudonymisierung, Personenbezug, Weiterverarbeitung**

- Der Europäische Datenschutzausschuss (EDSA) hat Leitlinien zur Pseudonymisierung angenommen, in welchen der EDSA insb die Definition und Anwendbarkeit der **Pseudonymisierung** und deren Vorteile erläutert. Klargestellt wird, dass pseudonymisierte Daten, die einer Person (vom Verantwortlichen oder einer anderen Person) durch zusätzliche Informationen zugeordnet werden könnten, immer noch **personenbezogene Daten** sind. Die Pseudonymisierung kann Risiken reduzieren und die Nutzung **berechtigter Interessen** als Erlaubnistatbestand erleichtern, sofern alle anderen Anforderungen der DSGVO erfüllt sind. Die Pseudonymisierung kann dazu beitragen, iSd **Art 6 Abs 4 DSGVO** die Vereinbarkeit der Weiterverarbeitung mit dem ursprünglichen Zweck zu gewährleisten. Die Pseudonymisierung kann Organisationen auch helfen, ihren Verpflichtungen gemäß Art 5, 25 und 32 DSGVO nachzukommen. Bestimmte **technische Maßnahmen** und Garantien bei der Verwendung von Pseudonymisierung können zudem die Vertraulichkeit gewährleisten und eine unbefugte Identifizierung von Personen verhindern. **Anm: Die Leitlinien werden bis zum 28.02.2025 einer öffentlichen Konsultation unterzogen, um Interessenträgern Gelegenheit zur Stellungnahme zu geben.**

Erklärung zum Zusammenspiel von Datenschutz- und Wettbewerbsrecht


**Markt- und Wettbewerbsfaktoren, Datenschutzpraktiken, Regulierungsbehörden**

- Der EDSA hat eine Erklärung zum Zusammenspiel von **Datenschutz- und Wettbewerbsrecht** angenommen, in der Konstellationen erörtert werden, in denen sich diese Rechtsgebiete überschneiden können. Obwohl es separate Rechtsgebiete mit unterschiedlichen Zielen in unterschiedlichen Rahmen sind, können sie in bestimmten Fällen für dieselben Einrichtungen gelten. Unter bestimmten Voraussetzungen sollen Schritte zur Einbeziehung von **Markt- und Wettbewerbsfaktoren** in die **Datenschutzpraktiken** und zur Berücksichtigung von Datenschutzvorschriften bei Wettbewerbsbewertungen gemacht werden.

Die Zusammenarbeit zwischen den **Regulierungsbehörden** soll verbessert werden, ua indem eine zentrale Anlaufstelle eingerichtet wird, um die Koordinierung zwischen Regulierungsbehörden zu fördern.

### **EU-Rechtsakte**

- Am **15.01.2025** ist die "VO (EU) 2025/37 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 zur Änderung der Verordnung (EU) 2019/881 im Hinblick auf **verwaltete Sicherheitsdienste**", [ABI L 2025/37, 1](#), kundgemacht worden. Mit dieser VO werden europäische Schemata für die **Cybersicherheitszertifizierung** eingeführt. Zudem wird ua ein europäischer **Zertifizierungsrahmen** für die Cybersicherheit geschaffen.
- Am **15.01.2025** ist die "VO (EU) 2025/38 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der Verordnung (EU) 2021/694 (**Cybersolidaritätsverordnung**)", [ABI L 2025/38, 1](#), kundgemacht worden. Mit dieser VO werden Maßnahmen zur Stärkung der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von **Cyberbedrohungen** und **Sicherheitsvorfällen** festgelegt.



to the point

# Datenschutzmonitor. 04/2025 vom 29.01.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 23.01.2025, 31175/14, *Reznik/Ukraine* (Durchsuchung, Beschlagnahme, Anwaltsgeheimnis, wirksames Rechtsmittel)

- **Rechtsprechung des BVwG**

BVwG 16.12.2024, W137 2288040-1 (Rollenverteilung, Identitätsdokumentenregister)

BVwG 16.12.2024, W137 2292450-1 (Trafik, Video, Piktogramm, Geldstrafe)

BVwG 04.12.2024, W176 2295345-1 (Rechtsanwalt, Anwaltsgeheimnis, Beschwerdegegner)

BVwG 25.10.2024, W211 2295570-1 (Besetzung des Präsidiums des BVwG, "social watchdog")

BVwG 27.11.2024, W252 2299666-1 (Beschwerde, Untersagung, keine Geldbuße)

- **Rechtsprechung des BFG**

BFG 19.12.2024, RV/7102904/2021 (WiEReG, Meldepflicht)

- **Rechtsprechung der DSB**

DSB 16.10.2024, 2024-0.641.771 (Geldstrafe, handelsrechtlicher Geschäftsführer, Datenschutzbeauftragter)

DSB 21.09.2022, 2022-0.672.331 (Videoüberwachung, Mitwirkungspflicht, freie Beweiswürdigung)



## To the Point:

### Rechtsprechung des EGMR

EGMR 23.01.2025, 31175/14, *Reznik/Ukraine*

#### **Durchsuchung, Beschlagnahme, Anwaltsgeheimnis, wirksames Rechtsmittel**

- Ein Anwalt schloss einen Vertrag über Rechtsdienstleistungen mit dem ukrainischen Informationszentrum ab, in dem die Übermittlung von Dokumenten zur Untersuchung und Analyse vereinbart wurde. Nach Beginn strafrechtlicher Ermittlungen gegen die Leitung des Informationszentrums forderte dieses den Rechtsanwalt zur Rückgabe der übergebenen Dokumente auf. Dieser Aufforderung kam der Anwalt nach. Dennoch wurde ein Durchsuchungsbeschluss für die Wohnung des Anwalts genehmigt. Der stellvertretende Generalstaatsanwalt wurde ermächtigt, Dokumente über die finanzielle und kommerzielle Tätigkeit des Informationszentrums und anderer konkret benannten Unternehmen und Einzelpersonen, die mit dem Informationszentrum in Verbindung standen, sowie IT-Geräte, mobile Kommunikationsgeräte und Datenspeicher sicherzustellen. Der Beschluss wurde für unanfechtbar erklärt. Während der Durchsuchung, bei der ua auch Vertreter der Anwaltskammer anwesend waren, wurden ua ein Computer und ein USB-Stick beschlagnahmt und zur forensischen Untersuchung weitergeleitet. Die Einwände und Beschwerden der Vertreter der Anwaltskammer und des Anwalts blieben zunächst erfolglos. Schlussendlich wurden dem Anwalt die beschlagnahmten Datenspeicher zurückgegeben.

Der EGMR stellte fest, dass eine Verletzung von Art 8 und Art 13 EMRK vorliegt und sprach dem Anwalt EUR 6.000 immateriellen Schadenersatz und EUR 3.450 Kostenersatz zu.

Der EGMR hat erwogen: Die Durchsuchung der Wohnung und die Beschlagnahme von Dokumenten und Geräten greifen in die **Rechte des Anwalts auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs** ein. Ein solcher Eingriff muss gesetzlich vorgesehen sein, einem legitimen Ziel dienen und in einer demokratischen Gesellschaft notwendig sein.

Der Durchsuchungsbeschluss basierte auf der ukrainischen Strafprozessordnung und dem Anwaltsgesetz, die **spezifische Verfahrensgarantien** zum Schutz des **Anwaltsgeheimnisses** vorsahen. Die Gesetze verlangten, dass Durchsuchungen von Anwaltspraxen nur mit richterlicher Genehmigung und unter Anwesenheit eines Vertreters der Anwaltskammer durchgeführt werden. Der Vertreter der Anwaltskammer hatte das Recht, Fragen zu stellen und Einwände

zu erheben, die im Durchsuchungsprotokoll festzuhalten waren.

Die Einwände des Vertreters hatten jedoch keine praktische Wirkung, und sie konnten die Beschlagnahme der Gegenstände nicht verhindern. Die Durchsuchung und die Beschlagnahme wurden daher ohne ausreichende verfahrensrechtliche Schutzmaßnahmen durchgeführt, was zu einem **unverhältnismäßigen Eingriff** führte. Außerdem waren die Durchsuchung und Beschlagnahme in einer demokratischen Gesellschaft nicht notwendig, weil die richterliche Anordnung zu weit gefasst war und keine ausreichenden Gründe für die Annahme enthielt, dass relevante Beweismittel bei dem Anwalt gefunden würden.

Es muss ein **wirksames Rechtsmittel** zur Verfügung stehen, um die **Rechtmäßigkeit der Durchsuchung und Beschlagnahme** anzufechten. Das ukrainische Recht bietet keine Möglichkeit, eine Durchsuchungsanordnung anzufechten, sodass die verfügbaren Rechtsmittel unzureichend sind. Die Möglichkeit, beschlagnahmte Gegenstände zurückzufordern, reicht nicht aus, um die Beschwerden über die Rechtmäßigkeit der Durchsuchung zu behandeln.

### Rechtsprechung des BVwG

BVwG 04.12.2024, W176 2295345-1

#### **Trafik, Video, Piktogramm, Geldstrafe**

- Ein Trafikant brachte an der Außenmauer seiner Trafik zwei Videokameras an, um sich vor Überfällen zu schützen. Die Kameras erfassten Teile des öffentlichen Gehsteigs, den angrenzenden Fahrradweg und einen Abschnitt der Straßenbahngleise. Durch die Überwachung konnte der Trafikant ein Foto einer Passantin anfertigen, welches sie dabei zeigte, wie diese von Ihrem Hund hinterlassenen Exkremamente nicht wegräumte. Um auf das seines Erachtens unrechtmäßige Verhalten der Passantin aufmerksam zu machen, brachte der Trafikant das aufgenommene Foto vor seiner Trafik an. Durch einen leicht entfernbarer Sticker über das Gesicht der Passantin anonymisierte er das Foto. Der Sticker löste sich jedoch. Ein Bürger erhob gegen dieses Vorgehen Datenschutzbeschwerde bei der DSB. Die DSB verhängte wegen der unrechtmäßigen Datenverarbeitung und der nicht erteilten Information zu der Datenverarbeitung eine Geldstrafe iHv EUR 1.500 (zzgl. Verfahrenskostenbeitrag von EUR 150). Gegen das Straferkenntnis erhob der Trafikant (hinsichtlich der Strafhöhe erfolgreiche) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Mangels **Öffnungsklausel** in der DSGVO kommen die §§ 12 und 13 DSGVO bei der Prüfung der Zulässigkeit einer Videoüberwachung nicht zur

Anwendung. Nach der DSGVO dürfen personenbezogene Daten nur auf rechtmäßige Weise, nach **Treu und Glauben** und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Das Interesse am Schutz des Vermögens vor Angriffen in Form von Sachbeschädigungen, Raubfällen, etc überwiegt die Interessen Betroffener in einem kleinen Bereich vor der Trafik. Auch bei einer unbedingt erforderlich erscheinenden Videoüberwachung müssen jedoch Maßnahmen zur Einschränkung des Erfassungsbereichs getroffen werden. **Videoüberwachungsanlagen** dürfen den angrenzenden öffentlichen Raum geringfügig erfassen, sofern dies erforderlich ist, um eine sinnvolle Videoüberwachung zu ermöglichen. Eine Überwachung des gesamten öffentlichen Gehsteigs inkl weiter Teile des angrenzenden öffentlichen Raums ist nicht vom berechtigten Interesse gedeckt.

Am Aufzeigen des **Fehlverhaltens einer Passantin** besteht kein berechtigtes Interesse. Ein Überkleben mit einem leicht entfernbaren Sticker ist **kein geeignetes Mittel** zur **Anonymisierung**.

Die Erfüllung der Informationspflicht durch Kennzeichnung einer Videokamera durch **Piktogramme** kann zulässig sein, wenn es sich um die erste "Schicht" der Informationserteilung handelt und weitere Informationen zur Datenverarbeitung aufliegen.

Die **Geldstrafe** ist wegen des Hinzutretens eines **Milderungsgrundes** und der Verschlechterung der Vermögensverhältnisse des Trafikanten auf EUR 750 (zzgl EUR 75 Verfahrenskostenbeitrag) zu **reduzieren**.

#### BVwG 16.12.2024, W137 2292450-1

##### **Rechtsanwalt, Anwaltsgeheimnis, Beschwerdegegner**

- Ein Fitnesscentermitglied führte gegen die Betreiberin des Fitnesscenters wegen der unberechtigten Erhöhung von Mitgliedsbeiträgen ein zivilgerichtliches Verfahren. Im Verfahren vor dem **Landesgericht ("LG")** wurde vom Rechtsanwalt der Betreiberin des Fitnesscenters eine Mailkorrespondenz mit einer Zeugin als Beweis für das Zustandekommen von Mitgliederverträgen vorgelegt. Die Korrespondenz enthielt den Namen, die Mailadresse und die Information über das Vertragsverhältnis der Zeugin. Die Zeugin fühlte sich durch die Vorgehensweise in ihrem Recht auf Geheimhaltung verletzt und brachte explizit Datenschutzbeschwerde gegen die Betreiberin des Fitnesscenters bezüglich der Vorlage der E-Mails beim LG ein. Die Betreiberin stütze die Rechtmäßigkeit der Verarbeitung der Daten auf die Erfüllung eines Vertrags und auf ihr berechtigtes Interesse. Die DSB gab der Datenschutzbeschwerde statt. Dagegen erhob die

Betreiberin des Fitnesscenters Beschwerde an das BVwG, das den Bescheid der DSB ersatzlos behob.

Das BVwG hat erwogen: **Rechtsanwälte** handeln, wenn sie Daten für den Zweck der Vertretung ihrer Mandanten verarbeiten, regelmäßig als für die Verarbeitung Verantwortliche im Sinne der DSGVO. Die Entscheidung, welche Daten für die Erfüllung des Mandats zu verarbeiten sind, wird, vorbehaltlich eines Beweises für das Gegenteil, vom Rechtsanwalt ohne Weisung des Mandanten getroffen.

Die Rechte der Betroffenen kommen nur in dem Umfang zur Anwendung, als dem nicht das **Recht des Rechtsanwalts auf Verschwiegenheit** zum Schutz der Partei oder der Rechte und Freiheiten anderer Personen oder der Durchsetzung zivilrechtlicher Ansprüche entgegensteht, sonst bestünde die Gefahr, dass der (Prozess-)Gegner einer zivilrechtlichen Streitigkeit im Weg des Auskunftsrechts nach der DSGVO Auskünfte aus den Akten des gegnerischen Rechtsanwalts erhalten könnte.

Ausschließlicher Gegenstand des Verfahrens war die Übermittlung der E-Mailkorrespondenz als **Beweismittel im Gerichtsprozess** durch den eigenständig agierenden Rechtsanwalt. Das Verfahren hätte aber gegen den Rechtsanwalt der Betreiberin des Fitnesscenters und nicht gegen diese selbst geführt werden müssen.

Die nicht **rechtskundige Zeugin** hat in der Datenschutzbeschwerde den **falschen Beschwerdegegner** bezeichnet. Die richtige Einordnung des Rechtsanwalts als Verantwortlichen für die Datenverarbeitung kann aber von ihr nicht verlangt werden.

Da das BVwG das Beschwerdeverfahren nicht gegen den Rechtsanwalt anstelle der Betreiberin des Fitnesscenters führen darf, ist der Bescheid der DSB ersatzlos zu beheben. Das Verfahren ist damit **erneut** zur inhaltlichen Entscheidung **bei der DSB anhängig**.

#### BVwG 16.12.2024, W137 2288040-1

##### **Rollenverteilung, Identitätsdokumentenregister**

- Anlässlich einer Lärmerregung und Störung der öffentlichen Ordnung forderten Polizeibeamte eine Passantin zur Identitätsfeststellung in Form einer Ausweisleistung auf. Da sich die Passantin weigerte, ihren Ausweis vorzuzeigen, wurde sie schließlich von den Polizeibeamten festgenommen und zur nächstgelegenen Polizeiinspektion verbracht, wo eine Abfrage ihres Lichtbildes im **Identitätsdokumentenregister ("IDR")** erfolgte. Die Passantin brachte eine auf das Recht auf Geheimhaltung gestützte Datenschutzbeschwerde gegen den Magistrat der

Stadt Wien als **Passbehörde** ("MA 62") ein. Die DSB wies die Datenschutzbeschwerde ab. Die hiergegen erhobene Bescheidbeschwerde wies das BVwG ab.

Das BVwG hat erwogen: Die Stellung als **datenschutzrechtlicher Verantwortlicher** hat diejenige natürliche oder juristische Person, **Behörde**, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Ergibt sich die Stellung als Verantwortlicher nicht aufgrund gesetzlicher Bestimmungen, muss die Qualifikation einer Partei als Verantwortlicher auf der Grundlage einer Bewertung der tatsächlichen Umstände der Verarbeitung festgestellt werden.

Die Bestimmung des § 52 SPG ermächtigt die Sicherheitsbehörden, personenbezogene Daten von Personen zu verarbeiten, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Das SPG regelt jedoch nicht, wem die datenschutzrechtliche Verantwortlichkeit für eine Abfrage aus dem IDR im Zuge einer Identitätsfeststellung zukommt. Die Mittel- und Zweckentscheidung war daher aufgrund der tatsächlichen Umstände zu beurteilen. Die Polizeibeamten als Bedienstete der **Landespolizeidirektion ("LPD")** haben selbst und allein für die LPD bestimmt, dass sie nach einer erfolgten Festnahme der Beschwerdeführerin eine Abfrage aus dem IDR im Zuge der Identitätsfeststellung tätigen. Sie haben damit den Zweck der Datenverarbeitung – in *concreto* die Feststellung der Identität der Passantin – allein bestimmt. Damit ist die LPD, der das Handeln der Polizeibeamten zuzurechnen ist, als alleinige Verantwortliche anzusehen. Mangels Rechtswidrigkeit des angefochtenen Bescheids war die Bescheidbeschwerde vom BVwG als unbegründet abzuweisen.

Aus der weiteren Rechtsprechung des BVwG:

- Die Besetzung des **Präsidiums des BVwG** ist eine Angelegenheit des **Interesses der Allgemeinheit**. Dem um die Auskunft ersuchenden **Journalisten** kommt als "**social watchdog**" eine wichtige Rolle für die Garantie der **Meinungsäußerungs- und Informationsfreiheit** zu. Die **Namen jener Bewerber**, die von der eingesetzten Kommission nicht vorgeschlagen wurden, sind jedoch schützenswerte personenbezogene Daten. Diese Bewerber mussten nicht damit rechnen, dass ihre Identität und die Einschätzungen und Wertungen der Kommission veröffentlicht werden. Die Herausgabe des **ungeschwärtzten Gutachtens** der Kommission sowie des **ungeschwärtzten Minderheitsvotums** wird daher **verweigert** ([BVwG 25.10.2024, W211 2295570-1](#)).
- Gibt die DSB einer Datenschutzbeschwerde statt, ist der Betroffene in keinem

subjektiven Recht verletzt. Die Bescheidbeschwerde ist mangels **formeller Beschwer** unzulässig. Voraussetzung für eine **Untersagung** der Verarbeitung iSd **§ 22 Abs 4 DSG** ist, dass die Datenverarbeitung noch nicht abgeschlossen ist. Zudem gibt es keinen subjektiven Rechtsanspruch auf eine solche Untersagung. Im Administrativverfahren kann **keine Geldbuße** gegen einen Verantwortlichen verhängt werden. Auf das Verhängen einer Geldbuße besteht auch kein subjektiver Rechtsanspruch. Weiters kann gegen **Körperschaften des öffentlichen Rechts** gemäß § 30 Abs 5 DSG keine Geldbuße verhängt werden ([BVwG 27.11.2024, W252 2299666-1](#)).

### **Rechtsprechung des BFG**

Aus der Rechtsprechung des BFG:

- Der EuGH hat mit Urteil vom [22.11.2022, C-37/20 und C-601/20, Luxembourg Business Registers](#), entschieden, dass die Bestimmung des Art 30 Abs 5 der **5. Geldwäschrichtlinie**, die den öffentlichen Zugang zu Informationen über **wirtschaftliche Eigentümer** vorsieht, ungültig ist. Der EuGH begründete dies mit einem schwerwiegenden Eingriff in das Recht auf Achtung des Privat- und Familienlebens sowie das Recht auf **Schutz personenbezogener Daten**. Diese Entscheidung betrifft jedoch nur die öffentliche Einsicht in das Register der wirtschaftlichen Eigentümer gemäß **§ 10 WiEReG** und nicht die **Meldepflicht** selbst. Die Verpflichtung zur Meldung und deren Erzwingung verletzen keine Grundrechte ([BFG 19.12.2024, RV/7102904/2021](#)).

### **Rechtsprechung der DSB**

DSB 16.10.2024, 2024-0.641.771

#### **Geldstrafe, handelsrechtlicher Geschäftsführer, Datenschutzbeauftragter**

- Die DSB verhängte eine Geldstrafe von EUR 5.500 gegen ein Unternehmen, weil dieses ihren handelsrechtlichen Geschäftsführer ("**Gf**") als **Datenschutzbeauftragten ("DSBA")** benannte, ohne sicherzustellen, dass diese **Doppelrolle** nicht zu einem Interessenkonflikt führt. Das Unternehmen hat dadurch eine ungeeignete Person als Datenschutzbeauftragten benannt. Der Verstoß erstreckte sich über den Zeitraum von etwa drei Jahren.

Die DSB hat erwogen: Das Unternehmen verstieß gegen ihre Pflicht gemäß Art 38 Abs 6 DSGVO, indem sie ihren Gf zum DSBA benannte, obwohl dieser aufgrund seiner gleichzeitigen Tätigkeit als Gf und DSBA einem Interessenkonflikt unterlag, weshalb im Ergebnis eine ungeeignete Person als DSBA benannt wurde. Ein **Interessenkonflikt** liegt vor, wenn der DSBA zugleich Aufgaben

oder Pflichten wahrnimmt, die die Ausübung seiner Stellung beeinträchtigen könnten. Dies ist insbesondere bei **leitenden Managementpositionen** wie der Geschäftsführung der Fall. Dem DSBA dürfen keine Aufgaben oder Pflichten übertragen werden, die ihn dazu veranlassen, die Zwecke und Mittel der Verarbeitung personenbezogener Daten festzulegen, weil deren Überwachung unabhängig durchgeführt werden muss.

Bei der Strafzumessung ist insb der **Umsatz** (Geschäftsjahr 2023: EUR 4 Millionen), die Schwere der Zuwiderhandlung (niedrig; "low level of seriousness"), die Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes (Fahrlässigkeit, weil sich das Unternehmen nicht mit seinen Verpflichtungen auseinandergesetzt hat, obwohl dies zumutbar und möglich gewesen wäre), die bisherigen Verstöße (keine) und die Mitwirkung im Ermittlungsverfahren als Bemessungsgrundlage heranzuziehen. Eine Geldstrafe von EUR 5.000 (zzgl EUR 500 Verfahrenskostenbeitrag) ist angemessen.

DSB 21.09.2022, 2022-0.672.331

### **Videoüberwachung, Mitwirkungspflicht, freie Beweiswürdigung**

- Die Nachbarin der Betroffenen betrieb eine Kamera mit Video- und Tonüberwachung an ihrer Wohnungstüre, welche auch die Wohnungstüre der Betroffenen sowie den Stiegen- und Liftbereich umfasste. Nachdem die Nachbarin trotz Aufforderung, die Überwachung zu unterlassen, nicht reagierte, brachte die Betroffene bei der DSB eine Datenschutzbeschwerde wegen Verletzung ihres Rechts auf Geheimhaltung ein.

Die DSB forderte die Nachbarin mehrmals zur Stellungnahme auf, jedoch ohne Erfolg. Daraufhin leitete die DSB amtswegig ein Verwaltungsstrafverfahren wegen Verletzung der Mitwirkungspflicht iSd Art 31 DSGVO ein und verhängte eine Geldbuße.

Anschließend setzte die DSB das Administrativverfahren fort, stellte eine Verletzung des Rechts auf Geheimhaltung fest und trug der Nachbarin auf, den Bild- und Tonaufnahmebereich der von ihr betriebenen Kamera einzuschränken.

Die DSB hat erwogen: Dort, wo der Behörde die Ermittlung von Tatsachen ohne Mitwirkung der Partei nicht möglich ist, liegt es an der Partei, ihr Wissen einzubringen. Die nicht gehörige **Mitwirkungspflicht** im Beweisverfahren unterliegt der **freien Beweiswürdigung**, in dessen Rahmen die Behörde auch negative Schlüsse ziehen kann.

Die **Kamera** der Nachbarin erfasste den Wohnungseingangsbereich der Betroffenen und weitere genutzte Flächen in Bild und Ton, wodurch personenbezogene Daten verarbeitet wurden. Die Nachbarin hat keine

Einwilligung der Betroffenen eingeholt. Die Verarbeitung kann auf Art 6 Abs 1 lit f DSGVO gestützt werden, wenn sie zur Wahrung berechtigter Interessen erforderlich ist und die Interessen oder Grundrechte der betroffenen Person nicht überwiegen. Der **Schutz des Eigentums** oder der **Gesundheit** kann ein berechtigtes Interesse sein. Die Erforderlichkeit der Datenverarbeitung muss sich aber auf das für die Zwecke der Verarbeitung absolut notwendige Maß beschränken.

Die Erfassung des Wohnungseingangsbereichs der Betroffenen sowie des gesamten Stiegen- und Liftbereichs war nicht erforderlich, um die allenfalls verfolgten Zwecke der Nachbarin zu erreichen. Die Kamera könnte so eingestellt werden, dass nur der unmittelbare Wohnungseingangsbereich der Nachbarin erfasst wird. Die von der Nachbarin angebrachte Kamera zeichnete nicht nur zeitlich beschränkte Momente auf, sondern filmte bereits vor Betätigen der Türklingel. Die Möglichkeit zur ortsungebundenen Betrachtung der Kameraübertragung und die Tonaufnahme stellen einen **intensiveren Eingriff** in die Rechte der Betroffenen dar. Die Verarbeitung war daher unverhältnismäßig und rechtswidrig.

to the point

# Datenschutzmonitor. 05/2025 vom 06.02.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen veröffentlicht:

- **Rechtsprechung des EuG**

EuG 29.01.2025, T-70/23, *DPC/EDSA* (DPC, EDSA, Kohärenzverfahren, verbindlicher Beschluss)

- **Rechtsprechung des VwGH**

VwGH 19.12.2024, Ro 2022/15/0018 (Steuern, Spende, erhebliches öffentliches Interesse)

VwGH 05.12.2024, Ro 2023/01/0008 (Zentrale Personenstandsregister, Geschlechtseintrag, Transidentität)

VwGH 20.12.2024, Ra 2024/04/0425 (öffentliche Daten)

VwGH 20.12.2024, Ra 2024/04/0427 (Säumnisbeschwerde)

VwGH 11.12.2024, Ra 2024/04/0423 (keine aufschiebende Wirkung)

- **Rechtsprechung der Justiz**

OLG Linz 10.01.2025, 8Bs249/24k (Europäische Ermittlungsanordnung, Vollstreckungshindernis)

OLG Linz 15.01.2025, 2R174/24g; 15.01.2025, 2R172/24p (Vollmacht, Auskunft, Anerkenntnis, Kosten)

OLG Linz 23.01.2025, 1R4/25a (Vollmacht, Auskunft)

- **Rechtsprechung des BVwG**

BVwG 02.09.2024, W256 2251016-1 (Auskunft, Datenübertragung, neuer Verantwortlicher)

BVwG 18.12.2024, W252 2294338-1 (Rollenverteilung, Anwendungsbereich, Videoüberwachung)

BVwG 18.12.2024, W256 2285492-1 (Videoüberwachung, Arbeitsplatz, Anweisung, Geldbuße)

- **Rechtsprechung der DSB**

DSB 12.12.2024, 2024-0.796.258 (Aktfotos, Geldbuße)

- **Nationale Rechtsakte**

Gesundheitstelematik-Anpassungsverordnung 2025

## To the Point:

### Rechtsprechung des EuG

EuG 29.01.2025, T-70/23, DPC/EDSA

#### **DPC, EDSA, Kohärenzverfahren, verbindlicher Beschluss**

- Die **Data Protection Commission ("DPC")** erhob Klage gegen den **Europäischen Datenschutzausschuss ("EDSA")**. Die Klage richtete sich gegen **verbindliche Beschlüsse** des EDSA (3/2022, 4/2022 und 5/2022), mit welchen die DPC verpflichtet wurde, neue Untersuchungen zu Datenverarbeitungstätigkeiten der Meta-Dienste Facebook, Instagram und WhatsApp durchzuführen und ergänzende Beschlusssentwürfe zu erstellen. Die DPC beantragte, diese verbindlichen Beschlüsse teilweise für nichtig zu erklären. Das EuG wies die Klagen ab und bestätigte die Kompetenz des EDSA, entsprechende Beschlüsse zu erlassen.

Das EuG hat erwogen: Nach ständiger Rechtsprechung sind bei der Auslegung einer Unionsrechtsvorschrift nicht nur ihr Wortlaut, sondern auch ihr Zusammenhang und ihre Ziele zu berücksichtigen. Der EDSA kann gemäß Art 65 Abs 1 lit a DSGVO **verbindliche Beschlüsse** erlassen, wenn eine andere Aufsichtsbehörde einen maßgeblichen und begründeten Einspruch gegen einen **Beschlusssentwurf** der **federführenden Aufsichtsbehörde** einlegt. Dies schließt auch die Anweisung ein, eine fehlende Analyse nachzuholen und die Untersuchung zu vertiefen oder auszuweiten, wenn dies erforderlich ist.

Der Wortlaut des Art 65 Abs 1 lit a DSGVO unterstützt diese Auslegung. Die Zusammenarbeit zwischen den betroffenen Aufsichtsbehörden und die **Kohärenzkontrolle** durch den EDSA wird nicht beeinträchtigt, wenn der EDSA Weisungen zur Ausweitung der Untersuchung erteilt. Der Unionsgesetzgeber hat entschieden, dass anhaltende Meinungsverschiedenheiten zwischen den betroffenen Aufsichtsbehörden im Rahmen des **Kohärenzverfahrens** innerhalb des EDSA geschlichtet werden sollen. Eine nationale gerichtliche Kontrolle ist nicht geeigneter, um Einwände im Zusammenhang mit der Untersuchung zu prüfen.

### Rechtsprechung des VwGH

VwGH 19.12.2024, Ro 2022/15/0018

#### **Steuern, Spende, erhebliches öffentliches Interesse**

- Ein Arbeitnehmer machte in seiner **Arbeitnehmerveranlagung** eine **Spende** an einen gemeinnützigen Verein als **Sonderausgaben** geltend. Das Finanzamt berücksichtigte diese Sonderausgaben nicht, weil der Arbeitnehmer dem Zuwendungsempfänger

seinen Namen und sein Geburtsdatum nicht bekannt gab. Gegen den ablehnenden Bescheid des Finanzamts erhob der Arbeitnehmer Bescheidbeschwerde an das BFG. Die Bestimmung des § 18 Abs 8 Z 1 EStG 1988 sei aufgrund des Vorranges der DSGVO nicht anwendbar und verfassungswidrig. Seine Geldspende sei als Sonderausgabe zu berücksichtigen.

Das BFG wies die Bescheidbeschwerde ab, weil der Datenaustausch mit einem **verschlüsselten bereichsspezifischen Personenkennzeichen** für Steuern und Abgaben ("**vbPK SA**") erfolge und zulässig sei. Die Behandlung der **Erkenntnisbeschwerde** des Arbeitnehmers lehnte der **VfGH** ab. Der VwGH wies die Revision ab.

Der VwGH hat erwogen: Durch Art 9 Abs 2 lit g DSGVO kann eine Datenverarbeitung gerechtfertigt sein, wenn sie aus Gründen eines **erheblichen öffentlichen Interesses** erforderlich ist. Im Unterschied zu Art 6 Abs 1 lit e DSGVO, welcher nur ein öffentliches Interesse voraussetzt, braucht es bei der Rechtfertigung einer Datenverarbeitung nach Art 9 Abs 2 lit g DSGVO ein erhebliches öffentliches Interesse. Dieses setzt eine spezifische Abwägung und eine besondere Legitimation für die Verwendung solcher Daten voraus. Nicht nur die Erhebung von Steuern und Abgaben, sondern auch die Ermittlung der korrekten Steuerbemessungsgrundlagen ist ein **erhebliches öffentliches Interesse**.

Durch einen Datenaustausch mit Hilfe des "vbPK SA" ist für das Finanzamt eine Zuordnung zu einer Person ohne Verknüpfung mit anderen Daten möglich. Der Zweck des § 18 Abs 8 EStG 1988 ist dem Finanzamt die **Erfüllung seiner gesetzlichen Aufgabe** zu ermöglichen, die ua darin besteht, in Massenverfahren Manipulationsmöglichkeiten zu verhindern und eine Gleichmäßigkeit der Besteuerung sicherzustellen.

Das "**vbPK SA**" ist für die Zuordnung und Ermittlung der als Sonderausgaben zu berücksichtigenden Zuwendungen zu einem bestimmten Steuerpflichtigen erforderlich.

Verarbeitet werden nur jene Zuwendungen, die ein Steuerpflichtiger als Sonderausgaben in Abzug bringen will. Auch vor Einführung des § 18 Abs 8 EStG 1988 mussten Steuerpflichtige alle Zuwendungen lückenlos nachweisen. Die Erhebung erfolgt im konkreten Anlass und **nicht auf "Vorrat"**.

Aus der weiteren Rechtsprechung des VwGH:

- Die vollständige und richtige Eintragung von **Personenstandsdaten** in das **Zentrale Personenstandsregister ("ZPR")** ist von **erheblichem öffentlichem Interesse**. Gemäß § 2 Abs 1 iVm Abs 2 gehört das **Geschlecht** einer Person zu den allgemeinen Personenstandsdaten, die gemäß § 11 Abs 1

PStG verpflichtend von der Personenstandsbehörde einzutragen sind. Eine ersatzlose Streichung des Eintrags des Geschlechts aus dem ZPR ist unzulässig. § 41 Abs 1 PStG ermöglicht nur die Änderung des Geschlechtseintrags, nicht dessen Streichung. Der VfGH hat in seiner Entscheidung vom 15.06.2018, G 77/2018, festgestellt, dass das Geschlecht ein maßgebliches Personenstandsdatum ist. Der VfGH hat jedoch zwischen Intersexualität und **Transidentität** unterschieden, wobei lediglich für intersexuelle Personen alternative Einträge wie "divers", "inter" oder "offen" möglich sind. Diese Regelung gilt nicht für **transsexuelle Personen** ([VwGH 05.12.2024, Ro 2023/01/0008](#)).

- Wird durch die **Verknüpfung** personenbezogener Daten (Name und Adresse) mit einer **veröffentlichten Stellungnahme** die Urheberschaft der Stellungnahme offengelegt, entsteht in datenschutzrechtlicher Hinsicht ein **informationeller Mehrwert** ([VwGH 20.12.2024, Ra 2024/04/0425](#)).
- Gegen ein Erkenntnis des BVwG, mit dem ein **Säumnisbeschwerdeverfahren** eingestellt wurde, ist eine Revision, die Vorbringen nur zur Hauptsache enthält, unzulässig ([VwGH 20.12.2024, Ra 2024/04/0427](#)).
- Einer Revision gegen ein Erkenntnis des BVwG, mit dem eine Verletzung im Recht auf Geheimhaltung festgestellt wurde, kommt **keine aufschiebende Wirkung** zu ([VwGH 11.12.2024, Ra 2024/04/0423](#)). **Mit Beschluss vom 04.03.2024, Ra 2024/04/0010, erkannte der VwGH die aufschiebende Wirkung der Revision in einem Geheimhaltungsverfahren noch zu. Von dieser Rechtsprechung ist der VwGH nun wieder abgegangen. Begründend führt der VwGH aus, dass es darauf ankäme, ob die DSB der Zuerkennung entgegenstehende zwingende öffentliche Interessen einwendet. Allerdings hat die DSB keine solchen Interessen eingewendet.**

## **Rechtsprechung der Justiz**

Aus der Rechtsprechung der Justiz:

- Mit § 55d Abs 7 EU-JZG wird Art 31 der RL 2014/41/EU über die **Europäische Ermittlungsanordnung** in Strafsachen umgesetzt. Die Staatsanwaltschaft wird verpflichtet, bei Unterrichtung durch ausländische Behörden über eine Telekommunikationsüberwachung in Österreich das Vorliegen von Vollstreckungshindernissen nach § 55a Abs 1 EU-JZG zu prüfen. Bei deren Vorliegen hat die Staatsanwaltschaft der ausländischen Strafverfolgungsbehörde mitzuteilen, dass die Überwachung nicht durchgeführt werden kann und bereits gesammelte Ergebnisse nicht verwendet werden dürfen. § 55a Abs 1 Z 13 EU-JZG normiert ein

Vollstreckungshindernis, wenn die Überwachung in einem vergleichbaren innerstaatlichen Fall nicht genehmigt würde. Wurden die Daten durch die **Sicherstellung eines ausländischen (französischen) Servers** und nicht durch eine Telekommunikationsüberwachung gewonnen, liegt **kein Vollstreckungshindernis** vor ([OLG Linz 10.01.2025, 8Bs249/24k](#)).

- Wurde eine Vollmachtsurkunde entgegen der Anmerkung "handschriftlich" elektronisch unterzeichnet und weicht diese Unterschrift maßgeblich von jener auf dem Ausweis des Klägers ab, sind **Zweifel** an der Vollmachterteilung iSd Art 12 Abs 6 DSGVO **begründet**. Durch Verweigerung der Auskunftserteilung wird daher keine Veranlassung zur Klagsführung gegeben, sodass die **Kostenersatzpflicht nach § 45 ZPO** greift. Erst gegenüber dem Gericht kann sich ein **Rechtsanwalt** gemäß § 8 RAO auf die ihm erteilte Vollmacht berufen. **Anerkennt** daraufhin der beklagte Verantwortliche den Auskunftsanspruch, hat der klagende Betroffene die Prozesskosten zu tragen (OLG Linz [15.01.2025, 2R174/24q](#); [15.01.2025, 2R172/24p](#)).
- Gibt es **keinen Grund**, an der **Vollmachtserteilung** zu zweifeln, darf die **Auskunft** nicht verweigert werden. Verlangt der Verantwortliche dennoch einen speziellen Nachweis der Vollmacht, veranlasst er damit die Klagsführung und hat die Kosten zu tragen ([OLG Linz 23.01.2025, 1R4/25a](#)).

## **Rechtsprechung des BVwG**

[BVwG 02.09.2024, W256 2251016-1](#)

### **Auskunft, Datenübertragung, neuer Verantwortlicher**

- Ein Kunde beehrte Auskunft und Datenübertragung bei einem Finanzdienstleistungsunternehmen. Dieses stellte ihm seine personenbezogenen Daten sowie Informationen über abgeschlossene Verträge und Anträge in Form eines Excel-Dokuments bereit. Zudem standen ihm diese Daten im Kundenpostfach zur Verfügung. Der Kunde erhob Datenschutzbeschwerde bei der DSB, weil die Auskunft unvollständig und verspätet erteilt worden sei, die Datenübertragung verweigert worden sei und die Übertragung sensibler Kundendaten unverschlüsselt erfolgt sei. Die DSB wies die Datenschutzbeschwerde ab. Daraufhin erhob der Kunde Bescheidbeschwerde an das BVwG, das diese wegen der behaupteten Verletzung im Recht auf Auskunft abwies. Hinsichtlich des Rechts auf Datenübertragbarkeit gab das BVwG der Bescheidbeschwerde statt.

Das BVwG hat erwogen: Das Finanzdienstleistungsunternehmen hat dem Kunden sämtliche verarbeiteten Unterlagen übermittelt bzw. standen diese dem Kunden im

Postfach zur Verfügung. Eine Verletzung des Rechts auf Auskunft ist **gemäß § 24 Abs 6 DSGVO sanierbar**, der DSB kann daher nicht entgegengesetzt werden, wenn sie eine (ursprüngliche) Unvollständigkeit der Auskunft in dem vom Kunden aufgezeigten Umfang nicht angenommen hat.

Das **Recht auf Datenübertragbarkeit** setzt voraus, dass (i) die begehrten Daten vom Betroffenen bereitgestellt sein müssen, (ii) die Verarbeitung auf einer Einwilligung oder einem Vertrag beruhen muss und (iii) die Verarbeitung mithilfe automatisierter Verfahren erfolgt. Der Zweck des Rechts auf Datenübertragung besteht nicht in der Information des Betroffenen über die Datenverarbeitung, sondern in der Ermöglichung bzw Erleichterung des Anbieterwechsels. Da der Kunde eine Datenübertragung nicht an seine Person, sondern direkt an den **neuen Verantwortlichen** beantragt hat und ihm eine solche Form der Datenübertragung nach **Art 20 Abs 2 DSGVO** auch ausdrücklich zusteht, hätte das Finanzdienstleistungsunternehmen darauf zu reagieren gehabt.

BVwG 18.12.2024, W252 2294338-1

#### **Rollenverteilung, Anwendungsbereich, Videoüberwachung**

- Eine Stadt betrieb eine Videoüberwachungskamera im Stadtgebiet und fasste konkrete Pläne für die Installation weiterer Kameras zur Stärkung des subjektiven Sicherheitsgefühls, des Schutzes von Eigentum und der Dokumentation straf- oder zivilrechtlich relevanter Delikte. Die Aufnahmen der bereits installierten Kamera konnten nur von der Stadtpolizei eingesehen werden. Die DSB leitete ein amtswegiges Prüfverfahren ein und untersagte die Datenverarbeitung der installierten Überwachungskamera. Daneben sprach sie eine Warnung aus, dass die geplante Installation weiterer Kameras voraussichtlich gegen die DSGVO verstoßen werde. Dagegen richtete sich die (erfolglose) Beschwerde an das BVwG.

Das BVwG hat erwogen: Die Stadt ist **Verantwortliche**, weil ihre Organe Zweck und Mittel der Videoüberwachung bestimmt haben. Da die Stadtpolizei keine tragende Rolle bei der Festlegung von Zweck und Mittel spielte, hatte deren Erwähnung in der Datenschut-Folgenabschätzung keinen Einfluss auf die Qualifikation der Stadt als Verantwortliche.

Die DSGVO findet gemäß Art 2 Abs 2 lit d DSGVO **keine Anwendung** auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der **Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten** oder der **Strafvollstreckung**, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Da die

Stadtpolizei der Bezirkshauptmannschaft (BH) nur unterstellt ist, ist diese selbst keine Sicherheitsbehörde. Deren Eigenschaft als **Gemeindevachkörper** ändert daran nichts. Die DSGVO ist daher **anwendbar**.

Hinsichtlich der **Stärkung des subjektiven Sicherheitsgefühls**, der Dokumentation von straf- oder zivilrechtlich relevanten Delikten und eines allgemeinen vorbeugenden Schutzes von Personen oder Sachen ist die **Stadt als Behörde** zu qualifizieren, sodass sich diese nicht auf die Wahrung berechtigter Interessen berufen kann. Denkbar wäre ein rein auf den Schutz des Eigentums der Stadt beschränktes Handeln im Rahmen der **Privatwirtschaftsverwaltung**. Der Schutz des Eigentums ist grundsätzlich ein berechtigtes Interesse. Allerdings stehen hinsichtlich der Beschädigung öffentlicher Sitzgelegenheiten oder Straßenbeleuchtungen gelindere Alternativen zur Verfügung (zB Anti-Graffiti-Beschichtungen, häufigere Kontrollen durch die Stadtpolizei, Einfriedungen, etc).

Die DSB hat die Aufgabe, die Anwendung der DSGVO zu überwachen und durchzusetzen. Ein Verbot der Videoüberwachung ist für das Erreichen dieser Ziele geeignet, erforderlich und verhältnismäßig. Auch die Warnung wegen der geplanten Kameras ist gerechtfertigt, weil bei deren Inbetriebnahme ein Verstoß gegen die DSGVO zu erwarten ist.

BVwG 18.12.2024, W256 2285492-1

#### **Videoüberwachung, Arbeitsplatz, Anweisung, Geldbuße**

- Die DSB führte aufgrund einer anonymen Eingabe ein amtswegiges Prüfverfahren gegen einen Arbeitgeber wegen des Verdachts auf unrechtmäßige Datenverarbeitung durch eine Videoüberwachungsanlage. Ua wurden Arbeitsgroßraum, Küche, Besprechungszimmer und Flur, inkl den Eingängen zu den Toiletten, überwacht. Der Arbeitgeber rechtfertigte die Datenverarbeitung ua mit dem Schutz vor Diebstahl, Einbruch, körperlicher und emotionaler Gewalt und Vandalismus. Die Kameras seien auch freiliegend, sichtbar und per Klebeschild bei der Eingangstüre, welches ein Piktogramm und die Herstellerbezeichnung zeigte, gekennzeichnet. Die Kameras seien auf Wunsch der Mitarbeiter installiert worden, die über die Überwachung informiert wurden.

Daraufhin leitete die DSB ein Verwaltungsstrafverfahren ein und verhängte eine Geldstrafe iHv EUR 59.400 (zzgl EUR 5.940 an Verfahrenskosten) wegen der fehlenden Rechtsgrundlage gemäß Art 6 Abs 1 DSGVO (Spruchpunkt I), dem Nichterfüllen der Informationspflichten gemäß Art 13 DSGVO (Spruchpunkt II) und dem Nichtbefolgen einer Anweisung der Behörde (Spruchpunkt III). Der Arbeitgeber bekämpfte das



Straferkenntnis beim BVwG und brachte zusammengefasst vor, man habe stets kooperiert und den abschließenden Bescheid der DSB aus dem Prüfverfahren nicht bekämpft. Das BVwG gab der Bescheidbeschwerde hinsichtlich Spruchpunkt III statt und setzte die Geldstrafe auf EUR 11.000 (zzgl EUR 1.100 Verwaltungskosten) herab.

Das BVwG hat erwogen: Eine Verarbeitung gemäß Art 6 Abs 1 lit f DSGVO kann gerechtfertigt sein, wenn sie zur Wahrung berechtigter Interessen erforderlich ist und die Interessen oder Grundrechte der Betroffenen nicht überwiegen. Die Erforderlichkeit ist dabei eng mit dem Grundsatz der **Datenminimierung** verbunden. Die **Videoüberwachung** des Arbeitsgroßraums, der Küche, der Besprechungszimmer und des Flurs war für den Zweck des Eigentumsschutzes nicht erforderlich. Im Straferkenntnis muss die DSB die Zahl der konkret Betroffenen einer Datenverarbeitung nicht beziffern, es genügt die unrechtmäßige Datenverarbeitung an sich.

Klebeschilder, die lediglich eine bildliche Darstellung und die Herstellerbezeichnung von Kameras zeigen und keine weiteren **Informationen** zur Datenverarbeitung enthalten, entsprechen nicht den zu erteilenden Informationen gemäß Art 13 Abs 1 und 2 DSGVO. Allein aus der Tatsache, dass Kameras in einem Gebäude installiert sind, in dem ein Verantwortlicher seine Geschäftstätigkeit ausübt, kann ohne zusätzliche Informationen nicht auf die **datenschutzrechtliche Verantwortlichkeit** des Verantwortlichen geschlossen werden.

Der Auftrag in einem Bescheid, binnen zwei Wochen Nachweise über die Änderung einer Datenverarbeitung zu übermitteln, ist **keine Anweisung** nach Art 58 Abs 2 DSGVO und kein Begehren auf Zugang zu Information nach Art 58 Abs 1 lit e DSGVO und berechtigt beim Nichterfüllen nicht zum Verhängen einer Geldbuße

**Bilddaten**, die ausschließlich zum Eigentumsschutz angefertigt werden, sind nicht ohne weiteres sensible Daten nach Art 9 DSGVO. Wenn durch Kameras auch regelmäßig Mitarbeiter gefilmt werden, rechtfertigt dies noch nicht die Annahme einer **Mitarbeiterüberwachung**, wenn dies nicht Zweck der Überwachung ist. **Geldbußen** müssen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Aufgrund der mittleren Schwere des Verstoßes kommt eine bloße Abmahnung ohne Ausspruch einer Strafe nicht in Betracht.

## **Rechtsprechung der DSB**

DSB 12.12.2024, 2024-0.796.258

### **Aktfotos, Geldbuße**

- Ein Kameramann fertigte Aktfotos von einer Frau mit ihrer Einwilligung und ihrem eigenen Mobiltelefon an. In Folge leitete er die Aktfotos ohne ihre Zustimmung über einen Internetdienst von ihrem Mobiltelefon auf sein eigenes Mobiltelefon weiter. Die Frau forderte den Kameramann auf, die Fotos zu löschen, was dieser auch tat. Die Frau zeigte den Kameramann dennoch an und die DSB leitete ein Verwaltungsstrafverfahren ein. Der Kameramann äußerte sich trotz Aufforderung der DSB nicht zur Sache. Die DSB verhängte eine Geldstrafe iHv EUR 2.000.

Die DSB hat erwogen: Die erfassten Bilddaten sind personenbezogene Daten. Die Lichtbilder spiegeln intime Aufnahmen wider und erfassen **Daten zum Sexualleben** der Frau iSd Art 9 Abs 1 DSGVO.

Nach Art 9 Abs 1 DSGVO besteht grundsätzlich ein Verarbeitungsverbot für besondere Kategorien personenbezogener Daten. Die Verarbeitung besonderer Kategorien personenbezogener Daten ist erlaubt, wenn die Betroffene ausdrücklich einwilligt. Die Frau hat der Anfertigung der Lichtbilder zugestimmt, weshalb diese Verarbeitung zulässig war. Für die Übermittlung und Speicherung der Lichtbilder lag hingegen keine ausdrückliche Einwilligung vor. Die Übermittlung erfolgte ohne Wissen der Frau. Diese Datenverarbeitung war somit rechtswidrig.

### **Nationale Rechtsakte**

- Am **28.01.2025** wurde die "*Verordnung des Bundesministers für Soziales, Gesundheit, Pflege und Konsumentenschutz, mit der die Gesundheitstelematikverordnung 2013 und die ELGA-Verordnung 2015 geändert und die ELGA- und eHealth-Supporteinrichtungsverordnung sowie die eHealth-Verordnung 2025 neu erlassen wird (Gesundheitstelematik-Anpassungsverordnung 2025)*", [BGBl II 2025/11](#), kundgemacht. Mit dieser Verordnung wird neben der **Gesundheitstelematikverordnung 2013** auch die **ELGA-Verordnung 2015** novelliert und werden die **eHealth-Supporteinrichtungsverordnung** sowie die **eHealth-Verordnung 2025** neu erlassen. Die Verordnungen enthalten neue Regelungen zur Verarbeitung von **Gesundheitsdaten** und **genetischen Daten** durch **Gesundheitsdiensteanbieter**.

to the point

# Datenschutzmonitor. 06/2025 vom 12.02.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 04.02.2025, 33421/16, *Klimova ua /Russland* (Vorratsdatenspeicherung, Aktivistin, Meinungsfreiheit)

EGMR 04.02.2025, 8825/22, *Bazhenov ua /Russland* (Positive Pflicht, sexuelle Orientierung, soziales Netzwerk)

- **Rechtsprechung des EuGH**

EuGH SA 06.02.2025, C-413/23 P, *EDSB/SRB* (Personenbezug, Pseudonymisierung, Informationspflicht)

EuGH SA 06.02.2025, C-492/23, *Russmedia Digital* (Online-Marktplatz, Hosting, Rollenverteilung)

- **Rechtsprechung der Justiz**

OGH 17.01.2025, 6ObA2/23x (Betriebsrat, E-Mail-Herausgabe)

OLG Linz 27.01.2025, 11R1/25h (Identitätsnachweis, elektronische Signatur)

- **Rechtsprechung des BVwG**

BVwG 27.11.2024, W252 2280461-1 (Anwendungsbereich, StVO, Verwaltungsstrafverfahren, Straftat)

BVwG 10.01.2025, W108 2290157-1 (WEG, mündliche Mitteilung, gesetzliche Pflicht)

BVwG 09.01.2025, W256 2244544-1 (Auskunftsrecht, Dokumentenkopie, Antragsinhalt)

BVwG 09.01.2025, W211 2283857-1 (Video, Servitut, Ausdehnung der Datenschutzbeschwerde)

BVwG 07.01.2025, W108 2286042-1 (Prüfbescheinigung, Offizialmaxime)

BVwG 07.01.2025, W108 2284293-1 (Erlaubnistatbestände, Parteiengehör, Art 29 DSGVO)

BVwG 14.01.2025, W298 2263736-1 (Exzess, Missbrauchsabsicht, Zurückverweisung)

BVwG 14.01.2025, W298 2300879-1 (Beschwerdegegner, Passivlegitimation)

BVwG 14.01.2025, W298 2262670-1; 13.01.2025, W108 2285445-1 (Massenverfahren, Aussetzung)

- **EU-Rechtsakte**

Commission Guidelines on prohibited AI practices

Commission Guidelines on the definition of an AI system established

## To the Point:

### Rechtsprechung des EGMR

EGMR 04.02.2025, 33421/16, Klimova/Russland

#### **Vorratsdatenspeicherung, Aktivistin, Meinungsfreiheit**

- **Kommunikationsdienste** haben in Russland **Metadaten** über Internetkommunikationen für **ein Jahr** und **Inhaltsdaten** der Internetkommunikationen für **sechs Monate** aufzubewahren (= **Vorratsdatenspeicherung**). Diese Daten sind auf Anfrage von Polizei oder Sicherheitsdiensten vom Kommunikationsdienstleister herauszugeben. Eine gerichtliche Genehmigung ist dafür nicht zwingend erforderlich.

Eine Aktivistin administrierte eine öffentliche Community auf dem russischen sozialen Netzwerk VKontakte (**VK**), die sich für die Rechte von LGBTQI+ Personen einsetzte. Der russische Geheimdienst (Federal Security Service; **FSB**) erwirkte die Herausgabe von Nutzerdaten der Administratorin einschließlich weitreichender Informationen über den Inhalt und weiterer Teilnehmer der Community. Über die durch diese Herausgabe persönlich identifizierte Aktivistin wurden in der Folge wegen Förderung von Homosexualität bei Minderjährigen zwei Verwaltungsstrafen verhängt. Diese Strafen wurden im Rechtsmittelverfahren aufrechterhalten.

Der EGMR stellte einstimmig eine Verletzung der durch **Art 8** (Recht auf Achtung des Privat- und Familienlebens) und **Art 10 EMRK (Freiheit der Meinungsäußerung)** gewährleisteten Rechte fest und sprach der Aktivistin EUR 9.800 immateriellen Schadenersatz zu.

Der EGMR hat erwogen: Der EGMR ist zuständig, weil sich der Sachverhalt vor dem Austritt Russlands aus der EMRK mit 16.09.2022 ereignete.

Die vom FSB gesammelten Daten (Benutzerdaten, Informationen über die von der Aktivistin errichteten und moderierten Gruppen und deren Inhalt) fallen in den Bereich des durch Art 8 EMRK geschützten Privatlebens.

Eingriffe in das geschützte Privatleben müssen auf gesetzlichen Bestimmungen basieren, ein legitimes Ziel verfolgen und in einer demokratischen Gesellschaft notwendig sein. Das innerstaatliche Recht muss einen geeigneten Schutz dieser Daten vorsehen, vor allem, wenn Daten für polizeiliche Zwecke verwendet werden.

Das russische Informationsgesetz sieht zwar eine **gesetzliche Grundlage** zur Erhebung von Daten vor, enthält jedoch keine geeigneten Schutzgarantien. Der Schutz vor Missbrauch ist bei Plattformen sozialer Netzwerke besonders gering, weil Behörden

keine gerichtliche Genehmigung für den Zugriff auf personenbezogene Daten benötigen. Der Aktivistin stand zudem **kein wirksamer Rechtsbehelf** zur Verfügung, um die Übermittlung personenbezogener Daten an die FSB anzufechten. Denn im Rahmen des möglichen gerichtlichen Überprüfungsverfahrens sind Gerichte nicht verpflichtet, die Notwendigkeit und Angemessenheit des Zugriffs auf personenbezogene Daten im erforderlichen Ausmaß zu überprüfen. Die Erhebung der Nutzerdaten beruhte somit auf gesetzlichen Bestimmungen, die keine ausreichenden Garantien gegen Missbrauch boten.

Das **Verbot der Förderung von Homosexualität** dient darüber hinaus **nicht dem legitimen Ziel** des Schutzes der Sittlichkeit und Gesundheit. Bei der Prüfung, ob der Eingriff in das Recht auf Achtung der Privatsphäre "*in einer demokratischen Gesellschaft notwendig war*", ist die Art und Schwere der Straftat zu berücksichtigen. Der Straftatbestand der Förderung der Homosexualität ist nach dem innerstaatlichen Recht eine Verwaltungsübertretung, die auch keinen tatsächlichen (in ihrem Sinn) nachteiligen Erfolg verlangt. Die Erhebung großer Mengen personenbezogener Daten kann außerdem eine abschreckende Wirkung im Hinblick auf das Recht auf freie Meinungsäußerung haben. Unter diesen Umständen erscheint die Erhebung von sensiblen Daten zur Identifizierung der Aktivistin in einer demokratischen Gesellschaft nicht notwendig.

EGMR 04.02.2025, 8825/22 ua, Bazhenov ua/Russland

#### **Positive Pflicht, sexuelle Orientierung, soziales Netzwerk**

- Die personenbezogenen Daten, darunter die sexuelle Orientierung, von zwei Geschäftsleuten und einem Rechtsanwalt, die jeweils in gleichgeschlechtlichen Ehen in Europa bzw. in den USA lebten, wurden 2020 auf dem russischen sozialen Netzwerk VKontakte (**VK**) mit klar homophober Intention in homophoben Gruppen und auf privaten Kanälen veröffentlicht. Die Geschäftsleute und der Rechtsanwalt riefen die jeweils zuständigen Staatsanwaltschaften an. In Russland waren zwar entsprechende strafgesetzliche Bestimmungen vorhanden, die Staatsanwaltschaften blieben jedoch zunächst untätig. Mit reichlicher Verspätung forderte die Staatsanwaltschaft VK auf, die Identitätsdaten des Nutzers herauszugeben, der sich hinter dem verdächtigen Profil verbarg. Anschließend wurde das Verfahren jedoch ohne Rückmeldung von VK geschlossen. Die Geschäftsleute und der Rechtsanwalt riefen den EGMR an, der einen Verstoß gegen **Art 14 EMRK (Verbot der Benachteiligung)** iVm **Art 8 EMRK** (Recht auf Achtung des Privat- und Familienlebens) feststellte.

Der EGMR hat erwogen: Die vorgeworfene Tat ereignete sich vor dem 16.09.2022, als Russland aus der EMRK austrat. Der EGMR ist daher zuständig.

Das Offenlegen personenbezogener Daten auf homophoben öffentlichen und individuellen Kanälen hat die Geschäftsleute und den Rechtsanwalt einem erhöhten Risiko von Belästigung ausgesetzt und sie hatten Angst um ihr Leben. Das einwilligungslose Veröffentlichung der personenbezogenen Daten, einschließlich der sexuellen Orientierung, der Information über die gleichgeschlechtliche Ehe sowie von Fotos der Betroffenen, greift in deren Recht auf Privat- und Familienleben ein.

Der Staat hat eine **positive Pflicht**, das Recht auf Achtung des Privat- und Familienlebens ohne Diskriminierung zu schützen. **Sexuelle Minderheiten** sind **besonders schutzbedürftig**. Das innerstaatliche Recht enthielt zwar einen strafgerichtlichen Rechtsbehelf gegen das rechtswidrige Verbreiten von Informationen über das Privatleben einer Person, der Staat ist seiner positiven Pflicht jedoch nicht nachgekommen, weil er untätig blieb, bis die Verjährungsfristen abliefen.

Zwar stellte der Ermittler, bevor er das Verfahren betreffend die Geschäftsleute endgültig einstellte, eine Anfrage an VK, doch stellte er das Verfahren ein, ohne eine Antwort von VK erhalten zu haben. **Anm: Aus diesem Urteil kann geschlossen werden, dass es nach Ansicht des EGMR Sicherheitsbehörden geboten ist, zur Aufklärung von (bestimmten) Straftaten bei sozialen Netzwerken die Identitätsdaten der Nutzer dieser Netzwerke anzufragen. Allerdings gilt dies jedenfalls nicht, wie im zuvor besprochenen Fall Klimova/Russland gezeigt, wenn dies in einer demokratischen Gesellschaft nicht gerechtfertigt ist.**

## **Rechtsprechung des EuGH**

EuGH SA 06.02.2025, C-413/23 P, EDSB/SRB (EN)

### **Personenbezug, Pseudonymisierung, Informationspflicht**

- Im Rahmen des Abwicklungsverfahrens einer Bank veröffentlichte der **Einheitliche Abwicklungsausschuss (SRB)** – die für die Abwicklung insolvenzbedrohter Finanzinstitute zuständige Behörde der Europäischen Bankenunion – eine vorläufige Entscheidung über die Gewährung einer Entschädigung für betroffene Aktionäre oder Gläubiger. Er leitete ein Anhörungsverfahren ein, bei dem Betroffene eine Stellungnahme zur vorläufigen Entscheidung einreichen konnten. Die Stellungnahmen wurden vom SRB aggregiert, gefiltert und kategorisiert und dann an Deloitte zur Auswertung übermittelt. Die

Inhalte der Stellungnahmen waren von den Identifikationsdaten der Betroffenen getrennt und mit einem alphanumerischen Code gekennzeichnet, sodass nur der SRB die Daten verknüpfen konnte.

Fünf Bankkunden brachten Beschwerden beim EDSB ein, weil der SRB nicht darüber informiert hatte, dass ihre Daten an Deloitte weitergegeben werden. Der EDSB beschloss, dass die an Deloitte übermittelten Daten **pseudonymisierte Daten** waren und stellte einen Verstoß gegen die Informationspflicht fest.

Der SRB erhob Klage an das **EuG**. Dieses hob den Beschluss des EDSB auf, weil dieser Inhalt, Zweck oder Auswirkungen der an Deloitte übermittelten Informationen nicht geprüft habe. Mangels einer solchen Prüfung dürfe der EDSB nicht davon ausgehen, dass sich die an Deloitte übermittelten Informationen auf eine natürliche Person beziehen. Gegen diese Entscheidung richtet sich das Rechtsmittel des EDSB.

Der Generalanwalt hat erwogen: Eine Information bezieht sich auf eine bestimmte oder bestimmbare Person, wenn sie **aufgrund ihres Inhalts, ihres Zwecks oder ihrer Wirkung mit dieser verknüpft ist**. Bei Stellungnahmen ist zu unterscheiden, ob sie sich auf die bewertete Person beziehen, auf die im Text Bezug genommen wird, oder auf den Verfasser. Im zweiten Fall könnte man vermuten, dass sich eine Stellungnahme zwangsläufig auf ihren Verfasser bezieht. Auch mangels einer solchen Vermutung beziehen sich die Stellungnahmen aufgrund ihres Inhalts, Zwecks und ihrer Wirkung auf die Bankkunden, weil sie ihre Logik und Argumentation zeigten und somit ihre **subjektive Meinung** widerspiegeln. Die Stellungnahmen waren auch geeignet, sich auf die Interessen der Betroffenen in Bezug auf die finanzielle Entschädigung **auszuwirken**.

Die **Aggregation der Stellungnahmen** ändert nichts daran, dass es sich um personenbezogene Daten handelt, weil es andernfalls ausreichen würde, mehrere Standpunkte zusammenzufassen, um das Erfordernis zu umgehen, dass es sich um eine Information "über eine natürliche Person" zu handeln hat. Die fehlende Unterscheidbarkeit der Einzelmeinungen betrifft die Frage der Identifizierbarkeit, nicht jedoch die Verknüpfung mit einer natürlichen Person.

**Pseudonymisierung** ist eine Verarbeitung personenbezogener Daten, die die Möglichkeit offenlässt, dass Betroffene nicht identifizierbar sind. Während **anonymisierte Daten** nicht unter die DSGVO fallen, sind pseudonymisierte Daten nur insoweit ausgeschlossen, als Betroffene nicht identifiziert werden können. Daten können nur dann nicht als personenbezogene Daten eingestuft werden, wenn die Gefahr einer Identifizierung ausgeschlossen oder unbedeutend ist.

Es war daher zu prüfen, ob die Pseudonymisierung der Daten so robust war, dass die Bankkunden vernünftigerweise nicht identifizierbar waren. Falls Deloitte in der Lage gewesen wäre, die Bankkunden zu identifizieren, hätte es sich um personenbezogene Daten gehandelt.

Die **Informationspflicht** ist Teil des Rechtsverhältnisses zwischen den Betroffenen und dem Verantwortlichen. Sie entsteht zu dem Zeitpunkt, zu dem die Daten vom SRB erhoben werden und in Bezug auf die Informationen über den Empfänger spätestens dann, wenn dieser bekannt ist. Die Daten bleiben personenbezogen, unabhängig davon, ob sie gegenüber dem Empfänger pseudonymisiert wurden. Die Frage, ob die Pseudonymisierung ausreichend war, ist für die Informationspflicht nicht relevant, sodass Deloitte als **Empfänger** zu beauskunftet gewesen wäre.

EuGH SA 06.02.2025, C-492/23, Russmedia Digital

### **Online-Marktplatz, Hosting, Rollenverteilung**

- Auf dem Online-Marktplatz ("Publi24.ro"), die von der Gesellschaft Russmedia betrieben wird, wurde eine Annonce veröffentlicht, aus der hervorging, dass eine Person sexuelle Dienstleistungen anbiete. Diese Annonce enthielt Fotos und eine Telefonnummer, die aus den sozialen Netzwerken der Person stammten und ohne ihre Zustimmung verarbeitet wurden. Russmedia entfernte die Anzeige, doch wurde sie auf andere Websites kopiert. Die Person erhob Klage gegen Russmedia, woraufhin der EuGH angerufen wurde, um die Haftung des Betreibers eines Online-Marktplatzes zu klären.

Der Generalanwalt hat erwogen: Der Betreiber eines Online-Marktplatzes kann in den Genuss einer **Haftungsbefreiung** für den Inhalt der auf seinem Marktplatz veröffentlichten Anzeigen kommen, sofern seine Rolle neutral und rein technisch bleibt und er bei Kenntnis eines **rechtswidrigen Inhalts** diesen unverzüglich entfernt. Das gilt nicht, wenn aktiv in die Verwaltung der Inhalte, deren Änderung oder die Werbung für die Inhalte eingegriffen wird. Die Haftungsbefreiung ist auf Russmedia anwendbar, solange sie ihre Eigenschaft als neutraler **Hosting-Provider** nicht verliert, auch wenn in den allgemeinen Nutzungsbedingungen angeführt ist, sich das Recht vorzubehalten, die bereitgestellten Inhalte selbst zu nutzen, also auch zu kopieren, zu verbreiten, zu übermitteln etc.

Betreffend die datenschutzrechtliche **Rollenverteilung** ist anzunehmen, dass der Betreiber als **Auftragsverarbeiter** für den Inserierenden agiert. Er ist somit nicht verpflichtet, den Inhalt der veröffentlichten

Anzeigen zu überprüfen oder Sicherheitsmaßnahmen zu ergreifen, die geeignet sind, das Kopieren oder die Weiterverbreitung des Inhalts von Anzeigen zu verhindern. Er muss aber **geeignete organisatorische und technische Maßnahmen** treffen, um die Sicherheit der Verarbeitung gegenüber Dritten zu gewährleisten.

Hinsichtlich der personenbezogenen Daten der inserierenden Nutzer handelt der Betreiber als **Verantwortlicher**. In diesem Rahmen ist er verpflichtet, die Identität dieser inserierenden Nutzer zu überprüfen.

### **Rechtsprechung der Justiz**

#### Aus der Rechtsprechung der Justiz:

- Die Befugnisse des **Betriebsrats** bleiben durch das Datenschutzrecht unberührt. Das ArbVG wurde als **"spezifischere" Vorschrift** iSd **Öffnungsklausel** des Art 88 Abs 3 DSGVO bei der Europäischen Kommission **notifiziert**. Zwischen dem Betriebsverfassungs- und dem Datenschutzrecht besteht eine **"Sphärenharmonie"**. Im Bereich der **Pflichtkompetenzen** des Betriebsrats ist keine datenschutzrechtliche Interessenabwägung erforderlich, weil die Datenverarbeitung auf die Erfüllung **rechtlicher Verpflichtungen** gemäß Art 6 Abs 1 lit c und Art 9 Abs 2 lit b DSGVO gestützt werden kann. Außerhalb der **Pflichtbefugnisse** des Betriebsrats gelangen die Art 6 Abs 1 lit f und Art 9 Abs 2 lit b DSGVO als Erlaubnistatbestände zur Anwendung. Benötigt der Betriebsrat zur Kontaktaufnahme die **E-Mail-Adressen** der Arbeitnehmer, hat der Betriebsinhaber diese herauszugeben. Die **proaktive Kontaktaufnahme** gehört zwar nicht zu den Pflichtbefugnissen des Betriebsrats. Die Herausgabe kann aber auf das **berechtignte Interesse** des Betriebsrats gestützt werden, als Belegschaftsvertretung mit den Arbeitnehmern zu kommunizieren. Ein Recht des Betriebsrats auf Bekanntgabe **privater Telefonnummern** der Arbeitnehmer besteht hingegen nicht ([OGH 17.01.2025, 6ObA2/23x](#)).
- Ein elektronisches Auskunftersuchen muss nicht zwingend mit einer **qualifizierten elektronischen Signatur** versehen sein. Die DSGVO gibt keine konkrete Form des Identitätsnachweises vor. Ergibt sich hinsichtlich des **Identitätsnachweises** bereits ein hoher Grad an Verlässlichkeit, ist die Anforderung zusätzlicher Informationen unzulässig ([OLG Linz 27.01.2025, 11R1/25h](#)).

## Rechtsprechung des BVwG

BVwG 27.11.2024, W252 2280461-1

### **Anwendungsbereich, StVO, Verwaltungsstrafverfahren, Straftat**

- Mitarbeiter der Autobahnpolizeiinspektion fertigten auf einer Autobahn mit ihrer mobilen **Dienstkamera** ein Lichtbild eines Fahrzeugs an, weil dessen Halter gegen das Rechtsfahrgebot verstieß. Die Mitarbeiter brachten die straßenverkehrsrechtliche Verwaltungsübertretung bei der zuständigen Bezirkshauptmannschaft ("**BH**") zur Anzeige. Der Fahrzeughalter erachtete sich in seinem Geheimhaltungsrecht verletzt und erhob eine auch gegen die örtlich zuständige Landesregierung gerichtete Datenschutzbeschwerde an die DSB, welche diese abwies. Der Fahrzeughalter erhob (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die DSGVO findet ua keine Anwendung auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten. Ausnahmen vom Anwendungsbereich der DSGVO sind eng auszulegen. Der VwGH hat mit Beschluss vom 03.03.2022, Ra 2020/02/0241, Art 6 Abs 1 lit e iVm Abs 3 DSGVO in einem Verwaltungsstrafverfahren angewendet. Somit fallen nicht jegliche **Verwaltungsstrafen** unter den unionsrechtlichen Begriff der **Straftat**. Die DSGVO ist anzuwenden.

Die **Landesregierung** ist für die Handhabung der Verkehrspolizei auf Autobahnen zuständig. Sie kann hierfür Organe, die der Landespolizeidirektion angehören oder dieser zugeteilt sind und in Angelegenheiten des Straßenverkehrs besonders geschult sind, zur Handhabung der Verkehrspolizei ua auf Autobahnen einsetzen. Organe der Straßenaufsicht haben die Verkehrspolizei zu handhaben und bei der Vollziehung dieses Bundesgesetzes durch Maßnahmen, die für die Einleitung von Verwaltungsstrafverfahren erforderlich sind, mitzuwirken. Eine derartige Maßnahme, an der die Organe der Bundespolizei (hier jene der Autobahnpolizeiinspektion) mitzuwirken haben, kann ua die Anfertigung von Beweismaterial in Form von Lichtbildern sein. Dabei begründet die **Straßenverkehrssicherheit** eine Aufgabe im öffentlichen Interesse. Die Verarbeitung der vorliegenden Daten war für die Wahrnehmung der sich aus den Erfordernissen der StVO sowie aus dem **Verwaltungsstrafverfahren** ergebenden Aufgabe, die im **öffentlichen Interesse** liegt, erforderlich und daher rechtmäßig.

Auf den von der DSB angenommenen Erlaubnistatbestand des § 98e Abs 1 StVO konnte die Datenverarbeitung jedoch nicht gestützt werden. Wie sich aus den Gesetzesmaterialien ergibt, hatte der Gesetzgeber bei

der Schaffung des § 98e StVO "*die Überwachung aus Fahrzeugen (zB Zivilstreifen)*" vor Augen. Mangels planwidriger Rechtslücke war der von der DSB angestellte "teleologische Größenschluss" unzulässig.

BVwG 10.01.2025, W108 2290157-1

### **WEG, mündliche Mitteilung, gesetzliche Pflicht**

- Ein Wohnungseigentümer richtete mehrere E-Mails an seine Hausverwaltung, in denen er ua eine grobe Misswirtschaft und eine unzulässige Begünstigung eines Miteigentümers iZm mit einem geplanten Bauprojekt durch die Verwalterin kritisierte. Die Verwalterin verlas in einer Eigentümerversammlung in Abwesenheit des Wohnungseigentümers Auszüge dieser E-Mails und nahm deren Inhalt in das Sitzungsprotokoll auf. Dieses wurde anschließend an alle Wohnungseigentümer übermittelt. Der Wohnungseigentümer erachtete sich dadurch in seinem Recht auf Geheimhaltung verletzt.

Die DSB wies die Datenschutzbeschwerde ab und führte aus, dass die Offenlegung der E-Mails durch überwiegende berechtigte Interessen der Hausverwaltung und der Wohnungseigentümer gerechtfertigt war. Daraufhin erhob der Wohnungseigentümer (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Im Hinblick auf eine Verletzung des **Rechts auf Geheimhaltung** spielt es keine Rolle, auf **welche Weise Daten verarbeitet** werden. Auch eine **mündliche Mitteilung** kann eine **Verletzung** dieser Bestimmung **bewirken**.

Die **Vorwürfe** iZm den Pflichtverletzungen der Verwalterin **betrafen die gesamte Eigentümergemeinschaft**. Daher bestand jedenfalls ein **erhebliches Interesse der Hausverwaltung iSd § 1 Abs 2 DSG**, die vom Wohnungseigentümer übermittelten Informationen bzw erhobenen Vorwürfe den übrigen Miteigentümern zur Kenntnis zu bringen. Falls zutreffend, hätten sie zur Kündigung des Verwaltervertrags führen können bzw müssen und einen erheblichen finanziellen Schaden für die Eigentümergemeinschaft bedeutet.

Das Verschweigen der erhobenen Vorwürfe hätte jedenfalls einen **Verstoß gegen gesetzliche Pflichten gemäß § 20 Abs 1 WEG** sowie gegen **vertragliche Pflichten der Hausverwaltung** bedeutet.

Weiters war auch die **Bekanntgabe des Namens des Wohnungseigentümers gerechtfertigt**. Die übrigen Miteigentümer hatten ein Interesse, die **Vorwürfe zu überprüfen**, was nur mit Bekanntgabe des Urhebers möglich war. Nur so konnte eine Rücksprache oder ein **Austausch über Beweismittel** erfolgen.

Daher war die Datenverarbeitung jedenfalls auch für den geschilderten Zweck erheblich und notwendig, zumal lediglich der Name des Wohnungseigentümers offengelegt und seine Schreiben auch nur **auszugsweise verlesen bzw deren Inhalt paraphrasierend wiedergegeben** wurde. Damit ging auch ein **informationeller Mehrwert einher**.

BVwG 09.01.2025, W256 2244544-1

### **Auskunftsrecht, Dokumentenkopie, Antragsinhalt**

- Ein Landwirt stellte ein Auskunftersuchen an die Landwirtschaftskammer. Er forderte darin Auskunft über die zu seiner Person verarbeiteten Daten, die Zwecke der Verarbeitung und deren Empfänger. Zudem verlangte er die Übermittlung aller ihn betreffenden Unterlagen sowie allgemeine Unterlagen zum Bau einer Gasleitung und zur Angelegenheit Fischteiche. Die Landwirtschaftskammer beantwortete das Auskunftersuchen und übermittelte dem Landwirt 280 Seiten an Ausdrucken und Fotokopien, einschließlich allgemeiner Unterlagen. Der Landwirt erachtete die Auskunft für unvollständig und brachte bei der DSB eine Datenschutzbeschwerde ein. Die DSB wies die Datenschutzbeschwerde ab, weil die Landwirtschaftskammer eine vollständige Auskunft erteilt habe. Daraufhin erhob der Landwirt eine (erfolglose) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Art 15 Abs 1 DSGVO räumt Betroffenen das Recht auf Auskunft darüber ein, ob sie betreffende personenbezogene Daten verarbeitet werden und bejahendenfalls, um welche Daten es sich dabei konkret handelt. Die Mitteilung nach Art 15 Abs 1 DSGVO hat in präziser, transparenter, verständlicher und leicht zugänglicher Form zu erfolgen. Das Auskunftsrecht beschränkt sich auf personenbezogene Daten iSd Art 4 Abs 1 DSGVO. Im Einzelfall kann es erforderlich oder zweckmäßig sein, dass auch einzelne Textpassagen oder Dokumente zur Verfügung gestellt werden. Ein generelles **Recht auf Erhalt von Dokumenten** kann aus Art 15 DSGVO jedoch **nicht abgeleitet werden**. Dieses Recht besteht nur, wenn die Zurverfügungstellung unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch die DSGVO verliehenen Rechte zu ermöglichen. Die DSB und das BVwG können nur darüber absprechen, **was überhaupt beantragt wurde**, dh sie sind an den Inhalt des Antrags des jeweiligen Antragstellers gebunden. Das BVwG darf nicht jegliche möglichen Rechtsverletzungen prüfen. Die Landwirtschaftskammer hat dem Beschwerdeführer eine umfassende Auskunft erteilt. Sie hat ihm die zu seiner Person verarbeiteten

Daten, deren Herkunft und Empfänger mitgeteilt. Zudem hat sie ihm auch die ihn betreffenden Unterlagen zur Verfügung gestellt, weshalb keine Mangelhaftigkeit der Auskunft erkennbar ist. Der Landwirt hat keinen Anspruch auf allgemeine Unterlagen, die nicht seine Person betreffen.

BVwG 09.01.2025, W211 2283857-1

### **Video, Servitut, Ausdehnung der Datenschutzbeschwerde**

- Ein Ehemann installierte im Eingangsbereich seines Hauses eine Videokamera, die auch einen Teil eines über das Grundstück führenden Weges erfasste. An diesem Weg besteht eine Servitut zugunsten eines Servitutsberechtigten. Der Servitutsberechtigte brachte eine Datenschutzbeschwerde gegen die Ehefrau als Grundeigentümerin ein, die er im weiteren Verfahren auch gegen deren Ehemann ausdehnte. Die DSB bestätigte die Verletzung im Recht auf Geheimhaltung und forderte den Ehemann auf, den Aufnahmebereich der Kamera einzuschränken. Das BVwG gab der Bescheidbeschwerde des Ehemanns statt und änderte den Bescheid der DSB dahingehend ab, dass die Datenschutzbeschwerde abgewiesen wird.

Das BVwG hat erwogen: Die **Ausdehnung der Datenschutzbeschwerde** auf den Ehemann war zulässig. Sie änderte nicht das Wesen der Sache dieser Datenschutzbeschwerde, weil sie weder deren Rechtsqualität noch die anzuwendenden Materiegesetze oder die Behördenzuständigkeit veränderte.

Da die pflegebedürftige Grundeigentümerin und ihr ebenfalls betagter Ehemann alleine und abgeschieden am Dorfrand lebten, besteht an der Nutzung der Videokamera ein **objektiv nachvollziehbares Interesse** und somit ein Rechtfertigungsgrund iSd **Art 6 Abs 1 lit f DSGVO**. Die Videokamera war parallel zum Weg ausgerichtet und ihr Erfassungsbereich auf das eigene Grundstück beschränkt. Sie sollte also nicht in erster Linie der Überwachung des Servitutsberechtigten oder unbeteiligter Dritter dienen, sondern dem eigenen, berechtigten Bedürfnis nach effektivem Schutz der Gesundheit und des Eigentums. Dieses rechtfertigt auch eine allfällige Dokumentation von Geschehnissen über den eigentlichen, engen Eingangsbereich des Hauses hinaus. Das Interesse an der Datenverarbeitung überwiegt somit **das Geheimhaltungsinteresse** des Servitutsberechtigten.

Aus der weiteren Rechtsprechung des BVwG:

- Die **"Sache"** des bekämpften Bescheids bildet den äußersten Rahmen für die **Prüfungsbefugnis** des BVwG. Hat die DSB **jegliche Ermittlungstätigkeit** zu wesentlichen

Sachverhaltselementen unterlassen, ist die Angelegenheit jedoch zum Erlassen eines erneuten Bescheids an die DSB **zurückzuverweisen** ([BVwG 07.01.2025, W108 2286042-1](#)).

- Die Bestimmung des **Art 29 DSGVO** richtet sich an **Auftragsverarbeiter und** an jede dem Verantwortlichen oder dem Auftragsverarbeiter **unterstellte Person**. Bringt eine Person eine Beschwerde ein, muss sie damit rechnen, dass die **gesamte Beschwerde** – und nicht nur eine sinngemäße Inhaltswiedergabe – den anderen Verfahrensparteien zum **Parteiengehör** gestellt wird. Dies ergibt sich aus dem Grundsatz des **fairen Verfahrens**. Eine Datenverarbeitung kann **gleichzeitig** die **Erlaubnistatbestände** des **Art 6 Abs 1 lit c** und des **Art 6 Abs 1 lit e DSGVO** erfüllen ([BVwG 07.01.2025, W108 2284293-1](#)).
- Der EuGH hat mit Urteil vom [09.01.2025, C-416/23, Österreichische Datenschutzbehörde \(Demandes excessives\)](#), über die Frage entschieden, wann eine Datenschutzbeschwerde von der Aufsichtsbehörde als exzessiv abgelehnt werden darf. Die DSB hat die Behandlung der Datenschutzbeschwerde als **exzessiv** abgelehnt, ohne sich mit dessen Inhalt auseinanderzusetzen. Nach dem EuGH hätte die DSB eine **Missbrauchsabsicht** des Beschwerdeführers **nachzuweisen** gehabt. Da dahingehend keine Ermittlungen vorgenommen wurden, wird der Bescheid der DSB behoben und die Angelegenheit zum Erlassen eines neuen Bescheids an die DSB **zurückverwiesen** ([BVwG 14.01.2025, W298 2263736-1](#)).
- Besteht ein Betroffener trotz von der DSB eingeräumten Verbesserungsmöglichkeit auf die Fortsetzung des Verfahrens gegen einen **Beschwerdegegner**, der für die Verarbeitung nicht verantwortlich ist, ist die Datenschutzbeschwerde mangels **Passivlegitimation** des Beschwerdegegners abzuweisen ([BVwG 14.01.2025, W298 2300879-1](#)).
- Sind vor dem BVwG eine **erhebliche Anzahl** von Verfahren anhängig, in welchen dieselbe(n) Rechtsfrage(n) zu beantworten sind, die über eine Revision auch beim VwGH anhängen, kann das BVwG diese **Verfahren** mit Beschluss **aussetzen** ([BVwG 14.01.2025, W298 2262670-1](#); [13.01.2025, W108 2285445-1](#)).

### EU-Rechtsakte

- Am **04.02.2025** veröffentlichte die EU-Kommission den Entwurf der **Leitlinie zu verbotenen KI-Nutzungen**, in der die in Art 5 KI-VO beschriebenen **verbotenen KI-Systeme** genauer **definiert** werden. In der Leitlinie wird versucht, anhand von Beispielen die Grenze zwischen verbotenen und

noch erlaubten KI-Praktiken zu ziehen. Nach Art 5 KI-VO sind KI-Praktiken im Bereich (i) der schädlichen Manipulation und Täuschung, (ii) der schädlichen Ausnutzung von Schwachstellen, (iii) der Sozialbewertung, (iv) der Risikobewertung und Vorhersage von Straftaten, (v) des ungezielten automatischen Extrahierens (**Scraping**) von Gesichtsbildern zur Erweiterung von Datenbanken zur Gesichtserkennung, (vi) der Emotionserkennung, (vii) der biometrischen Kategorisierung und (viii) der Echtzeit-Fernbiometrischen Identifizierung für Strafverfolgungszwecke unter gewissen Umständen **verboten**. In den Beispielen der Kommission wird ua auf die Zulässigkeit von KI-Praktiken wie **Social Scoring** und **biometrischer Echtzeitidentifizierung** eingegangen. Die Leitlinie nimmt dabei auch Bezug auf die SCHUFA Entscheidung des EuGH, wonach es sich bei dem im Sachverhalt durchgeführten **Profiling** um eine Unterart des **Bewertens** iSd Art 5 Abs 1 lit c KI-VO handelt und diese Praktik unter gewissen Umständen auch in den **Anwendungsbereich** der KI-VO fällt und verboten sein kann. Ebenfalls geht die Leitlinie auf die Abgrenzung zu anderen Rechtsakten der EU, wie die DSGVO, den DSA etc ein und wie diese Bestimmungen im Zusammenspiel mit der KI-VO anzuwenden sind. Derzeit ist der Entwurf der Leitlinie nur auf Englisch verfügbar. Erst wenn alle Sprachfassungen verfügbar werden, wird die Leitlinie anwendbar.

- Am **06.02.2025** wurde der Entwurf der **Leitlinien zur Definition von KI-Systemen** veröffentlicht. Die Leitlinien verfolgen das Ziel, die sehr umfassende Definition des Begriffs **KI-Systeme**, welcher in Art 3 Z 1 KI-VO geregelt ist, konkreter zu definieren. In den Leitlinien werden aus der Definition sieben Prüfelemente abgeleitet. Der Begriff maschinengestützt umfasst Hardware und Software. Damit ist eine Vielzahl an Computersystemen gemeint, wie **Quantencomputing** und auch **biologische oder organische Systeme**, falls sie Rechenkapazität bieten. Die Leitlinie enthält darüber hinaus Ausnahmefälle, für die die KI-VO nicht anwendbar ist. Darunter fallen Systeme zur Verbesserung mathematischer Optimierung, einfache Datenverarbeitung, Systeme, die auf klassischer Heuristik basieren (eine Methode, bei der aus begrenztem Wissen und Zeit dennoch eine wahrscheinliche Lösung gefunden wird, bspw durch Zufallsstichproben oder "trial and error") und einfache Vorhersagesysteme. Als konkrete Beispiele für die **Ausnahmen** werden physikbasierte Systeme – zB zur **Wettervorhersage**, **Satellitentelekommunikationssysteme** zur Optimierung der Bandbreitenzuweisung, **Datenbankverwaltungssysteme**, die Daten nach spezifischen Kriterien sortieren oder filtern (zB finde alle Kunden, die mit "K" anfangen), und Systeme,



die **Aktienkurse vorhersagen** – genannt. Als Beispiel für die **Anwendbarkeit** der KI-VO werden KI-Systeme in **selbstfahrenden Autos** erwähnt, die **Echtzeitvorhersagen** in komplexen und dynamischen Umgebungen treffen.

to the point

# Datenschutzmonitor. 07/2025 vom 19.02.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 13.02.2025, 51409/19, *Macharik/Tschechien* (Schutz der Kommunikation, faires Verfahren)

- **Rechtsprechung des EuGH**

EuGH 13.02.2025, C-383/23, *ILVA* (Geldbuße, Unternehmensbegriff, Verhältnismäßigkeit)

EuGH 13.02.2025, C-612/23, *Verbraucherzentrale Berlin* (Telekommunikation, Mindestvertragslaufzeit)

- **Rechtsprechung des VwGH**

VwGH 16.01.2025, Ra 2024/04/0424 (Cookies, Widerruf)

VwGH 10.12.2024, Ra 2022/04/0107 (Nachholung des Auskunftersuchens)

- **Rechtsprechung der Justiz**

OGH 22.01.2025, 13Os105/24a (Erneuerungsantrag, Mobiltelefonauswertung)

OLG Linz 06.02.2025, 6R10/25w (Vollmacht, Identitätsnachweis, Ablehnung der Auskunft)

- **Rechtsprechung des BVwG**

BVwG 13.01.2025, W137 2304495-1 (Video, Servitut, Datenminimierung)

BVwG 10.01.2025, W252 2271738-1 (Beschwerdegegner, *res iudicata*)

BVwG 10.01.2025, W291 2261757-1; 22.01.2025, W108 2288262-1 (Massenverfahren, Aussetzung)

BVwG 27.12.2024, W258 2227269-1 (Geldbuße, Kontrollmaßnahmen, VVZ, DSFA)

- **EU-Rechtsakte**

DelegierteVO zur Ergänzung der DORA

DelegierteVO zu MiCAR

- **Nationale Rechtsakte**

FATF-Prüfungsanpassungsgesetz 2024

Änderung der BMKÖS-Datenaufbewahrungsverordnung

## To the Point:

### Rechtsprechung des EGMR

EGMR 13.02.2025, 51409/19, Macharik/Tschiechien

#### **Schutz der Kommunikation, faires Verfahren**

- Mit richterlichem Beschluss kam es zu einer Offenlegung von Kommunikationsdaten aus der Mailbox eines Unternehmens. Dadurch konnten die E-Mail-Kommunikation und deren Inhalte einer mit dem Unternehmen in Kontakt stehenden Beschuldigten erlangt werden. Die E-Mail-Kommunikation diente als Hauptbeweismittel im gegen die Beschuldigte eingeleiteten Verfahren, in dem sie verurteilt wurde. Im Verfahren beantragte sie erfolglos die Entfernung der E-Mail-Kommunikation aus den Verfahrensakten, weil diese Nachrichten keine Kommunikationsdaten iSd im Beschluss angeführten Gesetzes seien. Die angerufenen innerstaatlichen Gerichte erachteten die Verwertung der E-Mail-Kommunikation als Beweismittel unter Heranziehung unterschiedlicher Gesetzesbestimmungen für rechtmäßig. Die Beschuldigte wendete sich an den EGMR und monierte eine Verletzung ihres Rechts auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK sowie des Rechts auf ein faires Verfahren gemäß Art 6 EMRK. Darüber hinaus machte sie Schaden- und Aufwandsersatz geltend. Der EGMR bestätigte die Verletzung von Art 8 EMRK, lehnte aber das Begehren auf Schadenersatz ab und sprach einen Teil des Aufwandsersatzes iHv EUR 2.500 zu.

Der EGMR hat erwogen: Die **Vertraulichkeit** jeglicher privaten und beruflichen **Korrespondenz** wird von Art 8 EMRK umfasst. Ein Grundrechtseingriff ist nur zulässig, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist. Das Gesetz und etwaige Ermessensspielräume müssen hinreichend klar und nachvollziehbar formuliert sein. Die Sichtung von beruflichen E-Mails ist ein geringerer Eingriff in Art 8 EMRK als die Einsichtnahme in eine private Mailbox.

Die innerstaatlichen Gerichte zogen drei Normen als potenzielle Rechtfertigung für den Eingriff in das Grundrecht heran, wobei die von den letztinstanzlichen Gerichten herangezogene Norm zum Zeitpunkt des Eingriffs in dieser Form noch nicht in Kraft war. Die Speicherung und Herausgabe der Kommunikation war nach den genannten innerstaatlichen Bestimmungen nicht erlaubt. Die Anwendung der Bestimmungen erfolgte durch die Gerichte in einer nicht nachvollziehbaren Weise. Der Eingriff in das Grundrecht war daher weder **vorhersehbar** noch **gesetzlich vorgesehen**.

Die Verwendung von unzulässig erhobenen **Beweisen** ist keine Verletzung des Rechts

auf ein **fares Verfahren**, wenn der Eingriff nur geringfügig ist und **Verteidigungsrechte** sonst beachtet werden.

Den geltend gemachten Schadenersatz für die im Strafverfahren auferlegte Geldstrafe lehnte der EGMR mangels Kausalität zwischen der festgestellten Verletzung und dem geltend gemachten Schaden ab. **Immateriellen Schadenersatz** lehnte der EGMR ab, weil die **Feststellung einer Grundrechtsverletzung** eine ausreichende Entschädigung sei.

### Rechtsprechung des EuGH

EuGH 13.02.2025, C-383/23, ILVA

#### **Geldbuße, Unternehmensbegriff, Verhältnismäßigkeit**

- Das dänische Tochterunternehmen eines Konzerns speicherte zwischen Mai 2018 und Januar 2019 unrechtmäßig personenbezogene Daten von mindestens 350.000 ehemaligen Kunden. In Dänemark werden Geldbußen nicht von der Datenschutz-Aufsichtsbehörde verhängt, sondern auf Empfehlung der Aufsichtsbehörde von der Staatsanwaltschaft beim zuständigen Gericht beantragt. Die dänische Staatsanwaltschaft beantragte bemessen am Konzernumsatz eine Geldbuße iHv rund EUR 201.000. Das Erstgericht verhängte jedoch eine am Umsatz des Tochterunternehmens bemessene Geldbuße iHv rund EUR 13.400. Die Staatsanwaltschaft legte Berufung ein, weshalb das vorliegende Gericht den EuGH zur Auslegung des Begriffs "Unternehmen" in Art 83 Abs 4 bis 6 DSGVO befragte.

Der EuGH hat erwogen: ErwGr 150 DSGVO verweist iZm der Berechnung von Geldbußen nach Art 83 Abs 4 bis 6 DSGVO auf den Begriff "**Unternehmen**" iSd **Art 101 und 102 AEUV**. Dieser **Unternehmensbegriff** umfasst jede eine **wirtschaftliche** Tätigkeit ausübende **Einheit** unabhängig von ihrer Rechtsform und Finanzierungsart.

Nach Art 83 Abs 1 DSGVO stellt jede Aufsichtsbehörde sicher, dass **Geldbußen** nach Abs 4 bis 6 in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** sind. Art 83 Abs 2 DSGVO verlangt zudem, dass die zuständige Aufsichtsbehörde bei der Entscheidung über das Verhängen einer Geldbuße eine Reihe von **Kriterien** (ua Art, die Schwere und die Dauer des Verstoßes) berücksichtigt.

Diese Kriterien verweisen zwar nicht auf den Unternehmensbegriff iSd Art 101 und 102 AEUV, doch eine **Geldbuße** ist nur dann wirksam, verhältnismäßig und abschreckend, wenn sie nicht nur diese Kriterien, sondern auch die **materielle Leistungsfähigkeit** des Adressaten berücksichtigt. Daher ist zu prüfen, ob der Adressat einem

Unternehmen iSd Art 101 und 102 AEUV angehört.

In bestimmten **nationalen Rechtsordnungen**, etwa der Dänemarks, sind keine Geldbußen vorgesehen. Gemäß Art 83 Abs 9 DSGVO kann in diesen Fällen die zuständige Aufsichtsbehörde die Geldbuße in die Wege leiten, während die **nationalen Gerichte sie verhängen**.

Gemäß Art 83 DSGVO müssen die zuständigen Aufsichtsbehörden sicherstellen, dass bei der Berechnung der **tatsächlichen Höhe** der verhängten Geldbuße der **Grundsatz der Verhältnismäßigkeit** beachtet wird. Dies geschieht durch einen **angemessenen Ausgleich** zwischen dem allgemeinen Interesse am Schutz personenbezogener Daten und den Rechten des Verantwortlichen, des Auftragsverarbeiters oder des Unternehmens, dem diese angehören.

Auch wenn Verstöße gegen die DSGVO nicht mit administrativen, sondern mit von **Strafgerichten** verhängten Geldbußen geahndet werden, steht einer Anwendung des Begriffs "Unternehmen" iSd Art 101 und 102 AEUV im Rahmen von Art 83 Abs 4 bis 6 DSGVO nichts entgegen.

Der **Höchstbetrag einer Geldbuße** gegen einen Verantwortlichen, der ein Unternehmen ist oder einem Unternehmen angehört, wird auf Basis eines **Prozentsatzes des weltweiten Konzernumsatzes** berechnet. Der Konzernumsatz ist auch zu berücksichtigen, um die **tatsächliche oder materielle Leistungsfähigkeit** des Adressaten der Geldbuße zu beurteilen. Dadurch wird überprüft, ob die Geldbuße wirksam, verhältnismäßig und abschreckend ist.

EuGH 13.02.2025, C-612/23, Verbraucherzentrale Berlin

### **Telekommunikation, Mindestvertragslaufzeit**

- Eine Verbraucherzentrale erhob eine **Unterlassungsklage** gegen einen **Telekommunikationsanbieter** wegen deren **Geschäftspraxis**, die es Bestandskunden ermöglichte, vor Ablauf ihrer Erstverträge neue Folgeverträge mit einer Mindestlaufzeit von 24 Monaten abzuschließen. Die verbleibende Vertragslaufzeit der Erstverträge wurde dem neuen Vertrag hinzugerechnet. Nach Ansicht der Verbraucherzentrale verstieß dies gegen Art 30 der **UniversaldienstRL**, nach der keine anfängliche Mindestvertragslaufzeit von mehr als 24 Monaten vereinbart werden darf. Das vorliegende Gericht fragte den EuGH, ob der Begriff "anfängliche Mindestvertragslaufzeit" auch auf Verlängerungsverträge anzuwenden sei, was der EuGH bejahte.

Der EuGH hat erwogen: Die **UniversaldienstRL** ist in der Zwischenzeit durch den **europäischen Kodex für die**

**elektronische Kommunikation** (EKEK; Richtlinie [EU] 2018/1972) aufgehoben worden. Auf den Ausgangssachverhalt ist aber noch die **UniversaldienstRL** anzuwenden.

Art 30 Abs 5 **UniversaldienstRL** bestimmte, dass Verträge zwischen Verbrauchern und Unternehmen, die elektronische Kommunikationsdienste erbringen, keine anfängliche Mindestvertragslaufzeit von mehr als 24 Monaten beinhalten dürfen. Der Begriff "**anfängliche Mindestvertragslaufzeit**" bezieht sich sowohl auf die Laufzeit des Erstvertrags als auch auf die Laufzeit eines Folgevertrags zwischen denselben Parteien. Ein **Folgevertrag** darf keine Mindestvertragslaufzeit von mehr als 24 Monaten haben, auch wenn er vor Ablauf des Erstvertrags unterzeichnet und in Vollzug gesetzt wurde.

Die Festlegung zumutbarer Mindestlaufzeiten in Verbraucherverträgen ist nicht ausgeschlossen, darf aber **nicht mehr als 24 Monate betragen**. Der Unionsgesetzgeber wollte keine Unterscheidung zwischen Erst- und Folgeverträgen treffen. Ein Vergleich der Sprachfassungen der **UniversaldienstRL** bestätigt diese Auslegung. Der Schutz der Verbraucher war zentrales Ziel dieser RL und dieser darf nicht geringer sein, wenn ein Verbraucher Änderungen eines Vertrags mit einem Anbieter zustimmt, als wenn er erstmals eine Bindung mit einem neuen Anbieter eingeht. Dies gilt insbesondere, wenn der Folgevertrag wesentliche Änderungen gegenüber dem Erstvertrag enthält, wie etwa Preisgestaltung oder Leistungsinhalt.

### **Rechtsprechung des VwGH**

Aus der Rechtsprechung des VwGH:

- Die Anordnung des **Art 7 Abs 3 DSGVO**, dass der **Widerruf** so einfach sein müsse, wie die Erteilung der Einwilligung zur Verarbeitung personenbezogener Daten, ist nicht weiter auslegungsbedürftig. Die Frage, wie ein **Cookie-Banner** zu gestalten ist, ist jeweils anhand der für den **Einzelfall** maßgeblichen Umstände zu prüfen, weshalb diese Frage **nicht revisibel** ist ([VwGH 16.01.2025, Ra 2024/04/0424](#)).
- Gegenstand des Auskunftsverfahrens ist die **Verletzung der Auskunftspflicht** aufgrund eines bestimmten Auskunftsersuchens. Die Rechtswirksamkeit des Auskunftsersuchens ist somit Voraussetzung für eine Verletzung der Auskunftspflicht. Eine **Nachholung** des den Beschwerdegegenstand bildenden Auskunftsersuchens erst im datenschutzrechtlichen Verfahren ist **nicht möglich**, weil es sich bei der Stellung eines rechtswirksamen Auskunftsersuchens um die tatbestandsmäßige Voraussetzung dafür handelt, dass die (potenziell) Betroffene überhaupt in ihrem Recht verletzt werden

konnte. Durch diese Sichtweise entsteht **kein Rechtsschutznachteil**, weil jede (potenziell) Betroffene grundsätzlich jederzeit ein neues Auskunftersuchen an den Verantwortlichen richten kann ([VwGH 10.12.2024, Ra 2022/04/0107](#)).

### Rechtsprechung der Justiz

Aus der Rechtsprechung der Justiz:

- Die Behandlung von **Erneuerungsanträgen** in Strafverfahren ist auf die Prüfung der Verletzung eines Rechts nach der EMRK oder ihrer Zusatzprotokolle beschränkt. Die Bestimmungen des § 110 Abs 1 Z 1 und Abs 2 StPO sowie des § 111 Abs 2 StPO zur **Mobiltelefonauswertung** wurden mit Erkenntnis des VfGH als verfassungswidrig wegen Verstoßes gegen § 1 Abs 2 DSGVO iVm Art 8 Abs 2 EMRK aufgehoben. Wie der VfGH ausgesprochen hat, blieben diese aufgehobenen Bestimmungen jedoch aufgrund der gemäß Art 140 Abs 5 B-VG gesetzten Frist bis zum Ablauf des 31.12.2024 in Kraft. Sie waren daher zum Zeitpunkt der Entscheidung durch das Berufungsgericht anzuwenden ([OGH 22.01.2025, 130s105/24a](#)).
- Die DSGVO gibt keine bestimmte Form für den Identitätsnachweis im Rahmen eines Auskunftersuchens vor. Auch eine in diesem Zusammenhang erteilte Vollmacht muss daher nicht handschriftlich iSd § 886 ABGB sein. Bestehen begründete Zweifel an der Identität oder Vollmacht, muss der Verantwortliche dem Betroffenen seine **konkreten Bedenken** mitteilen. Die **pauschale Ablehnung** der Auskunft ist unzulässig ([OLG Linz 06.02.2025, 6R10/25w](#)).

### Rechtsprechung des BVwG

[BVwG 13.01.2025, W137 2304495-1](#)

#### **Video, Servitut, Datenminimierung**

- Zwei Grundstückseigentümer installierten eine Videokamera am Hauseingang, die auch einen Teil des von den Servitutsberechtigten genutzten Geh- und Fahrtwegbereich erfasste. Die Servitutsberechtigten erachteten sich in ihrem Recht auf Geheimhaltung verletzt und erhoben Datenschutzbeschwerde bei der DSB. Diese gab der Datenschutzbeschwerde statt und trug den Grundstückseigentümern auf, den Aufnahmebereich so einzuschränken, dass der Geh- und Fahrtwegbereich nicht mehr zu sehen ist. Gegen diesen Bescheid erhoben die Grundstückseigentümer (erfolglose) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Der Zweck der **Videoüberwachung** besteht grundsätzlich darin, das Grundstück der Grundstückseigentümer zu überwachen und ist als solcher berechtigt. Zwar besteht für die

Grundstückseigentümer ein **berechtigtes Interesse** am **Schutz ihres Eigentums** iSd Art 6 Abs 1 lit f DSGVO, allerdings überwiegt das Interesse der Servitutsberechtigten am Schutz ihres Privat- und Familienlebens bei der zweckmäßigen Nutzung ihrer Servitut.

Zudem haben die Grundstückseigentümer gegen den **Grundsatz der Datenminimierung** iSd Art 5 Abs 1 lit c DSGVO verstoßen, weil der Schutz ihres Eigentums auch dann erreicht werden könnte, wenn die Videokamera so positioniert wäre, dass diese nur den Eingangsbereich ihres Hauses überwacht.

Aus der weiteren Rechtsprechung des BVwG:

- Bestimmt die DSB irrtümlich den falschen **Beschwerdegegner** als Verantwortlichen, ist der Bescheid ersatzlos zu beheben. Wird ein Sachverhalt sowohl von einem Betroffenen als auch von der DSB aufgegriffen, um in einem Verfahren überprüft zu werden, führt dies zu keiner **res iudicata** ([BVwG 10.01.2025, W252 2271738-1](#)).
- Sind vor dem BVwG eine **erhebliche Anzahl** von Verfahren anhängig, in welchen dieselbe(n) Rechtsfrage(n) zu beantworten sind, die über eine Revision auch beim VwGH anhängen, kann das BVwG diese **Verfahren** mit Beschluss **aussetzen** ([BVwG 10.01.2025, W291 2261757-1; 22.01.2025, W108 2288262-1](#)).
- Ein beachtlicher **Ressourcen-Aufwand** bei der Vorbereitung auf die DSGVO schützt vor Strafe nicht und führt auch nicht zur Herabsetzung der **Geldbuße**. Ebenso wenig exkulpert die Einbindung einer **Datenschutzbeauftragten** von der Haftung oder führt zu einer Minderung der Geldbuße. Da die Anforderungen an die Rechtmäßigkeit der Datenverarbeitung und die Regelungen zu den Pflichten des Verantwortlichen unterschiedliche Ziele verfolgen, ist eine gleichzeitige Verurteilung wegen unrechtmäßiger Datenverarbeitung und fehlerhafter Führung des **Verarbeitungsverzeichnisses** sowie mangelhafter **Datenschutz-Folgenabschätzung** zulässig. Dies gilt auch dann, wenn allen Verstößen dieselbe rechtliche Fehlbeurteilung zugrunde liegt ([BVwG 27.12.2024, W258 2227269-1](#)).

### EU-Rechtsakte

- Am **13.02.2025** wurde die "*Delegierte Verordnung (EU) 2025/295 der Kommission vom 24. Oktober 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Harmonisierung der Bedingungen für die Durchführung von Überwachungsstätigkeiten*", [ABI L 2025/295, 1](#), kundgemacht. Mit dieser

DelegiertenVO ergänzt die Kommission die "VO (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor ..." (kurz: **DORA**) und legt fest, welche Informationen sog **IKT-Drittdienstleister** zur Verfügung zu stellen haben.

- Zur Ergänzung der "VO (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über **Märkte für Kryptowerte...**" (kurz: **MiCAR**) erließ die Kommission **fünf Delegierte Verordnungen**. Am **13.02.2025** wurden die DelegierteVO (EU) 2025/292, [ABI L 2025/292, 1](#); DelegierteVO (EU) 2025/296, [ABI L 2025/296, 1](#); DelegierteVO (EU) 2025/297, [ABI L 2025/297, 1](#); DelegierteVO (EU) 2025/298, [ABI L 2025/298, 1](#); DelegierteVO (EU) 2025/299, [ABI L 2025/299, 1](#), kundgemacht. Ergänzt wird die MiCAR durch mehrere **technische Regulierungsstandards**.

### **Nationale Rechtsakte**

- Am **10.02.2025** wurde das **FATF-Prüfungsanpassungsgesetz 2024**, [BGBl I 2025/5](#), kundgemacht. Mit dem FATF-Prüfungsanpassungsgesetz wurde das **Sanktionengesetz 2024** erlassen sowie ua das BWG, das FMABG und das KontRegG novelliert. Geregelt wird ua die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zur Umsetzung von Sanktionsmaßnahmen.
- Am **14.02.2024** wurde die "**Verordnung des Bundesministers für Kunst, Kultur, öffentlichen Dienst und Sport, mit der die **BMKÖS-Datenaufbewahrungsverordnung** geändert wird**", [BGBl II 2025/18](#), kundgemacht. Mit dieser V werden bestimmte **Aufbewahrungspflichten** bei der Verarbeitung der **Daten** von **Beamten** im Vergleich zu den Regelungen des § 280a BDG herab- oder heraufgesetzt.

to the point

# Datenschutzmonitor. 08/2025 vom 26.02.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 18.02.2025, 33067/22, *Kharazishvili/Georgien* (Anwaltsgeheimnis, Telefonüberwachung)

- **Rechtsprechung des VwGH**

VwGH 16.01.2025, Ra 2024/04/0438 (Auskunftersuchen, Auslegung)

- **Rechtsprechung der Justiz**

OGH 22.01.2025, 9ObA79/24v (sensible Daten, Dritte)

OLG Graz 30.12.2024, 10Bs118/24i (Sicherstellung, Mobiltelefon, Verhältnismäßigkeit)

- **Rechtsprechung des BVwG**

BVwG 19.12.2024, W287 2297969-1 (Bundespräsident, Journalist, Postenbesetzung)

BVwG 17.01.2025, W298 2293073-1 (Strafverfolgung, öffentliches Interesse, zwangsweise Unterbringung)

BVwG 09.12.2024, W292 2285487-1 (Unerbetene Nachricht, Selbstbelastungsverbot, Kosten des Beschwerdeverfahrens)

BVwG 23.01.2025, W605 2284399-1 (Mitwirkung, Geldbuße, Kosten des Beschwerdeverfahrens)

BVwG 07.01.2025, W108 2288748-1 (Auskunft, Empfänger, Speicherfrist, Beweisverfahren)

BVwG 09.09.2024, W176 2283061-1 (Auskunft, Datenkopie)

BVwG 13.01.2025, W137 2302430-1 (Wildkamera, Servitut, Selbsthilfe)

BVwG 22.01.2024, W108 2288584-1 (Rechtsschutzinteresse, formelle Beschwerde)

BVwG 28.01.2025, W252 2271964-1; W252 2271980-1 (Beschwerdegegner, *res iudicata*)

BVwG 11.12.2024, W603 2304073-1; 04.02.2025, L521 2306525-1; L521 2306682-1 (ORF-Beitrag, Zuständigkeit)

- **Rechtsprechung der LVwG**

LVwG Wien 13.01.2025, VGW-101/042/17553/2024 (Grundbuch, Abbruchbewilligung, Auskunft)

- **Rechtsprechung der DSB**

DSB 26.09.2024, 2024-0.112.476 (Maut, KFZ-Kennzeichen, Passage-Daten)

- **EU-Rechtsakte**

DelegierteVO und DurchführungsVO zur DORA

DelegierteVO und DurchführungsVO zur MiCAR

- **Nationale Rechtsakte**

Kundmachung der Vereinbarung gemäß Art 15a B-VG über die Organisation und Finanzierung des Gesundheitswesens (Tirol)

## To the Point:

### Rechtsprechung des EGMR

EGMR 18.02.2025, 33067/22, Kharazishvili/Georgien

#### **Anwaltsgeheimnis, Telefonüberwachung**

- Das georgische Finanzministerium leitete eine strafrechtliche Untersuchung wegen des Verdachts des illegalen Verkaufs von Zigarettenpackungen ein. Ein iransicher Staatsbürger soll dazu ein Unternehmen in Georgien gegründet haben, das von einer Anwältin vertreten wurde. Neben der Anwältin wurden ihr Ehemann und sechs weitere Personen des unrechtmäßigen Verkaufs großer Mengen verbrauchssteuerpflichtiger Waren ohne Verbrauchssteuerbanderolen verdächtigt. Auf Antrag der Generalstaatsanwaltschaft genehmigte das zuständige Stadtgericht das Abhören und Aufzeichnen ihrer Telefongespräche für 30 Tage. Dieser Beschluss wurde von der Anwältin und ihrem Ehemann ua deshalb angefochten, weil das Abhören aufgrund des Anwaltsgeheimnisses rechtswidrig sei. Das Berufungsgericht wies die Rechtsmittel ab. Der EGMR stellte eine Verletzung des Art 8 EMRK fest und sprach der Anwältin und ihrem Ehemann Schadenersatz zu.

Der EGMR hat erwogen: **Telefonüberwachung** fällt unter den Schutz von "Privatleben" und "Korrespondenz" nach Art 8 EMRK. Sie ist nur zulässig, wenn sie gesetzlich vorgesehen ist, ein legitimes Ziel verfolgt und in einer demokratischen Gesellschaft notwendig ist, um ein solches Ziel zu erreichen. Die gesetzliche Grundlage muss zugänglich und vorhersehbar sein. Besonders bei **geheimen Überwachungsmaßnahmen** sind klare, detaillierte Regeln erforderlich, um Willkür zu vermeiden.

Die Telefonüberwachung hatte ihre gesetzliche Grundlage in der georgischen Strafprozessordnung, die den Antragstellern auch zugänglich war. Diese regelte ua die Grundsätze, Voraussetzungen und Dauer der Datenverarbeitung und gab der Anwältin und ihrem Ehemann somit eine angemessene Vorstellung von den Umständen der **verdeckten Ermittlungsmaßnahme**.

Die georgische Strafprozessordnung verpflichtete Richter dazu, die **Notwendigkeit** und **Verhältnismäßigkeit** der verdeckten Ermittlungsmaßnahme zu prüfen. Der Gerichtsbeschluss enthielt allerdings weder konkrete Fakten, mit denen der Verdacht einer Straftat begründet wurde noch eine Bewertung der Notwendigkeit oder Verhältnismäßigkeit der verdeckten Ermittlungsmaßnahme.

Zudem versäumte das Berufungsgericht, das **Anwaltsgeheimnis** gegen die Erfordernisse der strafrechtlichen Untersuchung abzuwägen.

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Eine in vertretbarer Weise vorgenommene fallbezogene **Auslegung** eines **Auskunftersuchens** durch das BVwG ist nicht revisibel, weil ihr über den Einzelfall hinaus keine Bedeutung zukommt ([VwGH 16.01.2025, Ra 2024/04/0438](#)).

### Rechtsprechung der Justiz

OGH 22.01.2025, 90bA79/24v

#### **Sensible Daten, Dritte**

- Eine ehemalige diplomierte Gesundheits- und Krankenpflegerin (Krankenpflegerin) eines öffentlichen Bezirkskrankenhauses, das durch den Gemeindeverband betrieben wird, klagte Schadenersatz vom Betreiber ein. Sie behauptete, durch "Bossing-Handlungen" des Verwaltungsdirektors des Krankenhauses Gesundheitsbeeinträchtigungen erlitten zu haben. Der Verwaltungsdirektor berief deshalb eine Sonderkollegialführungssitzung ein, die die Entlassung der Krankenpflegerin beschloss, was durch den Gemeindeverbandsausschuss bestätigt wurde. Die Krankenpflegerin begehrte in der nunmehrigen Klage, es zu unterlassen, ihre Gesundheitsdaten und Verfahrensakten an Nichtorgane des Betreibers weiterzugeben. Hilfsweise verlangte sie, dass ihre Patientendaten datenschutzkonform geschützt werden. Das Erstgericht wies die Klage ab, was das Berufungsgericht bestätigte, aber dem Eventualbegehren teilweise stattgab. Der OGH wies die außerordentliche Revision der Krankenpflegerin zurück.

Der OGH hat erwogen: Entscheidungswesentlich war, ob der Betreiber berechtigt war, Inhalte aus dem Schadenersatzverfahren den im Hauptbegehren genannten Personen zur Kenntnis zu bringen. Der Gemeindeverbandsausschuss besteht aus landesgesetzlich bestimmten Mitgliedern. Der ärztliche Leiter, der Verwaltungsleiter und der Leiter des Pflegedienstes der Krankenanstalt sowie ein vom Betriebsrat entsandten Vertreter gehören dem Gemeindeverbandsausschuss mit beratender Stimme an und sind **keine "unbefugten Dritten"**.

Nur Personen, die ein Organ des Betreibers bilden, erlangten Kenntnis vom Inhalt des Schriftsatzes und den darin enthaltenen **sensiblen Daten** der Klägerin. Die Verarbeitung personenbezogener Daten war zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen** erforderlich (Art 9 Abs 2 lit f DSGVO). "**Erforderlich**" bedeutet, dass ohne die Daten die Geltendmachung des Anspruchs bzw eine Verteidigung dagegen nicht möglich oder wesentlich erschwert wäre. Die Kenntnis der Angehörigen des Gemeindeverbandsausschusses war von der erforderlichen Rechtsverteidigung



iSd Art 9 Abs 2 lit f DSGVO gedeckt. Das Interesse des Betreibers an der Rechtsverteidigung überwog das Geheimhaltungsinteresse der Krankenpflegerin.

OLG Graz 30.12.2024, 10Bs118/24i

### **Sicherstellung, Mobiltelefon, Verhältnismäßigkeit**

- Die Staatsanwaltschaft (StA) ermittelte gegen einen Jugendlichen, der Aufnahmen einer Minderjährigen beim Oralverkehr angefertigt und verbreitet haben soll. In diesem Zusammenhang ordnete die StA die Sicherstellung seines Mobiltelefons an. Der Jugendliche sah sich durch eine unzureichende Begründung der Sicherstellung in seinen Rechten verletzt. Das LG Graz gab dem Einspruch der Rechtsverletzung nicht Folge. Dagegen richtet sich die Beschwerde des Jugendlichen, der das OLG Graz teilweise Folge gab.

Das OLG Graz hat erwogen: Die **Sicherstellung eines Mobiltelefons** aus Beweisgründen iSd § 110 Abs 1 Z 1 StPO a.F. ist nur zulässig, wenn der Verdacht einer strafbaren Handlung besteht. In der schriftlichen Begründung der Sicherstellung müssen für alle konkreten Tatbestandselemente der vermuteten Straftat bestimmte, sinnlich wahrnehmbare Anhaltspunkte bezeichnet werden. Die Anordnung der StA war wegen Begründungsmängeln unzulässig.

Das Gericht kann eine Zwangsmaßnahme allerdings aufgrund eigener Erwägungen im Ergebnis als rechtsfehlerfrei beurteilen und den Einspruch verwerfen. Die Begründung der StA beinhaltete zwar keine ausreichenden Anhaltspunkte für den von ihr angeführten Verdacht der fortdauernden Belästigung im Wege einer Telekommunikation oder eines Computersystems nach § 107c StGB, aber sehr wohl für das Vergehen der pornographischen Darstellung Minderjähriger nach § 207a StGB. Die Sicherstellung war in diesem Zusammenhang aus Beweisgründen erforderlich. In Hinblick auf das Gewicht der (Sexual-)Straftaten zum Nachteil einer Minderjährigen, den Grad des Verdachts und des zu erwartenden Beitrags zur Sachverhaltsaufklärung war sie auch verhältnismäßig. Die **Verhältnismäßigkeit** ergibt sich zudem aus der ausdrücklichen Beschränkung der Auswertung auf das in Rede stehende Video und auf Nachrichtenverläufe während eines konkreten Zeitraums.

### **Rechtsprechung des BVwG**

BVwG 19.12.2024, W287 2297969-1

### **Bundespräsident, Journalist, Postenbesetzung**

- Ein **Journalist** brachte ein Auskunftsbegehren nach § 2 AuskunftspflichtG bei der

**Präsidenschaftskanzlei** ein. Insbesondere verlangte er die Übermittlung eines Gutachtens und eines Aktenvermerks zu einer **Postenbesetzung**. In Beantwortung des Begehrens übermittelte die Präsidenschaftskanzlei den Antrag auf Ernennung und eine Resolution zur Bestellung. Da Bewerberdaten im Gutachten enthalten waren und der Aktenvermerk ein nicht zu beauskunftendes Werturteil enthielt, lehnte der **Bundespräsident** die Übermittlung dieser Unterlagen mit Bescheid ab. Gegen den Bescheid erhob der Journalist erfolglose Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Bei der Einschränkung der **Auskunftsbeantwortung** hat die Behörde den (i) Zweck und das Ziel des Informationsansuchens, (ii) die tatsächliche Notwendigkeit des Informationsbegehrens für die Ausübung der Meinungsfreiheit, (iii) den Charakter der begehrten Informationen, (iv) die Rolle des Zugangswerbers und (v) die Existenz von bereits verfügbaren Informationen zu prüfen.

Die Verweigerungsgründe für Auskünfte sind eng auszulegen. Insbesondere wenn Journalisten als **public watchdog** die Auskunft begehren. Die Herausgabe des Gutachtens aus dem **Bewerbungsprozess** ist von der Auskunft nach dem AuskunftspflichtG jedoch ausgenommen. Die Bewerber mussten nicht damit rechnen, dass ihre Identität sowie die Einschätzungen und Wertungen der Kommission im **Gutachten** öffentlich gemacht werden. Bewerber, die aus der **Richterschaft** kommen, genießen dabei kein geringeres Geheimhaltungsinteresse.

Beim gegenständlichen **Aktenvermerk** handelt es sich um interne Abwägungs- und Willensbildungsprozesse, die bereits von der Akteneinsicht ausgenommen sind und auch nach dem AuskunftspflichtG nicht zu beauskunfteten sind.

BVwG 17.01.2025, W298 2293073-1

### **Strafverfolgung, öffentliches Interesse, zwangsweise Unterbringung**

- Ein aufgebrachter Bürger verursachte einen Polizeieinsatz. Bei der **zwangsweisen Unterbringung**, unter Anwendung von Körperkraft in eine **psychiatrische Anstalt**, wurde der Bürger verletzt. Zur Dokumentation des Einschreitens erstellten die Beamten ein **Anhalteprotokoll**, welches an verschiedene Stellen weitergeleitet wurde. Der aufgebrachte Bürger erhob Datenschutzbeschwerde wegen der Verletzung seines Rechts auf Geheimhaltung, Löschung, Berichtigung und der Weitergabe seiner Daten. Nachdem die DSB in ihrer Reaktion säumig war, erhob er **Säumnisbeschwerde**. Das BVwG entschied in der Sache selbst und wies die Bescheidbeschwerde ab.

Das BVwG hat erwogen: Eine Verarbeitung nach Art 6 Abs 1 lit e DSGVO ist rechtmäßig, wenn sie für die Wahrnehmung einer **Aufgabe im öffentlichen Interesse** erforderlich ist. Die **Öffnungsklausel des Art 9 Abs 2 lit g DSGVO** verlangt für die Zulässigkeit der Datenverarbeitung eine **gesetzliche Grundlage** im nationalen Recht oder im Unionsrecht. Diese muss in einem angemessenen Verhältnis zum verfolgten Ziel stehen, den Wesensgehalt des Datenschutzrechts wahren und Maßnahmen zur Interessenwahrung der Betroffenen vorsehen. Ergänzend muss ein **erhebliches öffentliches Interesse** an der Verarbeitung bestehen. Bei Erfüllung dieser Erfordernisse ist die Verarbeitung dann auch nach Art 6 Abs 1 lit e DSGVO rechtmäßig.

An **Maßnahmen zur Strafverfolgung** besteht ein **öffentliches Interesse**. Sicherheitsbehörden dürfen **Gesundheitsdaten** ua an den örtlichen Rettungsdienst und andere in § 39b UbG genannte Stellen weiterleiten. Das Weiterleiten von Daten zum Ausdruck eines **Waffenverbots** war nach § 39a UbG und das Weiterleiten der Daten an die StA nach § 100 StPO gerechtfertigt.

Da die Daten des Bürgers rechtmäßig verarbeitet wurden und mit § 10 Abs 3 der **Richtlinien-Verordnung** eine **Aufbewahrungspflicht** für Sicherheitsbehörden normiert war, waren diese nicht zu löschen.

BVwG 09.12.2024, W292 2285487-1

### **Unerbetene Nachricht, Selbstbelastungsverbot, Kosten des Beschwerdeverfahrens**

- Ein Arbeitsuchender veröffentlichte seine Kontaktdaten im eJob-Room des AMS, um eine Stelle zu finden. Ein Personalüberlassungsunternehmen übernahm diese Daten und speicherte sie für die Arbeitsvermittlung. Der Arbeitsuchende verlangte die Löschung seiner Daten, weil er kein Interesse mehr an Jobangeboten hatte. Dennoch speicherte das Unternehmen die Daten weiter und nutzte sie, um ihm weitere Jobangebote zuzusenden.

Der Arbeitsuchende brachte Datenschutzbeschwerde bei der DSB ein. Nachdem das Personalüberlassungsunternehmen auf mehrere Aufforderungen der DSB zur Stellungnahme nicht reagierte, leitete diese ein Verwaltungsstrafverfahren ein und verhängte eine Geldstrafe (zzgl Verfahrenskosten). Die Bescheidbeschwerde an das BVwG blieb erfolglos und das BVwG verpflichtete das Personalüberlassungsunternehmen zur Zahlung der **Kosten des Beschwerdeverfahrens iHv 20% der verhängten Strafe**.

Das BVwG hat erwogen: Die Verarbeitung personenbezogener Daten bei der Ausübung des Gewerbes der **Überlassung von Arbeitskräften** (§ 135 GewO) kann zum Zweck der Anbahnung neuer

Dienstverhältnisse ein **berechtigtes Interesse** iSd Art 6 Abs 1 lit f DSGVO sein. Es kommt dabei nicht darauf an, ob das Unternehmen die Kontaktdaten des Arbeitsuchenden im Rahmen der Arbeitskräfteüberlassung oder der Arbeitsvermittlung verwendete bzw ob es im relevanten Tatzeitraum zur Arbeitsvermittlung berechtigt war (§ 4 Abs 1 Z 4 AMFG).

Das Personalüberlassungsunternehmen hat jedoch dem Arbeitsuchenden via SMS Arbeitsangebote übermittelt, um eine Vertragsbeziehung anzubahnen (**Direktwerbung**). Das Versenden elektronischer Werbenachrichten an den Arbeitssuchenden verstieß gegen § 174 Abs 3 TKG 2021, weil dieser dem Unternehmen gegenüber zu keinem Zeitpunkt eine Einwilligung erteilt hatte und zwischen den Parteien auch keine Kundenbeziehung bestand.

Der Arbeitsuchende teilte dem Unternehmen via E-Mail unmissverständlich mit, dass er keine elektronischen Nachrichten mit Arbeitsangeboten erhalten möchte. Bei dieser Erklärung handelte es sich neben einem **Löschersuchen gemäß Art 17 DSGVO** auch um einen **Widerspruch nach Art 21 DSGVO**. Ab diesem Zeitpunkt war auch jegliche Verarbeitung seiner **Kontaktdaten** unzulässig.

Das Personalüberlassungsunternehmen verstieß zudem gegen seine Mitwirkungspflicht gemäß Art 31 DSGVO. Die Pflicht nach Art 31 DSGVO ist grundrechtskonform auszulegen und findet ihre Grenze im **Selbstbelastungsverbot**. Die Mitwirkungspflicht eines Verantwortlichen folgt jedoch bereits aus der **Rechenschaftspflicht** des Art 5 Abs 2 DSGVO und kann nicht von vornherein als grundrechtswidrig angesehen werden.

BVwG 23.01.2025, W605 2284399-1

### **Mitwirkung, Geldbuße, Kosten des Beschwerdeverfahrens**

- Die DSB forderte eine GmbH wiederholt zu Stellungnahmen in gegen sie anhängigen Datenschutzbeschwerdeverfahren auf und wies dabei jedes Mal auf die Mitwirkungspflicht gemäß Art 31 DSGVO sowie auf ein drohendes Verwaltungsstrafverfahren hin. Die GmbH reagierte auf keine dieser Aufforderungen und die Verfahren wurden ohne ihre Mitwirkung abgeschlossen. Daraufhin leitete die DSB ein Verwaltungsstrafverfahren gegen die GmbH ein, und verurteilte sie wegen Verletzung der Mitwirkungspflicht zu einer Geldstrafe. Die dagegen eingebrachte Bescheidbeschwerde wies das BVwG ab und es verpflichtete die GmbH zur Zahlung der **Kosten des Beschwerdeverfahrens iHv 20% der verhängten Strafe**.

Das BVwG hat erwogen: Den Verantwortlichen trifft gemäß Art 31 DSGVO eine Mitwirkungspflicht. Bei fehlender Kooperation ist

eine **Geldbuße** zu verhängen. Die Pflicht zur Zusammenarbeit erfordert keinen Erfolgseintritt, sondern die rechtzeitige und fristgerechte Beantwortung der Anfragen der Aufsichtsbehörde.

Die GmbH wurde als Verantwortliche aufgrund von gegen sie erhobenen Datenschutzbeschwerden zur Stellungnahme und Mitwirkung aufgefordert. Die Mitarbeiterin, die die Schreiben abgelegt haben soll, war zur Empfangnahme der Schreiben befugt. Die mittels RSb erfolgte Zustellung der Schreiben war daher unzweifelhaft rechtswirksam.

BVwG 07.01.2025, W108 2288748-1

### **Auskunft, Empfänger, Speicherfrist, Beweisverfahren**

- Ein Kunde stellte ein Auskunftersuchen an ein Energieversorgungsunternehmen. Er forderte Auskunft über die Empfänger seiner personenbezogenen Daten und die Löschung seiner E-Mail-Adresse. Da das Energieversorgungsunternehmen in seinem Antwortschreiben nur allgemeine Informationen bekanntgab und die Löschung der E-Mail-Adresse bestätigte, sah sich der Kunde in seinem Recht auf Auskunft sowie dem Recht auf Löschung verletzt und brachte eine Datenschutzbeschwerde bei der DSB ein. Die DSB gab der Datenschutzbeschwerde teilweise statt und stellte fest, dass das Energieversorgungsunternehmen den Kunden in seinem Recht auf Auskunft verletzt hat. Daraufhin richteten sowohl der Kunde als auch das Energieversorgungsunternehmen (teilweise erfolgreiche) Bescheidbeschwerden an das BVwG.

Das BVwG hat erwogen: Gemäß Art 15 Abs 1 lit c DSGVO haben Betroffene das Recht auf Information über die Empfänger oder Kategorien von **Empfängern**, gegenüber denen ihre personenbezogenen Daten offengelegt wurden oder noch offengelegt werden. Der Kunde hat in seinem Schreiben ausdrücklich Auskunft über die Empfänger seiner personenbezogenen Daten begehrt. Das Energieversorgungsunternehmen hatte **kein Wahlrecht**, ob es konkrete Empfänger oder Kategorien von Empfängern bekanntgibt, sondern musste die Empfänger benennen, soweit es diese kannte. Auch **Auftragsverarbeiter** gelten als Empfänger, nicht aber Beschäftigte oder sonstige Stellen, die dem Verantwortlichen unmittelbar unterworfen sind.

Gemäß Art 15 Abs 1 lit d DSGVO hat die betroffene Person das Recht auf Information über die geplante Dauer der Aufbewahrung der personenbezogenen Daten oder die Kriterien für die Festlegung dieser Dauer. Ein genereller Verweis auf **gesetzliche Aufbewahrungspflichten** oder die Geltendmachung/Abwehr von rechtlichen Ansprüchen

ohne konkrete Rechtsgrundlage ist **nicht ausreichend**. Das Energieversorgungsunternehmen hat jedoch in seiner Bescheidbeschwerde konkrete Rechtsgrundlagen (§ 132 BAO und § 1468 ABGB) angeführt, aus denen sich die Dauer der Speicherung ergibt. Diese Auskunft ist **ausreichend**.

Hinsichtlich des Rechts auf **Löschung** gemäß Art 17 DSGVO hat die DSB festgestellt, dass das Energieversorgungsunternehmen die E-Mail-Adresse des Kunden gelöscht hat. Der Kunde wurde jedoch nach behaupteter Löschung erneut über diese Adresse kontaktiert und hielt dies auch in seiner Bescheidbeschwerde fest. Die DSB hat sich diesbezüglich nur auf **schriftliche Stellungnahmen** der beiden Parteien beschränkt und somit keine ausreichenden Ermittlungen durchgeführt. Die DSB hätte ein **Beweisverfahren** durchzuführen gehabt, um den vollständigen, rechtlich relevanten und **wahren Sachverhalt** festzustellen. Der Kunde und das Energieversorgungsunternehmen hätten **förmlich einvernommen** werden müssen. Die Sache wird daher bezüglich der Frage, ob eine Verletzung des Rechts auf Löschung vorliegt, zur neuerlichen Entscheidung an die DSB **zurückverwiesen**.

Aus der weiteren Rechtsprechung des BVwG:

- Das **Recht auf eine Kopie** der personenbezogenen Daten bedeutet, dass der betroffenen Person eine **originalgetreue** und **verständliche Reproduktion** aller ihrer Daten ausgefolgt wird. Ein **zusätzliches Recht** auf Kopien von Auszügen aus Dokumenten, ganze Dokumente oder Auszüge aus Datenbanken räumt Art 15 Abs 3 Satz 1 DSGVO **nicht ein** ([BVwG 09.09.2024, W176 2283061-1](#)).
- Das **Wegerecht** ist eine **Felddienstbarkeit**. Besteht auf einer Zufahrtsstraße eine **Servitut**, darf sich der Servitutsberechtigte gegen die Behinderung der Ausübung des absoluten Rechts – hier des Wegerechts – durch **gerechtfertigte Selbsthilfe** zur Wehr setzen. Wird die Nutzung der Dienstbarkeit durch eine Hecke beeinträchtigt, darf der Servitutsberechtigte die Hecke zurückstutzen. Der Grundstückseigentümer ist nicht berechtigt, den Zufahrtsweg deshalb mit einer **Wildkamera** zu **überwachen** ([BVwG 13.01.2025, W137 2302430-1](#)).
- Prozessvoraussetzung für die Führung von Verfahren vor Verwaltungsgerichten ist ua das Bestehen eines **Rechtsschutzinteresses**. Wurde der Datenschutzbeschwerde von der DSB vollinhaltlich stattgegeben, steht der Bescheidbeschwerde der Mangel der **formellen Beschwer** und somit des Rechtsschutzbedürfnisses entgegen ([BVwG 22.01.2024, W108 2288584-1](#)).

- Bestimmt die DSB irrtümlich den falschen **Beschwerdegegner** als Verantwortlichen, ist der Bescheid ersatzlos zu beheben. Wird ein Sachverhalt sowohl von einem Betroffenen als auch von der DSB aufgegriffen, um in einem Verfahren überprüft zu werden, führt dies zu **keiner res iudicata** (BVwG 28.01.2025, [W252 2271964-1](#); [W252 2271980-1](#)).
- Das Grundrecht auf Datenschutz ist im Verfahren über die Festsetzung des **ORF-Beitrags nicht präjudiziell**, weshalb allfällige datenschutzrechtliche Bedenken der Festsetzung des ORF-Beitrags nicht entgegenstehen. Die in **§ 13 ORF-Beitrags-Gesetz 2024** vorgesehenen Datenübermittlungen werden für einen exakt definierten Zweck durchgeführt. Eine (unzulässige) **Vorratsdatenspeicherung** im Sinn einer Ermittlung von Daten zur Nutzung für einen späteren, zum Zeitpunkt der Ermittlung der Daten noch ungewissen Zweck, liegt nicht vor. Zudem ist die Zuständigkeit des BVwG im Kontext datenschutzrechtlicher Anbringen auf die Entscheidung über Datenschutzbeschwerden gegen Bescheide der DSB beschränkt (BVwG [11.12.2024, W603 2304073-1](#); 04.02.2025, [L521 2306525-1](#); [L521 2306682-1](#)).

### Rechtsprechung der LVwG

LVwG Wien 13.01.2025, VGW-101/042/17553/2024

### Grundbuch, Abbruchbewilligung, Auskunft

- Ein Abgeordneter des Wiener Gemeinderats beehrte beim Magistrat der Stadt Wien (**MA 37, Baupolizei**) Auskunft darüber, für welche Bauwerke im Jahr 2023 Ansuchen auf Abbruch wegen wirtschaftlicher Abbruchreife eingebracht und für welche dieser Bauwerke der Abbruch bewilligt respektive nicht bewilligt wurde. Dabei berief er sich auf das Wiener Auskunftspflichtgesetz (Wr. AuskunftspflichtG). Die MA 37 verweigerte die Auskunft der Liegenschaftsadressen, weil die Eigentümer der Gebäude über das öffentliche Grundbuch ausfindig gemacht werden könnten und die Adressen somit personenbezogene Daten seien. Dagegen richtete sich die (erfolgreiche) Bescheidbeschwerde des Abgeordneten.

Das LVwG Wien hat erwogen: Eine **Liegenschaftsadresse** ist ein personenbezogenes Datum. Das Wr. AuskunftspflichtG ist gesetzliche Grundlage der Auskunftsbefugnis der MA 37 iSd § 1 DSG. Ein Grund zur Verweigerung der Auskunft sind gesetzliche Verschwiegenheitspflichten, deren Vorliegen allerdings eng auszulegen ist.

Gemäß § 1 Wr. AuskunftspflichtG iVm § 1 Abs 2 DSG ist die Auskunft nur bei überwiegendem Interesse des Auskunftswerbers zulässig. Der **Abgeordnete** beantragte die

Auskunft nicht aus rein privater Neugier, sondern zur Wahrnehmung seiner Funktion als **public watchdog**. Zudem kommen ihm als Gemeinderats- und Landtagsabgeordneter aus der Bundesverfassung umfassende Kontrollpflichten zu, die nur auf Grundlage der beantragten Informationen ausgeübt werden können. Das Geheimhaltungsinteresse der Eigentümer ist hingegen vergleichsweise gering, weil Eigentümer einer Liegenschaft ohnehin durch Einsicht in das öffentliche **Grundbuch** ermittelt werden können. Die Auskunft liegt somit im **überwiegenden Interesse** des Abgeordneten.

Die Möglichkeit, dass Unbefugte mit Kenntnis von der Abbruchreife das Gebäude betreten und bewohnen könnten, rechtfertigt nicht die Verweigerung der Auskunft. Im Vergleich zu **unbewohnten Gebäuden** ist die Gefahr eines Einbruchsdiebstahls bei bewohnten Gebäuden eindeutig höher.

### Rechtsprechung der DSB

Aus der Rechtsprechung der DSB:

- Die Betreiberin des hochrangigen Straßennetzes in Österreich ist gemäß § 16a Abs 1 BStMG berechtigt, die zur Mauthebung, zur **Mautaufsicht** und zur Verfolgung von **Mautprellerei** erforderlichen personenbezogenen Daten (zB **Kfz-Kennzeichen**) automationsunterstützt zu verarbeiten und für ein Jahr ab der Mautstellen-Durchfahrt zu speichern. Die Verarbeitung erfolgt iSd **Datenminimierungsgrundsatzes**, ist dem gesetzlichen Zweck angemessen, erheblich und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt. Die Speicherung der **Passage-Daten** für ein Jahr ab der Mautstellen-Durchfahrt ist für die Zwecke der **Betrugsbekämpfung** und **Reklamation** angemessen ([DSB 26.09.2024, 2024-0.112.476](#)).

### EU-Rechtsakte

- Am **20.02.2025** wurde die "*Delegierte Verordnung (EU) 2025/301 der Kommission vom 23. Oktober 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung des Inhalts und der Fristen für die Erstmeldung, die Zwischenmeldung und die Abschlussmeldung schwerwiegender IKT-bezogener Vorfälle sowie des Inhalts der freiwilligen **Meldung erheblicher Cyberbedrohungen***", [ABI L 2025/301](#), kundgemacht. Mit dieser **DelegiertenVO** ergänzt die Kommission die "*VO (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor ...*" (kurz: **DORA**) und legt fest, welche Informationen

mit **Meldungen von IKT-Vorfällen** zu übermitteln sind.

- Am **20.02.2025** wurde die "Durchführungsverordnung (EU) 2025/302 der Kommission vom 23. Oktober 2024 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates im Hinblick auf Standardformulare, Vorlagen und Verfahren für Finanzunternehmen zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls oder einer erheblichen Cyberbedrohung", [ABI L 2025/302](#), kundgemacht. Auch diese **DurchführungsVO** wurde auf Grundlage der **DORA** erlassen und enthält Vorschriften zur **Meldung von IKT-Vorfällen**.
- Am **20.02.2025** wurde die "Delegierte Verordnung (EU) 2025/303 der Kommission vom 31. Oktober 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der von bestimmten Finanzunternehmen in die Mitteilung zur Bekundung ihrer Absicht zur **Erbringung von Krypto-Dienstleistungen** aufzunehmenden Angaben", [ABI L 2025/303](#), kundgemacht. Mit dieser **DelegiertenVO** ergänzt die Kommission die "VO (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über **Märkte für Kryptowerte** [...]" (kurz: **MiCAR**) und legt **technische Regulierungsstandards** fest.
- Am **20.02.2025** wurde die "Durchführungsverordnung (EU) 2025/304 der Kommission vom 31. Oktober 2024 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates im Hinblick auf Standardformulare, Muster-texte und Verfahren für die Mitteilung von bestimmten Finanzunternehmen zur Bekundung ihrer Absicht zur **Erbringung von Krypto-Dienstleistungen**", [ABI L 2025/304](#), kundgemacht. Auch diese **DurchführungsVO** wurde auf Grundlage der **MiCAR** erlassen und enthält Vorschriften zu **Regulierungsstandards**.

### **Nationale Rechtsakte**

- Am **18.02.2025** wurde die Kundmachung des Landeshauptmanns von Tirol betreffend die Vereinbarung gemäß Art 15a B-VG über die Organisation und Finanzierung des Gesundheitswesens, [LGBI 2025/9](#), kundgemacht. Die Vereinbarung behandelt ua **ELGA, eHealth** und die **eIDAS**-konforme Ausgestaltung des **e-card-Systems**.

to the point

# Datenschutzmonitor. 09/2025 vom 05.03.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH 25.02.2025, C-233/23, *Alphabet* (Missbrauch einer beherrschenden Stellung, Interoperabilität)

EuGH 27.02.2025, C-203/22, *Dun & Bradstreet* (Automatisierte Entscheidungsfindung, Profiling, Auskunftsrecht, Geschäftsgeheimnis)

EuGH 27.02.2025, C-638/23, *Amt der Tiroler Landesregierung* (Rollenverteilung per Gesetz, öffentliche Stelle)

EuGH SA 27.02.2025, C-57/23, *Policejní prezidium* (Biometrische und genetische Daten, DSRL-PJ, Recht der Mitgliedstaaten)

- **Rechtsprechung der Justiz**

OGH 18.02.2025, 14Os11/25m (SKY-ECC, Auswertung eines Mobiltelefons)

- **Rechtsprechung des BVwG**

BVwG 28.01.2025, W108 2286343-1 (Identifikationsregister, e-Card, Auskunft, Verantwortliche)

BVwG 31.01.2025, W258 2247059-1 (Löschung, Klaglosstellung, Feststellungskompetenz, allgemeines rechtliches Interesse)

BVwG 28.01.2025, W252 2271493-1; W252 2271450-1 (Beschwerdegegner, *res iudicata*)

BVwG 29.01.2025, W171 2262672-1; W171 2262379-1 (Massenverfahren, Aussetzung)

## To the Point:

### Rechtsprechung des EuGH

EuGH 25.02.2025, C-233/23, Alphabet

#### **Missbrauch einer beherrschenden Stellung, Interoperabilität**

- Google, eine Tochtergesellschaft von Alphabet, entwickelte das Betriebssystem Android OS und die digitale Plattform Android Auto. Ein italienisches Unternehmen führte eine App ein, die verschiedene Funktionen für das Aufladen von Elektrofahrzeugen bietet und ersuchte Google, die Interoperabilität der App mit Android Auto zu gewährleisten. Google lehnte dies "aus Sicherheitsgründen" und der "Notwendigkeit einer rationalen Zuweisung von Ressourcen" ab. Der Anbieter der App wandte sich an die italienische Wettbewerbsbehörde AGCM, die feststellte, dass Google gegen Art 102 AEUV (missbräuchliche Ausnutzung einer beherrschenden Stellung auf dem Binnenmarkt) verstoßen hatte. Google legte gegen diese Entscheidung Rechtsmittel ein.

Das vorliegende Gericht fragte den EuGH, (i) ob ein Unternehmen verpflichtet ist, seine Erzeugnisse anzupassen oder neu zu entwickeln, um anderen Zugang zu gewähren, und (ii) ob es dabei die Marktanforderungen und Bedürfnisse des ersuchenden Unternehmens berücksichtigen muss, sowie ob (iii) der Zugang zu einem Erzeugnis für die Ausübung einer bestimmten Tätigkeit auf einem benachbarten Markt unerlässlich ist und (iv) ob missbräuchliches Verhalten angenommen werden kann, wenn das ersuchende Unternehmen und seine Wettbewerber trotz fehlenden Zugangs auf dem Markt tätig bleiben und wachsen.

Der EuGH hat erwogen: Art 102 AEUV verbietet die **missbräuchliche Ausnutzung** einer **beherrschenden Stellung** auf dem Binnenmarkt. Ein **Missbrauch** liegt vor, wenn ein Unternehmen in beherrschender Stellung den Zugang zu einer Infrastruktur verweigert, die für die Ausübung der Tätigkeit eines Wettbewerbers **unerlässlich** ist und keinen tatsächlichen oder potenziellen Ersatz hat. Google entwickelte Android Auto nicht ausschließlich für eigene Zwecke, sondern ermöglichte Drittunternehmen den Zugang. Daher ist die Voraussetzung der **Unerlässlichkeit** nicht anwendbar. Der Umstand, dass das Unternehmen und seine Wettbewerber auf dem Markt tätig blieben und ihre Stellung ausbauten, obwohl sie die **Interoperabilität** nicht nutzen konnten, bedeutet nicht, dass die Weigerung keine wettbewerbswidrigen Auswirkungen haben konnte. Es ist zu prüfen, ob das Verhalten von Google geeignet war, die Aufrechterhaltung oder Entwicklung des Wettbewerbs zu behindern. Google kann sich als **objektive Rechtfertigung** für die Weigerung darauf

berufen, dass es zum Zeitpunkt des Ersuchens kein Template gab, das die Interoperabilität gewährleistete, wenn die Interoperabilität die Integrität oder Sicherheit der Plattform gefährden würde oder aus technischen Gründen unmöglich wäre. Ist dies nicht der Fall, ist Google **verpflichtet**, ein solches **Template** innerhalb eines angemessenen Zeitraums und gegebenenfalls gegen eine angemessene finanzielle Gegenleistung **zu entwickeln**. Eine genaue Definition des sachlich und räumlich relevanten Marktes ist nicht erforderlich.

EuGH 27.02.2025, C-203/22, Dun & Bradstreet

#### **Automatisierte Entscheidungsfindung, Profiling, Auskunftsrecht, Geschäftsgeheimnis**

- Ein Mobilfunkanbieter verweigerte einer Betroffenen den Vertragsabschluss bzw. -verlängerung, weil sie laut einem Bonitätsscore, den der Mobilfunkanbieter von Dun & Bradstreet (D&B) erhielt, nicht kreditwürdig gewesen sein soll. Die DSB trug D&B aufgrund der Datenschutzbeschwerde der Betroffenen auf, aussagekräftige Informationen über die "involvierte Logik" zu übermitteln. D&B beschwerte sich beim BVwG und berief sich ua auf das Vorliegen eines Geschäftsgeheimnisses. Das BVwG entschied, dass die von D&B erteilte Auskunft nicht ausreichte, um die Betroffene in die Lage zu versetzen, nachzuvollziehen, wie ihr Bonitätsscore prognostiziert wurde. Nachdem das Erkenntnis rechtskräftig und **vollstreckbar** wurde, beantragte die Betroffene beim **Magistrat der Stadt Wien die Vollstreckung** des Erkenntnisses, dh die Ergänzung der Auskunft. Obwohl D&B nach Erlass des Erkenntnisses keine weitere Auskunft erteilt hatte, wurde dieser Vollstreckungsantrag mit der Begründung abgewiesen, dass D&B ihrer Auskunftspflicht bereits ausreichend nachgekommen sei. Die Betroffene erhob Bescheidbeschwerde an das LVwG Wien, das den EuGH um Vorabentscheidung ersuchte.

Der EuGH hat erwogen: Aus Art 15 Abs 1 lit h DSGVO ergibt sich ein **echtes Recht auf Erläuterung** der Funktionsweise des **Mechanismus** der automatisierten Entscheidungsfindung. Die Wortfolge "**aussagekräftige Informationen über die involvierte Logik**" einer automatisierten Entscheidungsfindung umfasst alle maßgeblichen Informationen zum **Verfahren** und zu den **Grundsätzen** der automatisierten Verarbeitung zwecks Erreichen eines bestimmten Ergebnisses. Die zu erteilende Information soll der Betroffenen insbesondere ermöglichen, die ihr nach Art 22 Abs 3 DSGVO zustehenden **Rechte auf Darlegung ihres eigenen Standpunkts** und auf **Anfechtung der Entscheidung** auszuüben.

Um zu gewährleisten, dass die Betroffene in die Lage versetzt wird, die ihr vom Verantwortlichen übermittelten Informationen in vollem Umfang zu verstehen, sind sie in **präziser, transparenter, verständlicher** und **leicht zugänglicher Form** in einer **klaren** und **einfachen Sprache** zu übermitteln.

Die DSGVO verlangt **keine ausführliche Erläuterung** der verwendeten **Algorithmen** oder die Offenlegung des gesamten Algorithmus. Die Übermittlung einer **komplexen mathematischen Formel** und die detaillierte Beschreibung jedes Schritts einer automatisierten Entscheidungsfindung sind keine ausreichend präzisen und verständlichen Erläuterungen. Der Verantwortliche sollte einfache Möglichkeiten finden, die Betroffene über die der Entscheidungsfindung zugrunde liegenden Überlegungen bzw Kriterien zu informieren. Beim **Profiling** könnte es ausreichend transparent und nachvollziehbar sein, darzulegen, in welchem Maße eine **Abweichung** bei den berücksichtigten personenbezogenen Daten zu einem **anderen Ergebnis** geführt hätte.

Die gemäß Art 15 Abs 1 lit h DSGVO zu erteilenden Informationen können zu einer **Beinträchtigung** der Rechte und Freiheiten **anderer Personen** führen, insbesondere, wenn sie durch die DSGVO geschützte personenbezogene Daten Dritter oder ein **Geschäftsgeheimnis** enthalten. Diesfalls sind diese Informationen der zuständigen Aufsichtsbehörde oder dem zuständigen Gericht zu übermitteln, die die einander gegenüberstehenden Rechte und Interessen abwägen müssen, um den **Umfang des Auskunftsrechts** zu ermitteln.

Die Anwendung einer nationalen Bestimmung wie **§ 4 Abs 6 DSG**, die das Auskunftsrecht der betroffenen Person grundsätzlich ausschließt, wenn die Auskunft ein Geschäfts- oder Betriebsgeheimnis gefährden würde, steht im Widerspruch zu Art 15 DSGVO. Die Abwägung der einander gegenüberstehenden Rechte und Interessen muss auf **Einzelfallbasis** erfolgen. **Anm: Geradezu in einem Nebensatz erklärt der EuGH die Bestimmung des § 4 Abs 6 DSG für unionsrechtswidrig. Spannend an diesem Fall ist, dass er bereits die Vollstreckung eines Erkenntnisses des BVwG betrifft. Die erstinstanzliche Vollstreckungsbehörde verweigerte die Vollstreckung mit dem Einwand, dass der Spruch des Erkenntnisses viel zu unpräzise sei. Die zweite Instanz holte zunächst ein technisches Gutachten ein und stellte dann unzählige Fragen an den EuGH. Nach dem Urteil des EuGH bleibt weiterhin unklar, was tatsächlich zu beauskunften ist (zB: "Der Verantwortliche sollte einfache Möglichkeiten finden").**

EuGH 27.02.2025, C-638/23, Amt der Tiroler Landesregierung

### **Rollenverteilung per Gesetz, öffentliche Stelle**

- Das Amt der Tiroler Landesregierung (Amt) versendete im Rahmen von Maßnahmen zur Bekämpfung der Covid-19-Pandemie Impferinnerungsschreiben an alle im Land Tirol wohnhaften volljährigen Personen, die noch nicht gegen das Virus geimpft waren. Zur Ermittlung der Adressaten beauftragte das Amt zwei private Unternehmen, die die Daten des **zentralen Impfreisters** mit jenen des **Patientenindex** abglichen. Einer der Adressaten reichte daraufhin eine Datenschutzbeschwerde bei der DSB ein, weil er die Verarbeitung seiner personenbezogenen Daten für unrechtmäßig hielt. Die DSB stellte fest, dass das Amt für das Impfreister und den Patientenindex nicht zugriffsberechtigt und die Verarbeitung daher rechtswidrig war. Das Amt erhob eine Bescheidbeschwerde an das BVwG, welche abgewiesen wurde. Daraufhin erhob das Amt Revision an den VwGH, der den EuGH fragte, ob das Amt durch die Bestimmung des § 2 Abs 1 lit a Tiroler Datenverarbeitungsgesetz ("TDVG") als "Verantwortlicher" iSd Art 4 Z 7 DSGVO gilt, obwohl es keine juristische Person ist und nur als Hilfsapparat des Landeshauptmanns an der Verarbeitung beteiligt war und keine Rechtspersönlichkeit und Rechtsfähigkeit hat.

Der EuGH hat erwogen: Der Begriff des **Verantwortlichen** iSd Art 4 Z 7 DSGVO umfasst natürliche oder juristische Personen, **Behörden**, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Nationale Regelungen können Verantwortliche festlegen, wenn die Zwecke und Mittel der Verarbeitung durch das nationale Recht vorgegeben sind. Die weite Definition des Begriffs "Verantwortlicher" soll einen wirksamen und umfassenden Schutz der Betroffenen gewährleisten.

Die Feststellung, ob eine Person oder Einrichtung als Verantwortliche einzustufen ist, erfordert die Prüfung, ob diese allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet oder ob ihre Rolle als Verantwortliche durch das nationale Recht vorgegeben ist. Eine **Stelle** kann auch dann als Verantwortliche eingestuft werden, wenn sie **keine Rechtspersönlichkeit** besitzt, solange sie über eine gewisse **Entscheidungs- und Handlungsfähigkeit** bei der Verarbeitung personenbezogener Daten verfügt. Die Verantwortliche muss die rechtlichen Verpflichtungen erfüllen können, die die DSGVO auferlegt, unabhängig davon, ob die Stelle **Rechtspersönlichkeit** und eine **eigene Rechtsfähigkeit** hat. Die **unmittelbare Benennung** einer



Stelle als Verantwortliche ist **rechtswirksam**, wenn die nationale Regelung den Umfang der Verarbeitung personenbezogener Daten vorgibt. Es ist jedoch **nicht erforderlich**, dass der Gesetzgeber **alle Verarbeitungsvorgänge abschließend aufzählt**. Eine nationale Regelung, die eine Stelle als Verantwortliche benennt, ist mit Art 4 Z 7 DSGVO vereinbar, wenn diese Regelung **explizit** oder **implizit** den Umfang der Verarbeitung personenbezogener Daten vorgibt.

Eine nach nationalem Recht als Verantwortliche **benannte Stelle** muss nicht selbst über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden, um als Verantwortliche Anfragen beantworten zu müssen, die Betroffenen aufgrund ihrer Rechte aus der DSGVO an sie richten. Die **Rechtswirksamkeit** einer unmittelbaren Benennung wird nicht dadurch berührt, dass die benannte Stelle keine Kontrolle über die personenbezogenen Daten ausübt, die sie zu verarbeiten hat. Daher steht Art 4 Z 7 DSGVO einer nationalen Regelung, in der als Verantwortliche ein **Hilfsapparat** der Verwaltung benannt ist, der keine Rechtspersönlichkeit und keine eigene Rechtsfähigkeit hat, nicht entgegen, sofern diese Stelle die Pflichten eines Verantwortlichen erfüllen kann und die nationale Regelung den Umfang der Verarbeitung personenbezogener Daten vorgibt, für die diese Stelle verantwortlich ist.

EuGH SA 27.02.2025, C-57/23, *Policejní prezidium*

### **Biometrische und genetische Daten, DSRL-PJ, Recht der Mitgliedstaaten**

- In einem Ermittlungsverfahren wurden von einer Verdächtigen genetische Daten durch einen Mundhöhlenabstrich erhoben. Das geltende tschechische Recht erlaubte diese Maßnahme bei Personen, die einer Vorsatztat beschuldigt oder verdächtigt wurden, unabhängig von der Strafhöhe. Eine Höchstspeicherungsdauer der erhobenen Daten war nicht festgelegt. Das vorliegende Gericht fragte den EuGH, (i) ob die in der Richtlinie 2016/680 (**DSRL-PJ**) festgelegten Anforderungen eine undifferenzierte Erhebung biometrischer und genetischer Daten erlauben, (ii) ob für die Speicherung eine feste zeitliche Beschränkung vorgesehen sein muss und (iii) ob Rechtsprechung nationaler Verwaltungsgerichte als "Recht der Mitgliedstaaten" zu verstehen ist.

Der Generalanwalt hat erwogen: Die Kriterien für die Bewertung der Erforderlichkeit einer Datenverarbeitung nach Art 10 der DSRL-PJ sind die Art und Schwere der mutmaßlichen Straftat, die besonderen Umstände der Straftat, der Zusammenhang der Tat mit laufenden Verfahren sowie die Vorstrafen oder das individuelle Profil der

Betroffenen. Eine Regelung, welche die Erhebung **biometrischer und genetischer Daten** aller Personen erlaubt, die beschuldigt oder verdächtigt werden, eine vorsätzliche Straftat begangen zu haben, ist unzulässig, wenn keine **Einzelfallprüfung** der unbedingten Erforderlichkeit der Datenverarbeitung vorgesehen ist.

Nach der DSRL-PJ sind keine fest definierten **Löschfristen** erforderlich, eine periodische Überprüfung der Notwendigkeit der Speicherung von Daten reicht aus. Zusätzlich zu der periodischen Überprüfung brauchen Betroffene das Recht, **Auskunft** über die Dauer, oder die Kriterien für die Festlegung der **Dauer der Datenspeicherung** zu erhalten, um ihre Betroffenenrechte ausüben zu können. Für die Speicherung **biometrischer und genetischer Daten** müssen Bestimmungen klare und deutliche Zwecke enthalten, um die **Zweckerreichung** und damit den **Löschzeitpunkt** ableiten zu können. **Kriterien zur Beurteilung** der Speicherdauer sind die Art und Schwere des Sachverhalts, die verstrichene Zeit, die verbleibende gesetzliche Aufbewahrungsfrist, die Höhe des Risikos weiterer Straftaten, der Kontext der Straftat, ein Zusammenhang mit anderen laufenden Verfahren oder die Vorgeschichte und das Profil der Betroffenen.

**Rechtsprechung von Mitgliedstaaten** ist, wenn sie zugänglich, vorhersehbar und konstant ist sowie hinreichende materielle Charakteristika aufweist, als "**Recht der Mitgliedstaaten**" iSd DSRL-PJ zu sehen. Dennoch reicht auch eine **Rechtsprechung**, die eine **ständige Verwaltungspraxis** bestätigt, nicht aus, um an die Stelle einer allgemein geltenden Vorschrift zu treten. Denn bei der Verarbeitung **besonders sensibler Daten** müssen hinreichend strenge Garantien in einem verbindlichen und in der Anwendung vorhersehbaren Rechtsakt, der im Bereich der Verarbeitung dieser Daten maßgebend ist, festgelegt sein. **Anm: Der Generalanwalt spricht bei biometrischen und genetischen Daten von einer besonderen Sensibilität. Sollte der EuGH sich dieser Ansicht anschließen, entsteht eine Rangordnung zwischen den sensiblen Datenkategorien.**

### **Rechtsprechung der Justiz**

Aus der Rechtsprechung der Justiz:

- Der Tatverdacht zum Vorwurf des Überlassens von Suchtgift stützte sich nicht auf die Auswertung der **SKY ECC-Chatprotokolle (Auswertung eines Mobiltelefons)**, sondern auf belastende Angaben der Suchtmittelabnehmer und die Sicherstellung von Suchtgift. Da somit bereits ein dringender Verdacht auf erheblichen Suchtgifthandel bestand, fehlte es der Grundrechtsbeschwerde an einer hinreichenden

Begründung für einen Beweisverwertungsmangel und einer Verletzung des Grundrechts auf persönliche Freiheit lag nicht vor. Mit der Behauptung einer Verletzung der Grundrechte auf ein **faïres Verfahren** gemäß Art 6 EMRK und auf **Schutz der Privatsphäre** gemäß Art 8 EMRK durch die Verwertung von SKY ECC-Chats wird keine Garantie des **Grundrechts auf persönliche Freiheit** gemäß Art 5 EMRK thematisiert und solcherart der Anfechtungsrahmen einer **Grundrechtsbeschwerde** verlassen ([OGH 18.02.2025, 14Os11/25m](#)).

### Rechtsprechung des BVwG

BVwG 28.01.2025, W108 2286343-1

#### **Identifikationsregister, e-Card, Auskunft, Verantwortliche**

- Einer Betroffenen wurde eine neue **e-Card** mit **aufgebrachtem Lichtbild** zugesandt. Die **Polizei** führte während eines Verwaltungsstrafverfahrens eine Abfrage des Lichtbilds des Reisepasses der Betroffenen durch. Beide Abfragen erfolgten aus dem **Identifikationsregister ("IDR")**, das von den **Passbehörden** als **Gemeinsam Verantwortliche** betrieben wird. Die Betroffene stellte ein Auskunftersuchen an die zuständige Passbehörde. In der erteilten Auskunft schienen weder der **Hauptverband der Sozialversicherungsträger** noch die **Polizei** als **Empfänger** auf.


Die Betroffene erachtete sich in ihrem **Recht auf Auskunft** verletzt und brachte gegen die zuständige Passbehörde eine Datenschutzbeschwerde bei der DSB ein. Diese gab der Datenschutzbeschwerde teilweise (aber aus anderen Gründen) statt und stellte ua fest, dass die Passbehörde nur unvollständige Auskunft über konkret verarbeitete (Stamm-)Daten erteilt hat. Im Übrigen wurde die Datenschutzbeschwerde abgewiesen. Dagegen erhob die Betroffene (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die Passbehörden stellen nur die Infrastruktur zur Verfügung, um Abfragen aus dem IDR zu ermöglichen. Die **Sicherheitsbehörden** und der **Dachverband der österreichischen Sozialversicherungsträger** sind **selbständige Verantwortliche**. Sie haben eine automatische Zugriffsmöglichkeit auf Daten des IDR, die an keine Zustimmung und keinen Verarbeitungsvorgang innerhalb der Passbehörde geknüpft ist. Eine gemeinsame Verantwortlichkeit mit den Passbehörden besteht nicht. Vielmehr hatten Bedienstete der Sicherheitsbehörden bzw Mitarbeiter des Dachverbands der Sozialversicherungsträger für ihre jeweilige Behörde gewisse Abfragen aus dem IDR hinsichtlich des Lichtbilds der Betroffenen zu tätigen. Mangels **Verantwortlicheneigenschaft** der zuständigen Passbehörde war die

erteilte Auskunft in dieser Hinsicht nicht mangelhaft.

#### Aus der weiteren Rechtsprechung des BVwG:

- Entspricht ein Verantwortlicher im Laufe des Verfahrens vor dem BVwG einem **Löschungersuchen**, wird der Betroffene dadurch **klaglos** gestellt und ist das Verfahren einzustellen. Ein Recht auf **Feststellung einer Rechtsverletzung in der Vergangenheit** besteht nicht. Dem Betroffenen ist auch **kein subjektives öffentliches Recht** eingeräumt, ein **allgemeines rechtliches Interesse** durchzusetzen ([BVwG 31.01.2025, W258 2247059-1](#)).
- Bestimmt die DSB irrtümlich den falschen **Beschwerdegegner** als Verantwortlichen, ist der Bescheid ersatzlos zu beheben. Wird ein Sachverhalt sowohl von einem Betroffenen als auch von der DSB aufgegriffen, um in einem Verfahren überprüft zu werden, führt dies zu **keiner res iudicata** ([BVwG 28.01.2025, W252 2271493-1](#); [W252 2271450-1](#)).
- Sind vor dem BVwG eine **erhebliche Anzahl** von Verfahren anhängig, in welchen dieselbe(n) Rechtsfrage(n) zu beantworten sind, die über eine Revision auch beim VwGH anhängen, kann das BVwG diese **Verfahren** mit Beschluss **aussetzen** ([BVwG 29.01.2025, W171 2262672-1](#); [W171 2262379-1](#)).



to the point

# Datenschutzmonitor. 10/2025 vom 12.03.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung der Justiz**

OGH 29.01.2025, 12Os79/24w (Sicherstellung personenbezogener Daten, Einspruch nach § 106 StPO)

OLG Graz 19.12.2024, 2R192/24h (Auskunftersuchen, Identitätsnachweis, Vollmacht)

- **Rechtsprechung des BVwG**

BVwG 05.02.2025, W291 2298821-1 (Geldbuße, veröffentlichte Gesundheitsdaten, Rechtsanspruch, Weiterverarbeitung)

BVwG 30.01.2025, W101 2248744-1 (berechtigtes Interesse, Identifizierbarkeit, Grundbuch)

BVwG 30.01.2025, W101 2248650-1 (berechtigtes Interesse, Erforderlichkeit)

- **Rechtsprechung der LVwG**

LVwG Tirol 20.02.2025, LVwG-2024/44/2718-6 (Wassergenossenschaft, Mitgliederverzeichnis, Vertragserfüllung)

- **EU-Rechtsakte**

VO (EU) 2025/327 über den europäischen Gesundheitsdatenraum

- **Nationale Rechtsakte**

Transparenzdatenbank-Abfrageverordnung

Änderung der Verordnung über den elektronischen Rechtsverkehr (ERV 2021)

## To the Point:

### Rechtsprechung der Justiz

OGH 29.01.2025, 12Os79/24w

#### **Sicherstellung personenbezogener Daten, Einspruch nach § 106 StPO**

- Die Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption (**WKStA**) führte ein Ermittlungsverfahren wegen verschiedener Straftaten gegen zwei **Amtsträger**. Die WKStA richtete eine **Sicherstellungsanordnung** an das Bundesamt für Korruptionsbekämpfung (**BAK**) und ordnete die Sicherstellung folgender Gegenstände an: Innerhalb eines näher umschriebenen Zeitraums die E-Mail-Postfächer, eOffice-Dokumente, sonstige Co-Working-Spaces sowie Laufwerke samt Backups und Sicherungskopien sämtlicher Mitarbeiter des Bundeskanzleramtes (**BKA**) in den Bereichen Öffentlichkeitsarbeit, Informationstätigkeit und Kabinett des Bundeskanzlers.

Die Republik Österreich, vertreten durch die **Finanzprokurator**, erhob Einspruch gemäß § 106 Abs 1 StPO und beantragte die Aufhebung der Sicherheitsanordnung, ua weil eine Vielzahl privater und sensibler Daten betroffen wären. Das LG für Strafsachen Wien wies den Einspruch ab. Das OLG Wien gab der dagegen erhobenen Beschwerde zwar keine Folge, erklärte den Einspruch aber grundsätzlich für zulässig. Daraufhin erhob die **Generalprokurator** eine (erfolglose) **Nichtigkeitsbeschwerde zur Wahrung des Gesetzes** an den OGH.

Der OGH hat erwogen: Der Begriff des "subjektiven Rechts" iSd hier relevanten § 106 Abs 1 Z 2 StPO stellt auf eine **Kontrolle von Grundrechten** und darauf ab, dass der Einspruchswerber sich selbst **unmittelbar** in einem subjektiven Recht verletzt erachtet.

Im **Hoheitsvollzug** sind **staatliche Organe keine Grundrechtsträger**, sondern allein grundrechtsverpflichtet. Der Bund kann aber nach Art 17 B-VG (Privatwirtschaftsverwaltung) **Träger von Privat-rechten** sein, womit ihm auch als Rechtsunterworfenen die Ausübung von subjektiven Rechten zur Kontrolle von Grundrechten zustehen kann.

Die Vorinstanzen haben keine Aussage darüber getroffen, in Erfüllung welcher staatlicher Aufgabe das BKA oder der Bund den **Gewahrsam** an den von der Sicherstellungsanordnung **umfassten Daten** begründet haben. Die Generalprokurator machte jedoch keine entsprechenden Feststellungs- oder Begründungsmängel geltend, daher ist kein Gesetzesverstoß bei der Annahme der Zulässigkeit des vorliegenden Einspruchs auszumachen.

### Aus der weiteren Rechtsprechung der Justiz:

- Richtet ein Rechtsanwalt für seinen Mandanten ein **Auskunftsersuchen** an einen Verantwortlichen, reicht eine **elektronisch signierte Vollmacht** gemeinsam mit einer **Kopie des Personalausweises** des Mandanten als **Identitätsnachweis** aus. Für den Abschluss eines Bevollmächtigungsvertrags gelten keine besonderen Formvorschriften, sodass die Vorlage einer vom Mandanten handschriftlich mit Tinte unterfertigten Vollmacht nicht gefordert werden darf ([OLG Graz 19.12.2024, 2R192/24h](#)).

### Rechtsprechung des BVwG

BVwG 05.02.2025, W291 2298821-1

#### **Geldbuße, veröffentlichte Gesundheitsdaten, Rechtsanspruch, Weiterverarbeitung**

- Eine Patientin verfasste eine negative Rezension über einen Facharztbesuch auf Google, in der sie auch ihr Krankheitsbild offenlegte. In seiner Antwort veröffentlichte der Facharzt **zusätzlich** die **Diagnose der Patientin** ("Reizung eines Sehnenansatzes"). Die DSB sah darin einen Verstoß gegen Art 9 Abs 1 DSGVO sowie gegen die Grundsätze der Verarbeitung gemäß Art 5 Abs 1 lit a, b und c DSGVO. Sie verhängte eine Geldstrafe iHv EUR 4.000. Daraufhin erhob der Facharzt (eine der Höhe nach teilweise erfolgreiche) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die Information betreffend die **medizinische Diagnose** der Patientin ist ein **Gesundheitsdatum iSd Art 4 Z 15 DSGVO**.

Eine auf Google veröffentlichte Rezension erfüllt die geforderte Öffentlichkeit iSd Ausnahmetatbestands nach **Art 9 Abs 2 lit e DSGVO**. Der Schutz besonderer Kategorien personenbezogener Daten iSd Art 9 Abs 2 lit e DSGVO entfällt nur dann, wenn die Betroffene **das sensible Datum (offensichtlich) selbst veröffentlicht hat**. Der Ausnahmetatbestand iSd **Art 9 Abs 2 lit f DSGVO** setzt voraus, dass ein rechtlicher Konflikt bereits besteht. Dieser **Ausnahmetatbestand** greift somit nur, soweit sich die Datenverarbeitung auf **von der Betroffenen veröffentlichte Daten bezieht**. Der Facharzt ergänzte jedoch die von der Patientin selbst veröffentlichten Gesundheitsdaten um weitere Informationen (die Diagnose) und generierte dadurch einen **informationellen Mehrwert**.

Die Verarbeitung kann, solange die Möglichkeit einer abstrakten rechtlichen Auseinandersetzung bloß **abstrakt** besteht, auch nicht auf Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen gestützt werden (Art 9 Abs 2 lit f DSGVO).

Da der Facharzt die **Diagnose** der Patientin im Rahmen seiner ärztlichen Tätigkeit

erstellte und die Daten nur dafür erhoben wurden, **verstieß er gegen den Grundsatz der Zweckbindung** (Art 5 Abs 1 lit b DSGVO). Zudem lag **keine** konkrete, kohärente oder ausreichend enge **Verbindung** zwischen dem **ursprünglichen Zweck der Datenerhebung und der Weiterverarbeitung der Daten** vor. Weiters war es für die Patientin **nicht vorhersehbar**, dass der Facharzt Daten zu ihrer medizinischen Diagnose als Reaktion auf ihre Google-Rezension veröffentlichen wird. Darüber hinaus verstieß die Veröffentlichung gegen den Grundsatz der **Datenminimierung** nach Art 5 Abs 1 lit c DSGVO, weil es dem Facharzt möglich gewesen wäre, seine **Sichtweise auch ohne die Preisgabe der Diagnose** darzulegen.

Die **Geldstrafe** war dennoch auf **EUR 3.000 herabzusetzen**, weil gegen den Facharzt keine einschlägigen Vorstrafen vorlagen, der Facharzt seine Antwort gelöscht hatte und seine persönlichen Verhältnisse zu berücksichtigen waren.

BVwG 30.01.2025, W101 2248744-1

#### **Berechtigtes Interesse, Identifizierbarkeit, Grundbuch**

- Eine Marktgemeinde und zwei Anrainer der Gemeinde führten aufgrund einer Meinungsverschiedenheit ein Zivilverfahren vor dem Bezirksgericht ("**BG**"), wobei einer der Anrainer auf einer mit dem Bürgermeister konkurrierenden Parteiliste stand. Die Marktgemeinde veröffentlichte in Folge ein Anwaltschreiben und den Beschluss des BG auf ihrer Website unter der Rubrik "**Amtstafel**". Diese Dokumente enthielten die Namen, Geburtsdaten, Anschriften und Grundstücksnummern der Anrainer. Nachdem die Anrainer die Löschung ihrer Daten forderten, schwärzte die Marktgemeinde die Namen, Geburtsdaten und Anschriften, veröffentlichte die Dokumente jedoch weiterhin unter der Rubrik "Aktuelles" mit sichtbaren Grundstücksnummern. Da sich die Anrainer dadurch in ihrem Recht auf Geheimhaltung verletzt sahen, brachten sie eine Datenschutzbeschwerde bei der DSB ein, die eine Verletzung des Rechts auf Geheimhaltung durch die Marktgemeinde feststellte. Die Bescheidbeschwerde der Marktgemeinde an das BVwG blieb erfolglos.

Das BVwG hat erwogen: Die Veröffentlichung bzw Offenlegung von Daten im Internet auf einer frei aufrufbaren Website ist eine **Datenverarbeitung** iSd Art 4 Z 2 DSGVO. Die Marktgemeinde ist **Verantwortliche** iSd Art 4 Z 7 DSGVO, weil sie über die Mittel und Zwecke der Verarbeitung entschieden hat.

Eine Verarbeitung personenbezogener Daten kann etwa zur **Wahrung berechtigter Interessen** des Verantwortlichen oder eines

Dritten zulässig sein (Art 6 Abs 1 lit f DSGVO). Die Verarbeitung muss aber **erforderlich** sein und sich auf das **absolut Notwendige beschränken**.

Die Marktgemeinde verfolgte ein berechtigtes Interesse an der Information der Öffentlichkeit bzw der Gemeindebewohner über Ereignisse eines Verfahrens im Zusammenhang mit der Gemeinde. Die Marktgemeinde hätte ihr Ziel jedoch auch mit einer von vornherein vollständig **geschwärzten Version** der Dokumente erreichen können.

Auch die Veröffentlichung der Dokumente mit geschwärzten Namen, Geburtsdaten und Anschriften, aber sichtbaren **Grundstücksnummern, verletzt das Recht auf Geheimhaltung** der Anrainer. Denn eine Person ist **identifizierbar**, wenn die Information dieser Person zugeordnet werden kann, sobald sie mit weiteren Informationen verknüpft wird. Der Begriff "Informationen" ist weit zu verstehen. Auch sachliche Informationen, wie Vermögens- und Eigentumsverhältnisse werden davon umfasst. Eine Abfrage des **Grundbuchs** ist einfach und kostengünstig möglich, wodurch die Identifizierung der Anrainer durch die **Grundstücksnummern** erleichtert wird. Die Grundstücksnummern im Beschluss des BG wurden mit einem Schreiben einer Rechtsanwaltskanzlei kombiniert und waren personenbezogene Daten. Die Marktgemeinde hat zwar ein berechtigtes Interesse, jedoch war die ungeschwärzte Veröffentlichung nicht erforderlich.

BVwG 30.01.2025, W101 2248650-1

#### **Berechtigtes Interesse, Erforderlichkeit**

- Ein Anrainer brachte eine Klage wegen einer Meinungsverschiedenheit gegen seine Marktgemeinde beim BG ein. Die Marktgemeinde veröffentlichte in Folge den Beschluss des BG samt Namen, Geburtsdatum und Anschrift des Anrainers auf ihrer Website jeweils unter der Rubrik "Aktuelles" und "Gemeindezeitung". Der Anrainer erhob daraufhin eine Datenschutzbeschwerde bei der DSB. Nachdem die DSB der Datenschutzbeschwerde stattgab, erhob die Marktgemeinde eine (teilweise erfolgreiche) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Der Gegenstand eines Verwaltungsverfahrens wird inhaltlich grundsätzlich durch die Begründung des Antrags festgelegt, mit dem das Verwaltungsverfahren eingeleitet wird. Da der Sachverhalt hinsichtlich der Veröffentlichung unter der Rubrik "Aktuelles" bereits teilweise **Gegenstand eines anderen** bei der DSB abhängigen **Verwaltungsverfahrens** war (siehe oben: BVwG 30.01.2025, W101 2248744-1), hätte die DSB über diesen Sachverhalt nicht absprechen dürfen. Der

Bescheid der DSB war daher in diesem Umfang aufzuheben.

Die Marktgemeinde verfolgte ein **berechtigtes Interesse** an der Information der Öffentlichkeit bzw der Gemeindebewohner über Ereignisse im Zusammenhang mit der Gemeinde. Die Kandidatur des Anrainers kann jedoch nicht bereits als Betreten der politischen Bühne gewertet werden. Es fehlt zudem am notwendigen Bekanntheitsgrad.

Vor diesem Hintergrund ergeben sich keine Gründe, welche die Anwendung eines **veränderten Maßstabs** an das Interesse des Anrainers betreffend die Geheimhaltung seiner personenbezogenen Daten rechtfertigen würde. Da die Marktgemeinde ihr Ziel auch ohne die namentliche Nennung des Anrainers hätte erreichen können, war die Veröffentlichung des Namens **nicht erforderlich**. Die Veröffentlichung des Namens, Geburtsdatums und der Adresse des Anrainers auf der Website der Marktgemeinde war daher rechtswidrig.

### Rechtsprechung der LVwG

Aus der Rechtsprechung der LVwG

- Die **Mitglieder einer Wassergenossenschaft** haben das **Recht**, die **anderen Genossenschaftsmitglieder zu kennen**. Die **Herausgabe personenbezogener Daten** eines Genossenschafters an einen anderen Genossenschaftler ist vom Erlaubnistatbestand des Art 6 Abs 1 lit b DSGVO (**Verpflichtung zur Vertragserfüllung**) gedeckt. Daher hat eine Wassergenossenschaft ihren Mitgliedern Einsicht in das **Mitgliederverzeichnis samt Adressen, einbezogener Liegenschaften und Stimmrechten** zu gewähren ([LVwG Tirol 20.02.2025, LVwG-2024/44/2718-6](#)).

### EU-Rechtsakte

- Am **05.03.2025** wurde die "*VO (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen **Gesundheitsdatenraum** sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847*", [ABl L 2025/327](#), kundgemacht. Diese VO präzisiert ua die in der DSGVO festgelegten Rechte natürlicher Personen bei **der Primär- und Sekundärnutzung ihrer personenbezogenen elektronischen Gesundheitsdaten**. Ziel der VO ist, den Zugang natürlicher Personen zu ihren personenbezogenen elektronischen Gesundheitsdaten zu verbessern.

### Nationale Rechtsakte

- Am **28.02.2025** wurde die "*Änderung der Verordnung über den elektronischen*

*Rechtsverkehr (ERV 2021)*", [BGBl II 2025/27](#), kundgemacht. Die Änderungen der ERV betreffen etwa **Grundbuchverfahren** und die **E-ID**.

- Am **03.03.2025** wurde "*die **Transparenzdatenbank-Abfrageverordnung 2025***", [BGBl II 2025/41](#), kundgemacht. Geregelt werden darin die **Leseberechtigungen** in Leistungsangebote mit besonderen Kategorien personenbezogener Daten ("**sensible Daten**") in der Transparenzdatenbank.

to the point

# Datenschutzmonitor. 11/2025 vom 19.03.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH 13.03.2025, C-247/23, *Deldits* (Berichtigung, öffentliches Register, Geschlechtseintrag, Transidentität, Nachweis)

- **Rechtsprechung des VwGH**

VwGH 10.12.2024, Ro 2021/04/0022 (Suchmaschine, Unterlassungsanspruch, Löschung, De-Indexierung, Informationsfreiheit)

- **Rechtsprechung der Justiz**

OGH 18.02.2025, 6Ob102/24d (Vorabentscheidungsersuchen, Verantwortliche, Datenherkunft, Schadenersatz, Amtshaftung)

OGH 18.02.2025, 6Ob137/24a (Auskunft, Schadenersatz, Aussetzung)

OLG Innsbruck 08.01.2025, 4R136/24t (Personenbezug, Zuordnung, Differenzgeschäfte)

OLG Linz 05.03.2025, 2R32/25a (Auskunft, Vollmacht, Kostenersatz)

- **Rechtsprechung der LVwG**

LVwG NÖ 01.12.2023, LVwG-M-55/001/2022 (Unzuständigkeit)

- **EU-Rechtsakte**

DelegierteVO (EU) 2025/416 (Handelsplattformen für Kryptowerte, Auftragsbuchaufzeichnungen)

DelegierteVO (EU) 2025/417 (Handelsplattformen für Kryptowerte, Transparenz)

Entwurf einer DurchführungsVO zur Cyberresilienz-Verordnung samt Anhängen

## To the Point:

### Rechtsprechung des EuGH

EuGH 13.03.2025, C-247/23, Deldits

#### **Berichtigung, öffentliches Register, Geschlechtseintrag, Transidentität, Nachweis**

- Ein iranischer Staatsangehöriger erhielt in Ungarn die Flüchtlingseigenschaft zuerkannt. In den ärztlichen Attesten, die er zur Stützung seines Antrags vorgelegt hatte, wurde bescheinigt, dass er als Frau geboren wurde, aber eine männliche Geschlechtsidentität hat. Dennoch wurde der Asylberechtigte im **Flüchtlingsregister** als Frau eingetragen. Im Jahr 2022 beantragte der Asylberechtigte bei der zuständigen Ausländerbehörde gemäß Art 16 DSGVO die Berichtigung seines Geschlechtseintrags sowie die Änderung seines Vornamens im Flüchtlingsregister. Die Behörde lehnte den Antrag ab, weil der Asylberechtigte keine geschlechtsangleichende Operation nachweisen konnte. Das vorliegende Gericht stellte dem EuGH mehrere Fragen iZm der Auslegung von Art 16 DSGVO, ua zur Notwendigkeit eines Nachweises für den Berichtigungsantrag und zur Anforderung einer geschlechtsangleichenden Operation.

Der EuGH hat erwogen: Gemäß **Art 16 DSGVO** hat der Betroffene das Recht, von dem Verantwortlichen unverzüglich die **Berichtigung** ihn betreffender unrichtiger personenbezogener Daten zu verlangen. Weiters ist auch der **Grundsatz der Datenrichtigkeit** (Art 5 Abs 1 lit d DSGVO) zu beachten, wonach die verarbeiteten Daten sachlich richtig und **erforderlichenfalls** auf dem **neuesten Stand** sein müssen. Die **Richtigkeit** und Vollständigkeit personenbezogener Daten sind nach dem **Zweck** zu beurteilen, für den die Daten erhoben wurden.

Da Ungarn bereits im Asylverfahren anerkannt hatte, dass der Betroffene eine transgeschlechtliche Person ist, war die im Flüchtlingsregister enthaltene Angabe zur **Geschlechtsidentität bereits zum Zeitpunkt ihrer Eintragung unrichtig**. Ein Mitgliedstaat kann sich **nicht** auf spezifische, auf der Grundlage von Art 6 Abs 2 und 3 DSGVO erlassene nationale **Bestimmungen berufen, um das Recht auf Berichtigung zu verweigern**. Diese Bestimmungen dienen nur dazu, die Anwendung der Vorschriften der DSGVO **genauer festzulegen**, nicht aber dazu, von ihnen abzuweichen.

Ein Mitgliedstaat kann das Recht auf Berichtigung auch nicht mit der Begründung verweigern, dass es in seinem nationalen Recht kein Verfahren zur rechtlichen Anerkennung von **Transidentität** gibt. Somit ist eine nationale Regelung, die einer transgeschlechtlichen Person wegen fehlender Anerkennung ihrer Geschlechtsidentität **den Zugang zu einem unionsrechtlich geschützten**

**Anspruch verwehrt**, mit dem **Unionsrecht unvereinbar**. Folglich ist Art 16 DSGVO dahingehend auszulegen, dass eine **nationale Behörde**, die ein **öffentliches Register** führt, personenbezogene Daten zur **Geschlechtsidentität berichtigen muss**.

Der Betroffene kann verpflichtet sein, **Nachweise** vorzulegen, die vernünftigerweise verlangt werden können, um die Unrichtigkeit der Daten festzustellen. Ein Mitgliedstaat darf das **Recht auf Berichtigung** jedoch nur unter Beachtung von **Art 23 DSGVO beschränken**.

Eine **Verwaltungspraxis**, wonach eine transgeschlechtliche Person ihr Recht auf **Berichtigung** der Geschlechtsidentität in einem **öffentlichen Register** nur ausüben kann, wenn sie eine **geschlechtsangleichende Operation nachweist**, ist mit Art 16 DSGVO unvereinbar. Darüber hinaus beeinträchtigt eine solche Verwaltungspraxis den **Wesensgehalt der Grundrechte auf Unversehrtheit** (Art 3 der EU-Grundrechtecharta; **GRC**) und **auf Achtung des Privatlebens** (Art 7 GRC). Nach der Rsp des EGMR darf die Anerkennung der Geschlechtsidentität einer transgeschlechtlichen Person nicht davon abhängig gemacht werden, dass sich diese Person entgegen ihrem Wunsch einer Operation unterzieht.

### Rechtsprechung des VwGH

VwGH 10.12.2024, Ro 2021/04/0022

#### **Suchmaschine, Unterlassungsanspruch Löschung, De-Indexierung, Informationsfreiheit**

- Ein ehemaliger österreichischer Dienstnehmer eines international führenden Investmentbanking- und Wertpapierhandelsunternehmens in London wurde beschuldigt, eine Frau vergewaltigt zu haben. Er wurde jedoch im Strafverfahren von allen Vorwürfen freigesprochen. Mehrere Medien im Vereinigten Königreich berichteten über den Vorwurf und das Strafverfahren unter Nennung seines vollen Namens. Die Berichte erschienen auch in der **Ergebnisliste einer Suchmaschine**, die von einer Suchmaschinenbetreiberin mit Sitz in den USA betrieben wird. Der Dienstnehmer erhob bei der DSB eine Datenschutzbeschwerde gegen diese Suchmaschinenbetreiberin und zwei ihrer Tochtergesellschaften wegen Verletzung seines Rechts auf Löschung gemäß Art 17 DSGVO und seines Rechts auf Geheimhaltung gemäß § 1 DSG. Er beantragte unter anderem die Entfernung der Suchergebnisse und die Unterlassung der neuerlichen Indexierung dieser und sinngleicher Inhalte. Nachdem die DSB die Datenschutzbeschwerde abwies, erhob der Dienstnehmer eine (erfolglose) Bescheidbeschwerde beim BVwG. Die gegen das



Erkenntnis des BVwG gerichtete Revision des Dienstnehmers war teilweise erfolgreich.

Der VwGH hat erwogen: Das **Recht auf Löschung** umfasst das Recht auf dauerhafte Löschung, dh das Recht, dass die gelöschten bzw zu löschenden Daten, solange deren Verarbeitung eine Verletzung des Schutzes personenbezogener Daten darstellt, gelöscht bleiben.

Die bloße Löschung unrechtmäßig verarbeiteter Daten beseitigt die Rechtsverletzung nicht vollständig, wenn die Gefahr besteht, dass die Daten erneut vom Verantwortlichen unrechtmäßig verarbeitet werden. Einem Betroffenen steht daher bei Vorliegen von **Wiederholungsgefahr** neben dem Lösungsanspruch auch ein **Unterlassungsanspruch** zu. Da vom BVwG nicht klar festgestellt wurde, ob die URL trotz zwischenzeitiger Auslistung in Zukunft wieder online gestellt und in weiterer Folge die ausgelisteten Suchergebnisse wieder gelistet werden könnten, wurde das Unterlassungsbegehren aufgrund eines **sekundären Feststellungsmangels** fälschlich abgewiesen.

Das **Recht auf Vergessenwerden** gemäß Art 17 Abs 3 lit a DSGVO kann eingeschränkt werden, wenn die neuerliche Indexierung bereits ausgelisteter Suchergebnisse unter anderem zur **Ausübung des Rechts auf Informationsfreiheit iSd Art 11 GRC** erforderlich ist. Es bedarf einer **Abwägung** zwischen den Grundrechten auf Achtung des Privatlebens und auf Schutz personenbezogener Daten einerseits und dem Recht auf Informationsfreiheit andererseits unter Berücksichtigung der Umstände des Einzelfalls. Dabei sind einige **wesentliche Kriterien** wie etwa der **Beitrag zu einer Debatte** von allgemeinem Interesse und der **Bekanntheitsgrad** der Betroffenen zu beachten. Insbesondere dann, wenn die Betroffene im **öffentlichen Leben** eine Rolle spielt, muss sie ein höheres Maß an Toleranz aufbringen, weil sie in diesem Fall zwangsläufig und bewusst im Blick der Öffentlichkeit steht.

Im Rahmen der **Interessenabwägung** ist zu beachten, dass der Dienstnehmer von dem Vorwurf des sexuellen Missbrauchs **rechtskräftig freigesprochen** wurde und bereits erhebliche wirtschaftliche und soziale Nachteile nicht auszuschließen sind. Da der Dienstnehmer erst durch die Berichterstattung über das gegen ihn anhängige Strafverfahren einer breiten Öffentlichkeit bekannt wurde, ist seine berufliche und soziale Stellung im Rahmen der Interessenabwägung daher besonders zu berücksichtigen.

Die DSB hat bei Feststellung einer Verletzung des Schutzes personenbezogener Daten geeignete, erforderliche und verhältnismäßige Abhilfemaßnahmen zu ergreifen. Dazu werden in Art 58 Abs 2 DSGVO verschiedene Abhilfebefugnisse aufgezählt. Der Betroffenen steht jedoch **kein subjektives**

**Recht** auf eine **bestimmte Abhilfemaßnahme** zu. Die DSB hat unter Berücksichtigung aller Umstände des Einzelfalls das geeignete Mittel zu wählen. Der Dienstnehmer hat neben dem Recht auf Löschung also kein Recht auf Ergreifen einer bestimmten Abhilfemaßnahme.

Während 18 der 24 URL von der Suchmaschinenbetreiberin **gelöscht** wurden, weigerte sich die Suchmaschinenbetreiberin, sechs weitere URL auszulisten. Diese wurden ohne Einschreiten der Suchmaschinenbetreiberin ausgelistet, weil die Quellseiten offline gegangen sind, weshalb diese URL jederzeit wieder indexiert werden könnten. Der Dienstnehmer kann daher trotz Löschung seiner unrechtmäßig verarbeiteten Daten weiterhin die Feststellung der Rechtsverletzung begehren, weil die bloße Löschung die Rechtsverletzung nicht vollständig beseitigt und **Wiederholungsgefahr** besteht.

### Rechtsprechung der Justiz

OGH 18.02.2025, 6Ob102/24d

#### **Vorabentscheidungsersuchen, Verantwortliche, Datenherkunft, Schadenersatz, Amtshaftung**

- Ein **Volksschulleiter** ("Schulleiter") organisiert Fortbildungsprogramme für seine Lehrer, für die von der Pädagogischen Hochschule ua **Prozessbegleiter** zur Verfügung gestellt werden. In einem mündlichen Gespräch erkundigte sich der Schulleiter bei einem Lehrer über den von der Pädagogischen Hochschule vorgeschlagenen Prozessbegleiter. Daraufhin äußerte er seinen beruflichen E-Mail-Zugang Bedenken. Über das Gespräch wurde kein Aktenvermerk oder sonst ein Dokument angelegt. Der Prozessbegleiter erfuhr vom Inhalt der E-Mail und forderte den Schulleiter auf, ihm Auskunft zu erteilen und eine Kopie der verarbeiteten personenbezogenen Daten zu übersenden. Der Schulleiter teilte ihm mit, dass er nie dessen personenbezogene Daten besessen oder weitergegeben habe, er habe lediglich seine Bedenken zur Besetzung der Prozessbegleitung geäußert. Der Prozessbegleiter klagte auf **Auskunftserteilung, Herausgabe einer Kopie der Daten** und Zahlung von **immateriellem Schadenersatz**.

Der OGH beschloss das Verfahren **auszusetzen** und dem EuGH mehrere Fragen zur **Vorabentscheidung** vorzulegen, die (i) den Begriff des **Verantwortlichen**, (ii) das Auskunftsrecht zur **Datenherkunft** sowie (iii) den **immateriellen Schadenersatz** betreffen.

Der OGH hat erwogen: Eine juristische Person, Einrichtung, Behörde oder andere Stelle kann letztlich nur durch das Handeln der für sie tätigen natürlichen Personen agieren. Der Wortlaut von Art 4 Z 7 DSGVO lässt offen, ob

eine natürliche Person, die nicht im eigenen Interesse, sondern im Interesse der Organisation handelt, als **Verantwortlicher** anzusehen ist, oder ob die Haftung als Verantwortlicher stets die Organisation trifft. Denkbar wäre auch eine Haftung der Organisation und der natürlichen Person nebeneinander.

Unklar ist, wie weit der Begriff des Art 15 Abs 1 lit g DSGVO "**alle verfügbaren Informationen**" reicht. Die in der E-Mail enthaltenen Daten könnten als vom Schulleiter stammend gelten oder auch meinungsbildende Parameter erfassen. Es ist daher die Reichweite der Einbeziehung von Umständen und Einflüssen auf die Meinungsbildung des Äußernden zu klären. Dabei ist auch die Frage zu lösen, ob bereits Vorgänge, die eine bloße "Vorstufe" für die spätere Datenverarbeitung bilden, unter die Transparenzpflicht fallen.

Mit der Auskunft über den mündlichen "**Informanten**" werden auch dessen Rechte und Freiheiten berührt. Fraglich ist, ob bei der Abwägung zwischen den Interessen des Informanten und des Betroffenen den Umständen des Gesprächs Bedeutung zukäme (zB Vertraulichkeit des Gesprächs, Autoritätsverhältnis zwischen den Gesprächspartnern). Das Ziel eines hohen Schutzniveaus für personenbezogene Daten könnte dafür sprechen, auch Informationsquellen einer rufschädigenden Aussage offenzulegen – unabhängig davon, ob diese Person wusste, dass ihre Äußerung verarbeitet wird.

Zu klären ist auch, ob ein **Verstoß gegen die Auskunftspflicht** nach Art 15 DSGVO allein einen **Schadenersatzanspruch** nach Art 82 DSGVO begründet. **Dagegen spricht**, dass die Auskunftspflicht nicht zwingend mit einer Datenverarbeitung verknüpft ist und auch Negativauskünfte umfasst. Eine verspätete oder widersprüchliche Auskunft könnte jedoch Zweifel an der Rechtmäßigkeit einer Datenverarbeitung hervorrufen. Aufgrund des Ziels eines hohen Schutzniveaus könnte eine verspätete, widersprüchliche oder nicht erteilte Auskunft selbst eine DSGVO-widrige Datenverarbeitung (anlässlich der Auskunftserteilung) darstellen.

Die direkte Inanspruchnahme des Schulleiters ist nach nationalem Recht ausgeschlossen. Der Geschädigte müsste **Amtshaftungsansprüche** bei den in § 1 AHG genannten Rechtsträgern geltend machen. Da Art 82 Abs 2 DSGVO die Haftung des Verantwortlichen vorsieht, stellt sich die Frage, ob die nationalen Bestimmungen des AHG insoweit wegen Unionsrechtswidrigkeit **unangewendet** bleiben müssen.

#### Aus der weiteren Rechtsprechung der Justiz:

- Der Kläger beehrte **immateriellen Schadenersatz**. Der OGH setzte das Verfahren

bis zur Entscheidung des EuGH in mehreren Vorabentscheidungsverfahren aus. Der **EuGH** hat in diesen Vorabentscheidungsverfahren **entschieden**, daher war das Verfahren **fortzusetzen**. Der Kläger beehrte jedoch ua **Schadenersatz** wegen der **unvollständigen Beantwortung seines Auskunftsersuchens**. Die Frage, ob eine Verletzung des Rechts auf Auskunft einen Schadenersatz begründet, ist Gegenstand des parallel beim EuGH gerade neu eingeleiteten Vorabentscheidungsverfahrens zu **6 Ob 102/24d**. Das Verfahren hat daher bis zur Entscheidung des EuGH in diesem **neuen Vorabentscheidungsverfahren ausgesetzt** zu bleiben ([OGH 18.02.2025, 6Ob137/24a](#)).

- Die **Höhe von bestimmten – Differenzgeschäften** zu Grunde liegenden – **Hebeln** sind **personenbezogene Daten**. Dies auch dann, wenn die Hebel bei hunderten Kunden und tausenden **Trades** gleich hoch sein können. Daten, die für sich alleine keine "personenbezogenen" Daten sind, **können** zu personenbezogenen Daten **werden**, wenn sie sich in der **Sphäre einer Person** befinden, die bei vernünftiger Betrachtung über die Mittel verfügt, um sie einer **bestimmten Person** zuzuordnen ([OLG Innsbruck 08.01.2025, 4R136/24t](#)). **Anm: Das OLG Innsbruck unterscheidet – leider in schon gewohnter Tradition der österreichischen Rechtsprechung – nicht zwischen der "Information über eine Person" und der "Identifizierbarkeit einer Person". Der Begriff des Personenbezugs wird – unnötig und zu Lasten der Verantwortlichen – nochmals erweitert. In der bisherigen Rechtsprechung hat die bloße Möglichkeit der Zuordnung für den Personenbezug nicht ausgereicht und wurde sogar ausdrücklich verneint.**
- Wurde eine **Vollmachtsurkunde** entgegen der Anmerkung "handschriftlich" elektronisch unterzeichnet und **weicht diese Unterschrift maßgeblich** von jener auf dem Ausweis des Klägers ab, sind **Zweifel** an der Vollmachterteilung iSd Art 12 Abs 6 DSGVO **begründet**. Durch Verweigerung der Auskunftserteilung wird daher keine Veranlassung zur Klagsführung gegeben, sodass die **Kostenersatzpflicht** nach § 45 ZPO greift. Erst gegenüber dem Gericht kann sich ein Rechtsanwalt gemäß § 8 RAO auf die ihm erteilte Vollmacht berufen. Anerkennt daraufhin der beklagte Verantwortliche den Auskunftsanspruch, hat der **Kläger die Prozesskosten** zu tragen ([OLG Linz 05.03.2025, 2R32/25a](#)).

## **Rechtsprechung der LVwG**

Aus der Rechtsprechung der LVwG:

- Gegen Verletzungen des Datenschutzrechts besteht der **Rechtsschutz** bei der **DSB** und gegen Entscheidungen der DSB beim **BVwG**. Das LVwG NÖ ist **unzuständig** ([LVwG NÖ 01.12.2023, LVwG-M-55/001/2022](#)).

## **EU-Rechtsakte**

- Am **14.03.2025** wurde die "*Delegierte Verordnung (EU) 2025/416 der Kommission vom 29. November 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung des Inhalts und des Formats von Auftragsbuchaufzeichnungen für **Anbieter von Kryptowerte-Dienstleistungen, die eine Handelsplattform für Kryptowerte betreiben***", [ABI L 2025/416](#), kundgemacht. In dieser DelegiertenVO werden Regulierungsstandards festgelegt, die **Anbieter von Kryptowerte-Dienstleistungen, die eine Handelsplattform für Kryptowerte betreiben**, bei **Auftragsbuchaufzeichnungen** einzuhalten haben.
- Am **14.03.2025** wurde die "*Delegierte Verordnung (EU) 2025/417 der Kommission vom 28. November 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung der Art der Darstellung von Daten zur Transparenz durch **Anbieter von Kryptowerte-Dienstleistungen, die eine Handelsplattform für Kryptowerte betreiben***", [ABI L 2025/417](#), kundgemacht. In dieser DelegiertenVO werden für **Anbieter von Kryptowerte-Dienstleistungen, die eine Handelsplattform für Kryptowerte betreiben**, **Transparenzvorschriften** festgelegt.
- Am **13.03.2025** veröffentlichte die **Europäische Kommission**, die **Entwürfe** der "*Commission Implementing Regulation on the technical description of the categories of **important and critical products with digital elements** pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council*" samt Anhängen zur **Konsultation**. Mit dieser DurchführungsVO bzw in ihren Anhängen werden die **technischen Spezifikationen** der in den Anhängen III und IV der **Cyberresilienz-Verordnung** aufgelisteten "Wichtigen Produkte mit Digitalen Elementen" und "Kritischen Produkte mit Digitalen Elementen" umschrieben. **Rückmeldungen** sind bis (einschließlich) 15.04.2025 möglich.

to the point

# Datenschutzmonitor. 12/2025 vom 26.03.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH SA 20.03.2025, C-655/23, *Quirin Privatbank* (Unterlassungsanspruch, Wiederholungsgefahr, Schadenersatz)

- **Rechtsprechung des VfGH**

VfGH 25.02.2025, G160/2024 (NRWO, Wahlkarte, Identitätsdiebstahl, Identitätsprüfung)

VfGH 11.03.2025, E4624/2024 (Massenverfahren, ORF-Beitrag, Datenschutz)

- **Rechtsprechung der Justiz**

OLG Linz 13.03.2025, 6R29/25i (Auskunftser-suchen, Identifizierung)

- **Rechtsprechung des BVwG**

BVwG 28.01.2025, W108 2274731-1 (Gesichtserkennungsplattform, Verarbeitungs-verbod, Abhilfemaßnahme, Antragsrecht)

BVwG 20.02.2024, W287 2306632-1 (Nichter-teilung der Auskunft, unvollständige Auskunft, Säumnisbeschwerde)

BVwG 05.02.2025, W298 2292389-1 (Bundes-präsident, Amtsverschwiegenheit, Datenschutz)

BVwG 11.02.2025, W256 2247121-1 (Bauver-fahren, Interessenabwägung, Datenaustausch aufgrund von Rechtsansprüchen)

BVwG 03.02.2025, W292 2285781-1 (Direkt-werbung, TKG, Widerspruch)

BVwG 03.02.2025, W292 2285575-1 (Lö-schung, Insolvenzdaten, keine rückwirkende Feststellung)

BVwG 26.02.2025, W101 2250871-1 (Warnliste der Banken, Berichtigung, Löschung)

BVwG 19.02.2025, W137 2305838-1 (Vertre-tungsvollmacht, Minderjähriger, Wiederauf-nahme)

BVwG 11.02.2025, W256 2293315-2 (Verfah-renshilfe)

- **Rechtsprechung des BFG**

BFG 19.02.2025, RV/5100235/2024 (Sonder-ausgaben, bPK)

- **EU-Rechtsakte**

DurchführungsVO (EU) 2025/512 (Zollkodex, Data Mining, künstliche Intelligenz)

## To the Point:

### Rechtsprechung des EuGH

EuGH SA 20.03.2025, C-655/23, Quirin Privatbank

#### **Unterlassungsanspruch, Wiederholungsgefahr, Schadenersatz**

- Ein Bewerber bewarb sich über Xing bei einer Bank. Eine Mitarbeiterin der Bank versendete im Rahmen dieses Bewerbungsprozesses eine Nachricht an eine dritte, nicht an diesem Bewerbungsprozess beteiligte Person. Diese leitete die Nachricht an den Bewerber weiter, der daraufhin die Unterlassung der unrechtmäßigen Datenverarbeitung und immateriellen Schadenersatz von der Bank forderte.

Der Generalanwalt hat erwogen: Ein **Unterlassungsanspruch** des Betroffenen bei unrechtmäßiger Verarbeitung seiner Daten lässt sich bei **Wiederholungsgefahr** aus Art 5 Abs 1 lit a und Art 6 Abs 1 iVm Art 79 Abs 1 DSGVO ableiten. Das **Recht des Betroffenen auf Rechtmäßigkeit der Datenverarbeitung** besteht, obwohl es in Kapitel III der DSGVO (Rechte der betroffenen Person) nicht ausdrücklich erwähnt ist, weil dieses Recht **vorausgesetzt** wird.

Das Recht, eine wiederholte unrechtmäßige Verarbeitung zu unterlassen, ist mit einem **gerichtlichen Reaktionsmechanismus** gekoppelt, auf den in Art 79 DSGVO Bezug genommen wird. Es spricht nichts dagegen, dass die Klage auch den Anspruch auf Verurteilung des Verantwortlichen zur Unterlassung einer wiederholten unrechtmäßigen Verarbeitung umfasst.

Art 17 und 18 DSGVO begründen **kein eigenständiges Recht**, vom Verantwortlichen die Unterlassung einer wiederholten rechtswidrigen Verarbeitung zu verlangen. Befolgt der Verantwortliche die Anweisung zur **Löschung**, stehen ihm die Daten nicht mehr zur Verfügung und er kann sie tatsächlich nicht mehr verarbeiten. Auch die **Einschränkung der Verarbeitung** bietet keinen ausreichenden Schutz, weil nur die Löschung vorübergehend ausgesetzt, nicht aber eine künftige unrechtmäßige Verarbeitung verhindert wird.

Es ist **Sache der nationalen Rechtsordnung**, unter Beachtung der Grundsätze der Äquivalenz und der Effektivität, die Voraussetzungen für die Erhebung einer gegen den für die Verarbeitung personenbezogener Daten Verantwortlichen gerichteten **Unterlassungsklage** zu regeln. Es spricht nichts dagegen, den **Nachweis der Wiederholungsgefahr** zu verlangen oder **eine (widerlegbare) Vermutung einer solchen Gefahr**, die sich aus einem bereits begangenen Verstoß ergibt, aufzustellen.

Durch eine Unterlassungsverfügung wird der immaterielle Schaden nicht ausgeglichen. Bei der **Schadensbemessung** kann ein **Unterlassungsanspruch** daher nicht anspruchsmindernd berücksichtigt werden.

### Rechtsprechung des VfGH

VfGH 25.02.2025, G160/2024

#### **NRWO, Wahlkarte, Identitätsdiebstahl, Identitätsprüfung**

- Eine Antragstellerin beehrte in Form eines **Individualantrags** beim VfGH die Aufhebung von Teilen des § 39 Abs 1 der **Nationalrats-Wahlordnung** ("NRWO") aufgrund von Verfassungswidrigkeit. Die angefochtene Bestimmung regelt die Ausstellung von Wahlkarten. Die Antragstellerin begründete ihre verfassungsrechtlichen Bedenken – kurz zusammengefasst – dahingehend, dass die angefochtene Bestimmung ihren Ausschluss von der Stimmabgabe bei der Nationalratswahl bewirkt habe, weil ein unbefugter Dritter "in ihrem Namen" eine Wahlkarte beantragt habe, die ihr nicht zugestellt wurde. § 39 Abs 1 NRWO könne einen solchen **"Identitätsdiebstahl"** nicht effektiv unterbinden, weil das darin geregelte Prozedere der Antragsbearbeitung von Wahlkarten niederschwellig und formlos konzipiert sei.

Der VfGH hat erwogen: Die von der Antragstellerin angefochtene Bestimmung regelt ausschließlich die **Identitätsprüfung** bei der **Ausstellung der Wahlkarte**. Die Zustellung der beantragten Wahlkarte ist hingegen in § 39 Abs 4 bis 8 NRWO geregelt. Erst aus § 70 Abs 1 und 2 NRWO ergibt sich schließlich, dass eine Person, für die eine Wahlkarte ausgestellt wurde, im **Wahllokal** die Wahlkarte vorzuweisen oder der Wahlbehörde zu übergeben hat, andernfalls diese Person zur Stimmabgabe nicht berechtigt ist. Das **Aufhebungsbegehren** umfasste allerdings ausschließlich § 39 Abs 1 NRWO, sodass der Antrag als **zu eng gefasst** vom VfGH zurückzuweisen war. **Anm: Nach ständiger Rechtsprechung des VfGH hat der Antragsteller eines Individualantrags all jene Normen anzufechten, die für die Beurteilung einer allfälligen Verfassungswidrigkeit der Rechtslage eine untrennbare Einheit bilden. Der Anfechtungsumfang der in Prüfung gezogenen Norm darf bei sonstiger Unzulässigkeit des Prüfungsantrags nicht zu eng gewählt werden. Bei der Prüfung dieser Zulässigkeitsanforderungen legt der VfGH einen strengen Maßstab an.**

#### Aus der weiteren Rechtsprechung des VfGH:

- Sind beim VfGH eine erhebliche Anzahl von Verfahren über Beschwerden iSd § 86a Abs 1 VfGG anhängig, in denen gleichartige Rechtsfragen zu lösen sind, oder besteht

Grund zur Annahme, dass eine erhebliche Anzahl solcher Erkenntnisbeschwerden eingebracht werden wird, kann der VfGH ein **Massenverfahren** einleiten. Wirkung des Massenverfahrens ist, dass sämtliche Verfahren ausgesetzt werden, bis die Rechtsfrage vom VfGH in einem "Hauptverfahren" gelöst wird. Beim VfGH sind bereits 18 **Erkenntnisbeschwerden** eingelangt, die sich gegen die Verfassungsmäßigkeit der Rechtsvorschriften des **ORF-Beitrags-Gesetzes 2024** richten und es ist mit einer erheblichen Anzahl weiterer solcher Erkenntnisbeschwerden zu rechnen. In den Erkenntnisbeschwerden wird ua ein Verstoß gegen das **Grundrecht auf Datenschutz** gemäß § 1 DSG geltend gemacht ([VfGH 11.03.2025, E4624/2024](#)).

### **Rechtsprechung der Justiz**

Aus der Rechtsprechung der Justiz:

- Die DSGVO gibt zur Ausübung der Betroffenenrechte keine konkrete Form der Identifizierung vor. Ein **elektronisches Auskunftersuchen** muss nicht zwingend mit einer **qualifizierten elektronischen Signatur** versehen sein. Nur wenn der Verantwortliche Zweifel hat, kann er nach Art 12 Abs 6 DSGVO weitere Informationen zur **Identifizierung** des Antragstellers einfordern ([OLG Linz 13.03.2025, 6R29/25i](#)).

### **Rechtsprechung des BVwG**

[BVwG 28.01.2025, W108 2274731-1](#)

#### **Gesichtserkennungsplattform, Verarbeitungsverbot, Abhilfemaßnahme, Antragsrecht**

- Ein Plattformbetreiber ohne Sitz in der EU betrieb eine **Gesichtserkennungsplattform**, deren Nutzer online gefundene Bilder mit Fotos von Personen abgleichen konnten. Nach einem Auskunftersuchen erlangte ein Nutzer Kenntnis über die Verarbeitung seiner Bilder auf der Plattform. Er brachte eine Datenschutzbeschwerde bei der DSB gegen den Plattformbetreiber ein. Zusätzlich beantragte der Nutzer die Anordnung eines **Verarbeitungsverbots** seiner personenbezogenen Daten innerhalb der EU. Die DSB gab der Datenschutzbeschwerde statt und ordnete als Abhilfemaßnahme die Löschung der Daten des Betroffenen an. Der Antrag auf Verbot der Verarbeitung wurde zurückgewiesen. Gegen diese Zurückweisung erhob der Nutzer erfolgreich Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Hat die DSB eine Datenschutzbeschwerde zurückgewiesen, ist "Sache" des Beschwerdeverfahrens nur die Frage der **Rechtmäßigkeit der Zurückweisung**.

Einer betroffenen Person kommt nach der DSGVO **kein subjektives Recht** zu, die Verhängung eines generellen **Verarbeitungsverbots** zu beantragen. Die Behörde hat lediglich die Verpflichtung, in geeigneter Weise mit **Abhilfemaßnahmen** zu reagieren, um der festgestellten Unzulänglichkeit abzuwehren.

Da kein subjektives Recht auf eine (bestimmte) Abhilfemaßnahme besteht, gibt es diesbezüglich auch **kein Antragsrecht**. Ein dennoch gestellter Antrag ist mangels Antragslegitimation zurückzuweisen.

Der von einer Partei unzulässig gestellte Antrag auf Verhängung einer bestimmten Maßnahme ist von der Behörde jedoch **inhaltlich** dahingehend **zu prüfen**, ob das Ergreifen einer in der DSGVO vorgesehenen Abhilfemaßnahme unter Berücksichtigung aller Umstände des konkreten Falles geeignet, erforderlich und verhältnismäßig ist, um der festgestellten Unzulänglichkeit abzuwehren. Die **durchgeführte Prüfung** des Antrags unterliegt anschließend **der vollen inhaltlichen Überprüfung durch ein Gericht**.

Die verabsäumte inhaltliche Prüfung und **Ermessensausübung** der DSB konnte vom BVwG weder saniert noch nachgeholt werden, weshalb der DSB die Fortsetzung des Verfahrens unter Abstandnahme vom gebrauchten Zurückweisungsgrund aufgetragen wird. **Anm: Das Zusammenspiel zwischen innerstaatlichem Recht und Unionsrecht entfaltet seltsame Blüten. Denn nach innerstaatlichem Recht setzt eine Zurückweisung gerade keine inhaltliche Prüfung voraus. Ebenso überrascht, dass trotz fehlenden Antragsrechts ein Recht auf das Erheben eines Rechtsmittels besteht.**

[BVwG 20.02.2025, W287 2306632-1](#)

#### **Nichterteilung der Auskunft, unvollständige Auskunft, Säumnisbeschwerde**

- Ein Auskunftswerber richtete ein Auskunftersuchen an einen Verantwortlichen. Dieser teilte ihm mit, dass seine Daten als Reaktion auf das Auskunftersuchen irrtümlich gelöscht wurden. Eine Auskunft erteilte der Verantwortliche nicht. Der Auskunftswerber erhob Datenschutzbeschwerde. Der Verantwortliche erteilte daraufhin Auskunft über die (noch) verarbeiteten personenbezogenen Daten des Auskunftswerbers. Die DSB betrachtete die Datenschutzbeschwerde als erledigt, der Betroffene bestand jedoch weiterhin auf die Erteilung einer vollständigen bzw. mangelfreien Auskunft. Der Betroffene erhob eine **Säumnisbeschwerde** an das BVwG.

Die DSB stellte das ursprüngliche Verfahren wegen Nichterteilung der Auskunft formlos ein und protokollierte die Säumnisbeschwerde als neue Datenschutzbeschwerde. Das BVwG wies die Säumnisbeschwerde ab.

Das BVwG hat erwogen: Gemäß § 13 Abs 8 AVG kann der **verfahrenseinleitende Antrag** (= Datenschutzbeschwerde) in jeder Lage des Verfahrens geändert werden, sofern die Sache ihrem Wesen nach nicht geändert und die sachliche und örtliche Zuständigkeit nicht berührt werden.

Da sich der Auskunftswerber im Laufe des Verfahrens nicht mehr wegen der **Nichterteilung**, sondern wegen der **mangelhaften bzw unvollständigen Erteilung der Auskunft** als beschwert erachtete, war nun auch eine inhaltliche Prüfung der Auskunft erforderlich. Deshalb war von der Zurückziehung der ursprünglichen Datenschutzbeschwerde bei gleichzeitiger Einbringung einer **neuen Datenschutzbeschwerde** auszugehen. Die Säumnisbeschwerde war zurückzuweisen, weil die Zulässigkeit einer Säumnisbeschwerde die Säumnis der DSB und somit die Verpflichtung, über den bei ihr eingebrachten Antrag mittels Bescheid zu entscheiden, voraussetzt (**Entscheidungspflicht**). Das Verfahren wegen der Nichterteilung der Auskunft war jedoch formlos einzustellen. Deshalb verletzte die DSB ihre Entscheidungspflicht nicht.

BVwG 05.02.2025, W298 2292389-1

#### **Bundespräsident, Amtsverschwiegenheit, Datenschutz**

- Ein **Nationalratsabgeordneter** (Parteimitglied) stellte ein Auskunftsbegehren an das Bürgerservice der Präsidentschaftskanzlei (§§ 2 und 3 AuskunftspflichtG). Gegenstand des Begehrens war insbesondere die Frage, welche Kosten im Zusammenhang mit den Festspielbesuchen des Bundespräsidenten und seiner Begleitung angefallen waren. Das Parteimitglied erachtete die Beantwortung seiner Anfrage für unvollständig. Mit Bescheid ergänzte der Bundespräsident seine Antwort. Dennoch hielt das Parteimitglied die erteilte Auskunft für nicht gesetzeskonform. Der Bundespräsident hielt fest, dass soweit die Auskunftserteilung zu einem Sicherheitsrisiko für den Bundespräsidenten, seiner Gemahlin oder von Mitarbeitenden führen kann, die Informationsweitergabe zwingend zu unterbleiben hat. Das Parteimitglied sei überdies kein "public watchdog". Die vom Parteimitglied erhobene Bescheidbeschwerde an das BVwG blieb erfolglos.

Das BVwG hat erwogen: Gemäß **§ 1 Abs 1 AuskunftspflichtG** haben die Organe des Bundes "über Angelegenheiten ihres Wirkungsbereiches" **Auskünfte zu erteilen**. Der Begriff "Auskunft" umfasst die **Pflicht zur Information über die Tätigkeit der Behörde**, nicht aber eine Verpflichtung zur Begründung behördlichen Handelns oder Unterlassens.

Aus **Art 10 Abs 1 EMRK** resultiert keine **Verpflichtung des Staates, den Zugang**

**zu Informationen zu gewährleisten** oder selbst Informationen bereitzustellen. Unter bestimmten Voraussetzungen ist jedoch ein **Recht auf Zugang zu Informationen** gewährleistet. Dies ist der Fall, wenn ua der Zugang für die Ausübung der Meinungsäußerungsfreiheit maßgeblich ist. Zum Beispiel, wenn Grundrechtsträger in der Funktion als "**public watchdog**" im öffentlichen Interesse tätig werden.

Auskünfte sind grundsätzlich zu geben, soweit eine gesetzliche Verschwiegenheitspflicht dem nicht entgegensteht (§ 1 Abs 1 AuskunftspflichtG). Sie sind insoweit zu erteilen, als dadurch die **Besorgung der übrigen Aufgaben eines Organes nicht wesentlich beeinträchtigt wird**. Auskunft ist weiters dann nicht zu erteilen, wenn sie **offenkundig mutwillig** begehrt wird (§ 1 Abs 2 AuskunftspflichtG).

Zur Beurteilung, ob ein **subjektiver Auskunftsanspruch** gegenüber dem Rechtsträger besteht, ist der **Zweck des Auskunftsersuchens relevant**. Wenn das Parteimitglied sein Auskunftsersuchen mit seiner **parlamentarischen Kontrollpflicht** begründet, kann daraus kein weitergehendes Recht auf Zugang zu Informationen iSd AuskunftspflichtG abgeleitet werden. Selbst die Privilegierung als "**public watchdog**" würde **keine Informationspflichten** begründen, **soweit Geheimhaltungspflichten** entgegenstehen.

Die **Verpflichtung zur Auskunftserteilung** kann durch andere verfassungsrechtliche Vorschriften (insb Art 20 Abs 3 B-VG und § 1 DSG) und auf Grundlage der in Art 20 Abs 4 B-VG enthaltenen Ermächtigung auch durch einfachgesetzliche Regelungen (zB **datenschutzrechtlichen Geheimhaltungspflichten**) beschränkt sein. Betreffend die **Amtsverschwiegenheit** sind die Interessen der Gebietskörperschaft und der Parteien zu berücksichtigen.

Eine **genaue Auflistung** der für einzelne Personen angefallenen Reisekosten **ist nicht notwendig**. Für die begehrte Auskunft müssten Daten von Dritten erhoben, verarbeitet und übermittelt werden, ohne dass ein entsprechender Verarbeitungsgrund vorliegt. Auch wenn die Begleitpersonen in der Auflistung nicht namentlich genannt sind, könnten vereinzelt dennoch **Rückschlüsse** auf diese gezogen werden. Ebenso würde die genaue Auskunft über die Auswahl der Transportmittel Rückschlüsse auf **personenbezogene Daten** einzelner Mitarbeiter des Bundespräsidenten und seiner Ehegattin zulassen. Weiters könnte dies die **Sicherheit des Bundespräsidenten** gefährden. Dies gilt auch in Bezug auf die Unterbringungskosten.

## **Bauverfahren, Interessenabwägung, Datenaustausch aufgrund von Rechtsansprüchen**

- Der Betroffene beauftragte eine Baufirma mit der Errichtung eines Doppelwohnhauses. Ein Nachbar des Betroffenen erhob wiederholt Einsprüche gegen dieses Vorhaben, was zu einem langwierigen Prozess führte. Gleichzeitig führte der Betroffene ein Verfahren wegen fehlerhafter Bauausführungen gegen die Baufirma. Im Zuge der Korrespondenzen bezüglich der Verfahren drohte die Baufirma dem Betroffenen an, den gesamten Mailverkehr und darin enthaltene Informationen zur Bauausführung an den Nachbarn weiterzugeben, falls der Betroffene die ausstehenden Zahlungen nicht leisten sollte.

Daraufhin erhob der Betroffene eine Datenschutzbeschwerde bei der DSB, welche diese abwies, weil die Datenübermittlung nicht festgestellt werden konnte. Der Betroffene richtete eine Bescheidbeschwerde an das BVwG und behauptete, dass der Nachbar E-Mails erhalten habe, die ausschließlich zwischen ihm und der Baufirma ausgetauscht wurden. Diese E-Mails enthielten Informationen, die der Nachbar in dem anhängigen Bewilligungsverfahren des Bauvorhabens verwendet hat.

Das BVwG hat entschieden: Gemäß § 1 Abs 1 DSG hat jedermann Anspruch auf **Geheimhaltung** der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Eine Beschränkung des Grundrechts auf Datenschutz ist gemäß § 1 Abs 2 DSG zulässig, wenn die Datenverarbeitung rechtmäßig ist und in der gelindesten, zum Ziel führenden Art vorgenommen wird. Eine Konkretisierung der Anforderungen einer rechtmäßigen Datenverarbeitung sieht Art 6 DSGVO vor.

Gemäß Art 6 Abs 1 lit f und Art 9 Abs 2 lit f DSGVO ist die Verarbeitung personenbezogener Daten zulässig, wenn die Verarbeitung zur **Wahrung berechtigter Interessen** des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte der betroffenen Person nicht überwiegen. Die **Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen** sind ein berechtigtes Interesse, das eine Verarbeitung von Daten legitimiert.

Zum Zeitpunkt der Datenübermittlung gab es einerseits zwischen dem Betroffenen und der Baufirma und andererseits zwischen dem Betroffenen und dem Nachbarn jeweils ein **anhängiges Verfahren**. Der **Datenaustausch erfolgte im direkten Zusammenhang** mit diesen beiden Rechtsstreitigkeiten zur Verteidigung und Geltendmachung von Rechtsansprüchen der Baufirma und des Nachbarn. Die **Baufirma hat ein berechtigtes Interesse**, sich gegen zivilgerichtliche

Vorwürfe zu verteidigen und dazu Unterstützung bei Dritten einzuholen. Auch der Nachbar hat ein **berechtigtes Interesse**, Informationen über die Einhaltung von Bauvorschriften zu erhalten, um Rechtsansprüche im Bewilligungsverfahren geltend zu machen. Die **Interessenabwägung** iSd Art 6 Abs 1 lit f DSGVO führt sohin zum Ergebnis, dass die Interessen des Betroffenen an der Vertraulichkeit seiner Daten die berechtigten Interessen der Baufirma und des Nachbarn nicht überwiegen. Die Übermittlung der Daten an den Nachbarn war daher rechtmäßig.

### Aus der weiteren Rechtsprechung des BVwG:

- Die **Verarbeitung von Kontaktdaten** potenzieller Arbeitnehmer zum Zweck der Anbahnung eines Dienstverhältnisses kann im Rahmen der Arbeitskräfteüberlassung ein **berechtigtes Interesse im Sinne von Art 6 Abs 1 lit f DSGVO** sein. Die **Übermittlung von Werbung** durch Telefonanruf bedarf jedoch ausnahmslos nach § 174 Abs 1 TKG 2021 einer **vorherigen Einwilligung**. Die **Voraussetzungen** für eine gültig abgegebene Einwilligung ergeben sich aus **Art 7 DSGVO**. Nach Abgabe einer **Widerspruchserklärung iSd Art 21 DSGVO** ist **jegliche Verarbeitung** personenbezogener Daten zum Zweck der Kontaktaufnahme mit dem Betroffenen, gleich ob auf elektronischem oder anderem Wege, gemäß Art 21 Abs 2 und 3 DSGVO **unzulässig** ([BVwG 03.02.2025, W292 2285781-1](#)).
- Werden während des **laufenden Verfahrens** die verfahrensgegenständlichen **Insolvenzdaten gelöscht**, ist das Verfahren einzustellen. Ein **subjektives Recht** auf die **rückwirkende Feststellung** einer zwischenzeitlich vom Verantwortlichen beseitigten Verletzung im Recht auf Löschung gewährt weder das DSG noch die DSGVO. Wurde vor der DSB die Feststellung der Verletzung des **Rechts auf Löschung** begehrt, darf die DSB die Verletzung anderer Rechte nicht feststellen ([BVwG 03.02.2025, W292 2285575-1](#)).
- Wird während des **laufenden Verfahrens** dem **Berichtigungersuchen** durch Löschung des Eintrags "Teilweise Tilgung" in der **Warnliste der Banken des "KSV 1870"** entsprochen, ist das Verfahren einzustellen. Durch Wegfall des **Rechtsschutzinteresses** wird der Betroffene **materiell klaglos gestellt** ([BVwG 26.02.2025, W101 2250871-1](#)).
- Der Betroffene hat mehrere Verfahren vor der DSB geführt, obwohl er über keine **Vertretungsvollmacht** für den **Minderjährigen** verfügte, für den er die Datenschutzbeschwerden eingebracht hat. Da der Betroffene weiterhin über keine Vertretungsbefugnis verfügt, war sein



**Wiederaufnahmeantrag zurückzuweisen** ([BVwG 19.02.2025, W137 2305838-1](#)).

- Verfügt ein **Antragsteller** über entsprechende Fähigkeiten im Verkehr mit Behörden und ist er in der Lage, seine Rechte selbst wahrzunehmen, ist in Verfahren vor den Verwaltungsgerichten (hier das BVwG) **kein Verfahrenshelfer** beizugeben. Bringt ein Betroffener eine **Datenschutzbeschwerde** und eine **Säumnisbeschwerde** ein, ist davon auszugehen, dass er in der Lage ist, seine Rechte selbst wahrzunehmen, sodass der Antrag auf Verfahrenshilfe abzuweisen ist. Denn anders als Zivilgerichte hat das BVwG die Beweise von **Amts wegen** zu erheben und den **Gang des Verfahrens** zu bestimmen ([BVwG 11.02.2025, W256 2293315-2](#)).

### **Rechtsprechung des BFG**

Aus der Rechtsprechung des BFG:

- Spenden sind nur dann als **Sonderausgaben** zu berücksichtigen, wenn dem Spendeneempfänger **Vor- und Zuname** und das **Geburtsdatum** des Leistenden bekannt gegeben werden und der Spendenempfänger der Abgabenbehörde das **verschlüsselte bereichsspezifische Personenkennzeichen ("bPK") für Steuern und Abgaben** des Leistenden und den Gesamtbetrag aller Spenden übermittelt. **Datenschutzrechtliche Bedenken** gegen diese Regelung **bestehen nicht** ([BFG 19.02.2025, RV/5100235/2024](#)).

### **EU-Rechtsakte**

- Am **20.03.2025** wurde die "*Durchführungsverordnung (EU) 2025/512 der Kommission vom 13. März 2025 über technische Modalitäten für die Entwicklung, Wartung und Nutzung elektronischer Systeme für den Austausch und die Speicherung von Informationen gemäß der Verordnung (EU) Nr. 952/2013 des Europäischen Parlaments und des Rates*", [ABI L 2025/512](#), kundgemacht. Mit dieser auf den **EU-Zollkodex** gestützten DurchführungsVO werden technische Modalitäten für nach den zollrechtlichen Vorschriften erforderlichen Austausch von Informationen in zentralen Systemen festgelegt. Ua soll auf **Data Mining** gesetzt werden. Unter **Data Mining** ist nach dieser DurchführungsVO die **Analyse großer Datenmengen in digitaler Form durch Analysetechniken zur Generierung von Informationen, die Muster, Trends und Korrelationen umfassen, um Risiken zu mindern und eine fundierte Entscheidungsfindung auf der Grundlage menschlicher Eingriffe zu ermöglichen**, zu verstehen. **Anm: Die DurchführungsVO (EU) 2025/512 sieht somit den Einsatz künstlicher Intelligenz vor.**

to the point

# Datenschutzmonitor. 13/2025 vom 03.04.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH/EuG**

EuGH SA 27.03.2025, C-654/23, *Inteligo Media* (Direktwerbung, ePrivacyRL, personenbezogene Daten als Ware)

EuGH SA 27.03.2025, C-97/23 P, *WhatsApp Ireland/EDSA* (WhatsApp, EDSA, verbindlicher Beschluss, Rechtsschutzsystem der EU)

EuG 26.03.2025, T-441/21, *UBS Group und UBS/Kommission* (Schutz von personenbezogenen Daten und Geschäftsgeheimnissen, alte Daten)

- **Rechtsprechung der Justiz**

OGH 19.03.2025, 9Ob48/24k (Streamingdienst, Verbraucherschutz)

OGH 25.02.2025, 11Os7/25a (Datenbetrug)

OGH 18.02.2025, 6Ob218/24p (Aussetzung, Smart Meter)

OLG Wien 27.08.2024, 17Bs267/24z (§ 63 DSG, Officialdelikt)

- **Rechtsprechung des BVwG**

BVwG 18.02.2025, W129 2303356-1 (Universität, Satzung, Videoaufzeichnungen)

BVwG 14.02.2025, W211 2299661-1 (Streitanhängigkeit, entschiedene Sache, Beschwerdeergänzung)

BVwG 11.02.2025, W254 2295624-1 (Auskunft, Empfänger, Zeitpunkt der Erteilung, Löschung, Widerspruch)

BVwG 17.02.2025, W274 2302842-1 (Geheimhaltung, veröffentlichte Daten, Einwilligung)

BVwG 14.02.2025, W211 2288888-1 (Wildkamera, Handykamera)

BVwG 14.02.2025, W211 2288825-1 (Lichtbild, Erforderlichkeit, Rechtsanspruch)

BVwG 14.02.2025, W208 2307243-1 (Disziplinarverstoß, PAD)

BVwG 04.02.2025, G314 2296792-1; G314 2296798-1 (ORF-Beitrag, Zuständigkeit)

- **Rechtsprechung des BFG**

BFG 03.03.2025, RV/7102539/2021 (Abgaben)

- **Rechtsprechung der DSB**

DSB 11.02.2025, 2024-0.195.679 (Straßenfotografie, Kunstfreiheit, Fotos)

## To the Point:

### Rechtsprechung des EuGH/EuG

EuGH SA 27.03.2025, C-654/23, Inteligo Media

#### **Direktwerbung, ePrivacyRL, personenbezogene Daten als Ware**

- Ein **Online-Pressemedium** bot seinen Nutzern eine begrenzte Anzahl kostenloser Artikel an. Um auf weitere Artikel zugreifen zu können, mussten die Nutzer ein **kostenloses Benutzerkonto** erstellen, ihre E-Mail-Adresse angeben und die Vertragsbedingungen für die Erbringung dieses "Premium-Dienstes" akzeptieren. Dieser kostenlose "Premium-Dienst" umfasste den Zugang zu zwei weiteren Artikeln pro Monat und einen täglichen E-Mail-Newsletter. Der Erhalt dieses Newsletters war standardmäßig aktiviert, konnte aber bei der Registrierung oder später abbestellt werden. Nutzer, die ein Benutzerkonto zu anderen Zwecken erstellt hatten, erhielten den Newsletter nicht. Gegen Zahlung einer Gebühr erhielten die Nutzer schließlich Zugang zu allen Artikeln und einen ausführlichen E-Mail-Newsletter.

Die zuständige Datenschutz-Aufsichtsbehörde verhängte eine Geldstrafe iHv ca EUR 9.000, weil das Online-Pressemedium den Newsletter ohne ausdrückliche Einwilligung der Nutzer verschickt habe. Das vorliegende Gericht stellte dem EuGH insbesondere Fragen zur Zulässigkeit von E-Mail-Newslettern nach Art 13 Abs 2 der Richtlinie 2002/58/EG (ePrivacyRL) und zur Anwendbarkeit der DSGVO.

Der Generalanwalt hat erwogen: Gemäß Art 13 Abs 1 ePrivacyRL ist **Direktwerbung** per Anruf, Fax oder elektronischer Post nur mit **vorheriger Einwilligung** zulässig. Eine **Ausnahme** besteht, wenn die Kontaktdaten iZm dem Verkauf eines Produkts oder einer Dienstleistung erlangt werden und zur Direktwerbung für ähnliche Produkte oder Dienstleistungen verwendet werden, sofern dem Nutzer eine **Widerspruchsmöglichkeit** eingeräumt wird.

Der Zweck des E-Mail-Newsletters bestand darin, Nutzer durch die Bereitstellung von Hyperlinks dazu zu verleiten, ihre monatlich kostenlosen Artikel schneller zu konsumieren und letztlich ein vollständiges kostenpflichtiges Abonnement zu erwerben. Der Newsletter verfolgte somit ein **kommerzielles Ziel**. Er richtete sich auch direkt und individuell an die Nutzer, indem er in deren E-Mail-Postfach erschien, sodass er als **Direktwerbung** anzusehen war.

Die Erlangung der E-Mail-Adressen ist "im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung" iSd Art 13 Abs 2 ePrivacyRL erfolgt. "**Verkauf**" umfasst die **Zahlung eines Entgelts** für eine Ware oder einen Dienst. Auch eine **indirekte Vergütung**, bei der die Kosten der

Zurverfügungstellung eines solchen Dienstes in den Verkaufspreis für die Hauptleistung einbezogen werden, erfüllt diese Voraussetzung. Zudem werden **personenbezogene Daten** selbst als **Ware** behandelt. Für eine Datenerhebung "im Zusammenhang mit einem Verkauf" reicht es daher aus, dass der Nutzer seine persönlichen Daten gegen eine Ware oder Dienstleistung zur Verfügung stellt. Ein solcher Newsletter ist "Direktwerbung" für "ähnliche Produkte oder Dienstleistungen", sodass eine **vorherige Einwilligung nicht erforderlich** war.

Das Verhältnis zwischen der ePrivacyRL und der DSGVO wird durch den Grundsatz **lex specialis derogat legi generali** geregelt. Existiert eine spezifische Bestimmung in der ePrivacyRL, die dasselbe Ziel verfolgt wie die DSGVO, ist die Bestimmung der ePrivacyRL anzuwenden. Art 13 Abs 2 ePrivacyRL regelt die Voraussetzungen und Zwecke der Verarbeitung sowie die Rechte der Betroffenen abschließend und erlegt dem Verantwortlichen **besondere Pflichten iSd Art 95 DSGVO** auf. Insbesondere wird die Frage der Einwilligung abschließend behandelt. Die Rechtmäßigkeit der Verarbeitung kann daher aufgrund des Art 13 Abs 2 ePrivacyRL festgestellt werden. Ein Rückgriff auf die DSGVO ist weder möglich noch erforderlich. **Anm:** Folgt der EuGH den Schlussanträgen des Generalanwalts, könnte das in Österreich große praktische Relevanz haben. Denn die DSB erachtet sich nicht nur hinsichtlich der elektronischen Direktwerbung (insb. Newsletter), sondern auch beim Erheben von Cookies, das ebenso in der ePrivacyRL (und im TKG 2021) geregelt ist, für zuständig.

EuGH SA 27.03.2025, C-97/23 P, WhatsApp Ireland/EDSA

#### **WhatsApp, EDSA, verbindlicher Beschluss, Rechtsschutzsystem der EU**

- Im Zuge der Anpassung ihrer Datenschutzrichtlinie an die DSGVO forderte **WhatsApp** seine Nutzer auf, den geänderten Bedingungen zuzustimmen oder die Nutzung einzustellen. Die irische Datenschutzbehörde ("**DPC**") begann aufgrund einiger Beschwerden eine Untersuchung über mögliche Verstöße gegen **Transparenzpflichten** iSd Art 12 bis 14 DSGVO. Angesichts der grenzüberschreitenden Verarbeitung leitete die DPC ein **Kohärenzverfahren** ein und übermittelte ihren **Beschlussentwurf** an die anderen **betroffenen Aufsichtsbehörden**. Einige davon erhoben **Einsprüche**, denen sich die DPC nicht anschloss.

Mit einem **Verbindlichen Beschluss** verpflichtete der Europäische Datenschutzausschuss ("**EDSA**") die DPC, ua "**Lossy-Hash-Daten**" (damit sind – soweit ersichtlich – in numerische Codes umgewandelte Telefonnummern gemeint) als personenbezogene

Daten zu qualifizieren und die vorgeschlagene Geldbuße zu erhöhen. Die irische Aufsichtsbehörde erließ daraufhin einen entsprechend angepassten endgültigen Beschluss. WhatsApp erhob gegen den Beschluss des EDSA **Nichtigkeitsklage** beim **EuG**. Das EuG erklärte die Klage für unzulässig und stellte fest, dass der streitige Beschluss keine "**anfechtbare Handlung**" iSd Art 263 Abs 1 AEUV war und dass WhatsApp von diesem Beschluss iSd Art 263 Abs 4 AEUV nicht "unmittelbar betroffen" war. Gegen diese Entscheidung richtet sich das Rechtsmittel von WhatsApp.

Der Generalanwalt hat erwogen: Die Veröffentlichung auf einer Website genügt dem Erfordernis der "**Bekanntgabe**" iSd **Art 263 Abs 6 AEUV**. WhatsApp hat den streitigen Beschluss innerhalb der mit der Veröffentlichung auf der Website des EDSA in Gang gesetzten Fristen angefochten. Somit ist es **für die Zulässigkeit der Nichtigkeitsklage unerheblich**, dass WhatsApp möglicherweise **vor** der vorgeschriebenen Veröffentlichung vom **wesentlichen Inhalt** dieses Beschlusses Kenntnis erlangt hat.

Es reicht für die Beantwortung der Frage, ob eine **Klage zulässig** ist, nicht aus, dass die fragliche Handlung verbindliche Rechtswirkungen gegenüber ihrem Adressaten oder gegenüber einer anderen Person erzeugt; vielmehr muss der EuGH auch prüfen, ob die fragliche Handlung die **Rechtsstellung des Klägers beeinträchtigt** (Art 263 Abs 4 AEUV).

Das EuG hat die Voraussetzungen des **Art 263 Abs 1 AEUV fehlerhaft beurteilt**. Es hat darauf fokussiert, dass der streitige Beschluss nicht der endgültige Beschluss im Rahmen des in der DSGVO vorgesehenen Kohärenzverfahrens ist. Jedoch hat es nicht geprüft, ob es sich bei diesem Beschluss um einen **endgültigen** oder **abschließenden Beschluss des EDSA handelt**, der für die DPC **verbindliche Rechtswirkungen** entfaltet.

Um die Frage der unmittelbaren Betroffenheit zu beurteilen, ist auf **das Wesen der angefochtenen Handlung abzustellen**. Insoweit genügt es, dass der Inhalt des streitigen Beschlusses, der die Rechtsstellung von WhatsApp beeinträchtigt, der DPC in den relevanten Punkten **keinen Ermessensspielraum** einräumte.

Nach der **Logik des Rechtsschutzsystems** der Union hätte die Nichtigkeitsklage nicht für unzulässig erklärt werden dürfen.

#### Aus der Rechtsprechung des EuG:

- Das EuG hat sich um einen **fairen Ausgleich** zwischen der **Veröffentlichung von Gerichtsentscheidungen** und dem **Recht auf Schutz personenbezogener Daten** sowie des **Geschäftsgeheimnisses** unter

den Umständen des jeweiligen Falles zu bemühen. Die Namen natürlicher Personen (hier: **Trader, Angestellte und Sachverständige**) wie auch die Namen der sie **beschäftigenden Gesellschaften** sind zu **anonymisieren**. Für eine vertrauliche Behandlung von über **13 Jahre alten relativen Daten** oder **Schätzdaten** gibt es keinen Anlass ([EuG 26.03.2025, T-441/21, UBS Group und UBS/Kommission](#)).

#### **Rechtsprechung der Justiz**

##### Aus der Rechtsprechung der Justiz:

- Ob das **Anbieten von Streamingdiensten**, bei denen **digitale Inhalte** (zB Video- oder Audiodateien) über das Internet "*live*" oder "*on demand*" zur Verfügung gestellt werden, unter den Begriff der "**digitalen Inhalte**" oder "**digitalen Dienstleistungen**" iSd RL 2011/83/EU (**VerbraucherrechteRL**) fällt, kann nicht eindeutig abgegrenzt werden. Da Rechtsprechung des EuGH fehlt, die sich mit der **Abgrenzung** zwischen digitalen Inhalten und digitalen Dienstleistungen auseinandersetzt, wird das Verfahren mit Beschluss ausgesetzt und diese Frage wird dem EuGH zur Vorabentscheidung vorgelegt ([OGH 19.03.2025, 9Ob48/24k](#)).
- **Datenbetrug** setzt voraus, dass der Täter zur Täuschung (iSd § 146 StGB) zur automationsunterstützten Datenverarbeitung aufbereitete (**personenbezogene** oder nicht personenbezogene) "falsche" oder "verfälschte" Daten oder Programme benützt. Die Angeklagte bestellte mit **falschen Daten Waren bei Versandhändlern auf Rechnung**. Dies genügt jedoch nicht, um zu beurteilen, ob die tatbestandsmäßige Täuschung erfolgt ist. Die Rechtssache ist im Umfang der Aufhebung an das Erstgericht zurückzuverweisen ([OGH 25.02.2025, 11Os7/25a](#)).
- Der Kläger strebt im Wesentlichen die **Unterlassung** des Einbaus eines digitalen Strommessgeräts ("**Smart-Meter**") an. Das **LG St. Pölten** hat dem EuGH ua Fragen zur Datenverarbeitung in Stromnetzen und zur Vereinbarkeit des **§ 1 Abs 6 Intelligente Messgeräte-Einführungsv** mit der DSGVO zur Vorabentscheidung vorgelegt. Der Beantwortung der Fragen des LG St. Pölten kommt teilweise auch für dieses Verfahren Bedeutung zu, weshalb dieses Verfahren bis zur Entscheidung des EuGH zu unterbrechen ist ([OGH 18.02.2025, 6Ob218/24p](#)).
- Ein Verstoß gegen **§ 63 DSGVO (Datenverarbeitung in Gewinn- oder Schädigungsabsicht)** ist ein **Offizialdelikt**. Ein Verstoß gegen § 111 StGB (üble Nachrede) ist ein Ermächtigungsdelikt. Nach § 196a Abs 1 StPO hat ein Beschuldigter bei Einstellung des Strafverfahrens Anspruch auf einen Pauschalersatz seiner Verteidigungskosten. Der

**Ersatzanspruch entfällt** jedoch, wenn eine **Verfolgungsermächtigung zurückgezogen** wird. Die Staatsanwaltschaft stellte das Verfahren wegen § 63 DSG mangels Vorliegen der Tatbestandsvoraussetzungen und hinsichtlich übler Nachrede wegen fehlender Ermächtigung ein. Dennoch besteht Anspruch auf den Pauschalersatz, weil bereits ursprünglich keine Ermächtigung für die Verfolgung der üblen Nachrede vorlag und insofern die Ermächtigung nicht zurückgezogen wurde ([OLG Wien 27.08.2024, 17Bs267/24z](#)).

### Rechtsprechung des BVwG

BVwG 18.02.2025, W129 2303356-1

#### **Universität, Satzung, Videoaufzeichnungen**

- Der Rektor einer Universität erließ zwei Beschlüsse, um festzulegen, dass bei Departmentsitzungen **Audioaufzeichnungen zu Protokollierungszwecken** zulässig sind und die Aufnahmen nach Genehmigung des Protokolls "umgehend zu löschen" sind. Der Bundesminister für Bildung, Wissenschaft und Forschung ("**Wissenschaftsminister**") behob beide Beschlüsse mit einem Bescheid. Gegen diesen Bescheid erhob der Rektor der Universität eine erfolglose Bescheidbeschwerde.

Das BVwG hat erwogen: Gemäß Art 81c Abs 1 B-VG dürfen Universitäten "im Rahmen der Gesetze" autonom handeln und "**Satzungen**" erlassen. Diese sog **Verordnungskompetenz** der Universitäten unterliegt nur einer **verdünnten Gesetzesbindung**. Verordnungen der Universitätsorgane dürfen zwar nicht gegen bestehende Gesetze verstoßen, sie bedürfen aber keiner gesetzlichen Grundlage; das Gesetz ist für das Handeln der Universitätsorgane **Schranke**, aber nicht unabdingbare Grundlage.

Mangels Einhaltung der universitätsrechtlichen Erzeugungsvorschriften kam eine Qualifikation der verfahrensgegenständlichen Beschlüsse als Satzungsbestandteil (und damit als Verordnung) jedoch nicht in Betracht. Ebenso wenig handelte es sich bei den Beschlüssen um eine Geschäftsordnung des Rektorats, weil sich die entsprechenden universitätsrechtlichen Grundlagen in einer personellen Zuweisung von Aufgaben durch den Rektor erschöpfen. Daraus folgt, dass die beiden Beschlüsse **keine geeignete Rechtsgrundlage** hatten, weshalb sie in **Widerspruch zu den Grundsätzen der DSGVO** stehen. Die Aufhebung der beiden Beschlüsse durch den Wissenschaftsminister erfolgte somit zu Recht.

BVwG 14.02.2025, W211 2299661-1

#### **Streitanhängigkeit, entschiedene Sache, Beschwerdeergänzung**

- Ein **Betroffener** brachte Datenschutzbeschwerde bei der DSB ein. Noch bevor ein Bescheid der DSB ergangen war, brachte der Betroffene einen neuen Schriftsatz ein, den er als "Beschwerde" betitelte aber mit den Worten einleitete "*Ergänzend zu meiner Beschwerde*". Die DSB deutete den Schriftsatz als "neue" Datenschutzbeschwerde und wies ihn wegen entschiedener Sache zurück. Der Betroffene erhob daher eine (erfolgreiche) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Ist eine Datenschutzbeschwerde durch die DSB zurückgewiesen worden, ist Sache des Beschwerdeverfahrens nur die Frage der **Rechtmäßigkeit der Zurückweisung**.

Die Zurückweisung wegen **entschiedener Sache** kommt nur in Frage, wenn die Angelegenheit durch einen rechtskräftigen **Vorbescheid** entschieden ist. Einen solchen Vorbescheid gab es nicht, weil die ursprüngliche Datenschutzbeschwerde bei der DSB noch anhängig war. Ungewiss war es auch, ob die DSB überhaupt ein Bescheid erlassen wird. Das **Rechtsinstitut der Streitanhängigkeit** iSd § 233 ZPO kennt das AVG nicht. Jeder Schriftsatz bedarf einer Auslegung nach dessen **objektiven Erklärungswert**. Wenn ein Schriftsatz mit "Ergänzend zu meiner Beschwerde" eingeleitet wird, ist davon auszugehen, dass es sich bei diesem Schriftsatz um eine **Beschwerdeergänzung** und um keine neue Beschwerde handelt. Auch aus diesem Grund war von keiner entschiedenen Sache auszugehen.

BVwG 11.02.2025, W254 2295624-1

#### **Auskunft, Empfänger, Zeitpunkt der Erteilung, Löschung, Widerspruch**

- Ein Wohnungseigentümer stellte Auskunftersuchen an seine Hausverwaltung. In der ihm erteilten Auskunft wurden nur die Empfängerkategorien, nicht jedoch die konkreten Empfänger benannt, weshalb der Wohnungseigentümer sich bei der DSB beschwerte. Die Hausverwaltung erteilte eine ergänzende Auskunft und beauskunftete die **konkreten Empfänger** samt **Übermittlungsgrund** und **Inhalt der übermittelten Daten**. Die DSB stellte daher das **Vorverfahren** gemäß **§ 24 Abs 6 DSGVO** ein.

Noch am selben Tag erhob der Wohnungseigentümer eine weitere Datenschutzbeschwerde, mit der er geltend machte, dass die **Auskunft** weiterhin **unvollständig und unrichtig** sei. Weiters machte er Verletzungen in seinen **Rechten auf Löschung** und **Widerspruch** geltend. Die DSB wies die Datenschutzbeschwerde in allen drei Punkten ab und stellte ua fest, dass Gegenstand der

datenschutzrechtlichen Auskunft die zum **Zeitpunkt des Einlangens des Auskunftersuchens** tatsächlich verarbeiteten Daten sind. Die vom Wohnungseigentümer erhobene Bescheidbeschwerde blieb erfolglos.

Das BVwG hat erwogen: Weder das DSG noch die DSGVO sehen in Bezug auf das Recht auf Auskunft die **Feststellung vergangener Rechtsverletzungen** vor, weshalb der Wohnungseigentümer durch die allenfalls verspätete Auskunftserteilung **nicht in seinem Recht auf Auskunft verletzt** ist.

Die **Verarbeitung** personenbezogener Daten ist ua dann **rechtmäßig**, wenn diese zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich ist, welcher der Verantwortliche unterliegt (Art 6 Abs 1 lit c DSGVO). Gemäß **§ 24 Abs 5 WEG 2002** sind **Beschlüsse** der Eigentümergeinschaft jedem Wohnungseigentümer sowohl durch **Anschlag** an einer deutlich sichtbaren Stelle des Hauses als auch durch Übersendung schriftlich **zur Kenntnis zu bringen**. Gemäß Abs 6 *leg cit* kann jeder Wohnungseigentümer **innerhalb eines Monats** ab Anschlag verlangen, dass die **Rechtsunwirksamkeit** des Beschlusses, zB wegen formeller Mängel, **gerichtlich festgestellt wird**. Der Wohnungseigentümer hat den verfahrensgegenständlichen Beschluss nicht angefochten. Daher ist dieser in Rechtskraft erwachsen.

Es ist dem Wohnungseigentümer verwehrt, über den Umweg des Datenschutzrechts eine Aufhebung dieses Beschlusses zu erwirken. Eine Datenschutzbeschwerde kann nicht dazu dienen, über die in die Zuständigkeit anderer Behörden bzw Gerichte fallenden Fragen zu entscheiden. Vor diesem Hintergrund besteht auch **kein Recht** des Wohnungseigentümers auf **Widerspruch gemäß Art 21 DSGVO** und **Löschung gemäß Art 17 DSGVO**.

Die Hausverwaltung ist verpflichtet, den Wohnungseigentümern gemäß § 34 WEG eine ordentliche und **richtige Abrechnung** zu legen. Auf Verlangen muss sie zudem jedem Wohnungseigentümer **Auskunft über Namen und Zustellanschriften** der übrigen Wohnungseigentümer erteilen, soweit dies zur Verständigung iZm der Ausübung von eigentümerbezogenen Rechten und Gestaltungsmöglichkeiten erforderlich ist. Hierfür ist die Verarbeitung von personenbezogenen Daten der einzelnen Wohnungseigentümer erforderlich. Ist die Datenverarbeitung für eine **rechtliche Verpflichtung** erforderlich, besteht kein **Recht auf Widerspruch**.

BVwG 17.02.2025, W274 2302842-1

### **Geheimhaltung, veröffentlichte Daten, Einwilligung**

- Ein Anrainer fühlte sich durch das in unmittelbarer Nähe liegende Nassholzlager gestört, weil es aufgrund mangelnder Wasserabflussrinnen zu enormen Mücken-, Gelsen und Insektenplagen kam. Vor diesem Hintergrund richtete er ein Auskunftersuchen an die **Bezirkshauptmannschaft ("BH")**, um einvernehmlich rechtliche und organisatorische Möglichkeiten mit dem Betreiber des Holzlagers auszuloten und das Problem zu lösen. Die BH leitete die E-Mail des Anrainers inklusive seines Namens, Adresse, E-Mail-Adresse und Handynummer an den Betreiber weiter und forderte diesen zur Stellungnahme auf. Daraufhin erhob der Anrainer eine Datenschutzbeschwerde bei der DSB, weil er sich durch die Weitergabe seiner Daten an den Betreiber in seinem **Recht auf Geheimhaltung** verletzt erachtete. Die DSB stellte hinsichtlich der Weitergabe der E-Mail-Adresse und der Handynummer eine Verletzung seines Rechts auf Geheimhaltung fest. Dagegen erhob die BH eine (erfolgreiche) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Gemäß § 1 DSG hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Dass bestimmte personenbezogene **Daten veröffentlicht** sind, führt nicht zur Annahme, dass das Datenschutzregime dafür nicht gelte. Sofern zulässigerweise veröffentlichte Daten nicht bloß reproduziert werden, sondern ein neues Element mit diesen Daten verknüpft wird, handelt es sich bei dieser Verknüpfung um eine Verarbeitung gemäß Art 4 Z 2 DSGVO.

Nach dem **objektiven Erklärungswert** ist das hinzufügen des Namens, der Adresse, der E-Mail-Adresse und Handynummer durch den Anrainer jedoch so zu verstehen, dass die BH diese Daten für die vom Anrainer gewünschten Bemühungen einer **raschen und einvernehmlichen Lösung** des Problems gegenüber dem Betreiber nutzen durfte.

Eine **Einwilligung** iSd DSGVO ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung. Aus Sicht der BH hat der Anrainer seine Kontaktdaten freiwillig preisgegeben, um sie zur Lösung des Problems einzusetzen. Es war **kein Hinweis** hinzugefügt, dass diese Daten durch die BH nur in eingeschränkter Weise verwendet werden durften. Da der Anrainer angab, zuvor bereits selbst an den Betreiber herantreten zu sein, ist davon auszugehen, dass er im Rahmen dessen bereits seine E-Mail-Adresse oder Handynummer offengelegt hatte.

Daher ist anzunehmen, dass die personenbezogenen Daten aufgrund einer

Einwilligung durch die BH verarbeitet wurden. Betroffene können nämlich auch **wirksam** eine Einwilligung zur Datenverarbeitung erteilen, **ohne dass ihnen vorab nähere Informationen bereitgestellt werden**. Die BH hat nicht auf öffentlich zugängliche Daten des Anrainers zugegriffen und diese verarbeitet, sondern jene Daten weitergeleitet, die ihr verfahrenseinleitend vom Anrainer übermittelt wurden. Zudem war die Handynummer des Anrainers durch Eingabe seines Vor- und Nachnamens in der Suchmaschine Google auffindbar und somit **allgemein zugänglich**. Dies steht der Feststellung einer Geheimhaltungspflichtverletzung gemäß § 1 DSGVO entgegen.

Aus der weiteren Rechtsprechung des BVwG:

- Eine **Wildkamera** kann, durch einen **Bewegungsmelder** ausgelöst, Aufnahmen machen und ist daher von anderen Formen der Videoüberwachung nicht zu unterscheiden. Durch die Wildkamera erfolgte eine **grundsätzlich permanente Beweissicherung** ua zwecks **Gewinnung von Beweismitteln für ein zivilrechtliches Verfahren**. Eine **Erforderlichkeit** der durchgeführten Datenverarbeitungen war jedoch nicht gegeben, weil ein gelinderes Mittel zur Verfügung stand, nämlich die **anlassfallbezogene Aufnahme** von Lichtbildern **mittels Handkamera** ([BVwG 14.02.2025, W211 2288888-1](#)).
- In einem **Zivilverfahren** betreffend eine mögliche Einschränkung von **Dienstbarkeiten** sind **Lichtbilder** ein wesentlicher Bestandteil des zwingend zu erstattenden Vorbringens des Klägers. Die **Erforderlichkeit** der Datenverarbeitung in Verbindung mit den berechtigten Interessen der **Geltendmachung und Verteidigung von Rechtsansprüchen** ist aus einer **ex ante-Sicht** zu prüfen und ausreichend **weit auszulegen**. Die Verarbeitung eines Lichtbilds zu einem **konkreten Anlassfall** ist zur Geltendmachung oder Verteidigung von **Rechtsansprüchen** zulässig ([BVwG 14.02.2025, W211 2288825-1](#)).
- Eine Abfrage von **Fremddaten** (Daten aus einem Fremddatensystem) im **Polizeilichen Akten-dokumentationssystem (PAD)**, die nicht im Rahmen der dienstlichen Aufgabenerfüllung erfolgt, ist verboten. Eine Beamtin hat sich der Ausübung des Amtes zu enthalten und ihre Vertretung zu veranlassen, wenn ihre **volle Unbefangenheit** in Zweifel gezogen werden kann. Ein **Disziplinarverstoß** ist verwirklicht, wenn aus **Freundschaft** Fremddaten abgefragt werden ([BVwG 14.02.2025, W208 2307243-1](#)).
- Allfällige **datenschutzrechtliche Bedenken stehen** der Vorschreibung des **ORF-Beitrags** nicht entgegen. Das BVwG ist

zudem für datenschutzrechtliche Anbringen nur **zuständig**, wenn eine Bescheidbeschwerde sich gegen einen Bescheid der DSB richtet ([BVwG 04.02.2025, G314 2296792-1](#); [G314 2296798-1](#)).

### Rechtsprechung des BFG

Aus der Rechtsprechung des BFG:

- Datenschutzrechtliche Bestimmungen verfolgen nicht den Zweck, die **Erhebung der Abgaben zu erschweren**. Die Vorlage von für die Festsetzung der Abgabe erforderlichen Unterlagen kann daher aus datenschutzrechtlichen Gründen nicht verweigert werden ([BFG 03.03.2025, RV/7102539/2021](#)).

### Rechtsprechung der DSB

DSB 11.02.2025, 2024-0.195.679

#### **Straßenfotografie, Kunstfreiheit, Fotos**

- Ein **Straßenfotograf** fertigte auf der Straße Fotos von Menschen – ua auch Kindern – an und veröffentlichte diese auf seiner Website. In einigen Fällen ließen die Bilder Rückschlüsse auf die Religionszugehörigkeit der abgebildeten Personen zu, und auf einem Foto war ein erheblicher Teil des Ausschnitts einer Betroffenen zu sehen. Die DSB wurde durch eine anonyme Anzeige darauf aufmerksam gemacht und leitete ein amtswegiges Prüfverfahren gemäß Art 58 Abs 1 lit b DSGVO ein.

Die DSB hat erwogen: Gemäß Art 8 GRC bzw § 1 DSGVO hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Gemäß Art 13 GRC bzw § 17a StGG sind **Kunst und Forschung frei**. Art 85 Abs 2 DSGVO legt fest, dass für die Verarbeitung zu wissenschaftlichen, **künstlerischen** oder literarischen Zwecken Abweichungen von bestimmten Kapiteln der DSGVO zulässig sind, um das Recht auf Schutz der personenbezogenen Daten mit der **Meinungsäußerungsfreiheit** in Einklang zu bringen.

Bei der Verarbeitung personenbezogener Daten nach **§ 9 Abs 2 DSGVO** zu künstlerischen Zwecken finden die Grundsätze des Art 5 DSGVO uneingeschränkt Anwendung. Es bedarf einer Interessenabwägung im Einzelfall, um das Grundrecht auf Datenschutz mit dem **Grundrecht auf Kunstfreiheit** in Einklang zu bringen. Das Anfertigen und die Veröffentlichung der Fotos sind jeweils eine Verarbeitung iSd Art 4 Z 2 DSGVO. Der Straßenfotograf ist der Verantwortliche für die Webseite und die Bildverarbeitungen.

Da die Gesichter der betroffenen Personen auf den Fotos eindeutig ersichtlich und die betroffenen Personen damit identifizierbar sind, sind die fotografischen Abbildungen

personenbezogene Daten. Das **Recht am eigenen Bild** ist eine besondere Erscheinungsform des **allgemeinen Persönlichkeitsrechts**. Bereits die Herstellung eines Bildnisses **ohne Einwilligung** des Abgebildeten kann einen unzulässigen Eingriff in dessen allgemeines Persönlichkeitsrecht darstellen. Minderjährige und Kinder sind als **vulnerable Betroffene besonders schutzbedürftig**. Auch Fotos, aus denen die Religionszugehörigkeit hervorgeht, auf welchen ein großer Teil des Ausschnitts zu sehen ist oder Betroffene beim Essen abbildet, unterliegen einer höheren Schutzwürdigkeit. Die Interessen der Betroffenen überwiegen in Summe den berechtigten Interessen auf Kunstfreiheit des Straßenfotografen. Die Einholung einer Einwilligung vor der Anfertigung des Bildes würde die **Kunstform der Straßenfotografie** zwar weitgehend verunmöglichen, jedoch wäre es dem Straßenfotografen zumutbar gewesen, zumindest im Nachhinein eine Einwilligung einzuholen. Daher ist dem Straßenfotograf aufzutragen, die genannten Fotos innerhalb einer Frist von zwei Wochen zu löschen.



to the point

# Datenschutzmonitor. 14/2025 vom 09.04.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 03.04.2025, 57748/21, *Kulák/Slovakia* (Rechtsanwalt, Kanzleidurchsuchung, Auswertung eines Computers)

EGMR 01.04.2025, 2799/16, *Ships Waste Oil Collector B.V. and Others/the Netherlands* (Telefonabhörung, Datenweitergabe, Beweismittel)

- **Rechtsprechung des EuGH**

EuGH 03.04.2025, C-710/23, *Ministerstvo zdravotníctví* (Vertreter juristischer Personen, personenbezogene Daten, Zugang zu amtlichen Dokumenten)

- **Rechtsprechung des VfGH**

VfGH 25.02.2025, G20/2025 (SKY ECC, § 134 Z 3 StPO, Legaldefinition)

- **Rechtsprechung des VwGH**

VwGH 27.02.2025, Ra 2024/04/0305 (GISA, schlicht-hoheitliches Handeln)

- **Rechtsprechung der Justiz**

OGH 27.02.2025, 8ObA61/24i (Einsichtsrechte des Betriebsrats)

OLG Graz 17.01.2025, 5R205/24t (Auskunft, Vollmacht, Rechtsanwalt, Kostenersatz)

- **Rechtsprechung des BVwG**

BVwG 26.02.2025, W101 2284403-1 (Videoüberwachung, Geldbuße, Strafzumessung)

BVwG 03.02.2025, W292 2289286-1 (Statistik Austria, Namensgleichheit, Register der statistischen Einheiten)

BVwG 11.03.2025, W292 2280453-2 (Videokamera, Rechtsanspruch, Vermieter)

BVwG 24.02.2025, W298 2296144-1 (historische Zahlungsinformationen, Inkasso, Kreditauskunftei, Löschung)

BVwG 24.02.2025, W298 2280884-1 (Exzess, Missbrauchsabsicht, Zurückverweisung)

- **Rechtsprechung der LVwG**

LVwG Tirol 26.03.2025, LVwG-2024/12/2583-3 (Sicherstellung und Auswertung von Mobiltelefonen, DSRL-PJ, vorherige Gerichtskontrolle)

- **EU-Rechtsakte**

Vier DelegierteVOs und eine DurchführungsVO zu Kryptowerte-Dienstleistungen

## To the Point:

### Rechtsprechung des EGMR

EGMR 03.04.2025, 57748/21, Kulák/Slovakia

#### **Rechtsanwalt, Kanzleidurchsuchung, Auswertung eines Computers**

- Ein slowakischer **Rechtsanwalt** geriet im Rahmen einer Korruptionsermittlung ins Visier der slowakischen Strafverfolgungsbehörden. Der Staatsanwalt ordnete die **Sicherung und Herausgabe von Computerdaten** an. Die Durchsuchung erfolgte ohne schriftlichen Durchsuchungsbefehl unter Berufung auf eine **Dringlichkeitssituation**. Der beschlagnahmte Computer wurde vollständig gesichert und blieb fast **fünfzehn Monate** im Gewahrsam der Behörden. Dieser enthielt auch **Mandantendaten**, die nicht im Zusammenhang mit dem anhängigen Ermittlungsverfahren standen. Die Extraktion der Daten erfolgte durch einen gerichtlich bestellten Sachverständigen. Dieser ging jedoch bei der Analyse über die im Sicherstellungsbefehl festgelegten **Suchbegriffe** hinaus.

Der Rechtsanwalt erhob zunächst Beschwerde gegen die Durchsuchung und Sicherstellung. Der Staatsanwalt hielt das Vorgehen für rechtmäßig, weil der tatsächliche Kanzleistandort erst nach der Festnahme bekannt geworden sei und eine Vor-Ort-Sichtung der Daten technisch nicht möglich gewesen sei. In weiterer Folge wandte sich der Rechtsanwalt mit einer Verfassungsbeschwerde erfolglos an das slowakische Verfassungsgericht. Auch eine zweite Verfassungsbeschwerde wegen der Datenauswertung wurde abgewiesen. Der Rechtsanwalt rief daraufhin den EGMR (erfolgreich) an.

Der EGMR hat erwogen: **Durchsuchungen und Beschlagnahmen** in Rechtsanwaltskanzleien greifen in die durch **Art 8 EMRK geschützten Rechte** ein. Sie betreffen insbesondere den **vertraulichen Austausch zwischen Rechtsanwalt und Mandant** sowie das **Anwaltsgeheimnis**, das das Vertrauensverhältnis zwischen beiden schützt und eine **ordnungsgemäße Rechtspflege** gewährleistet. Deshalb bedürfen solche Maßnahmen **besonderer verfahrensrechtlicher Sicherungen**. Die Vertraulichkeit der anwaltlichen Kommunikation unterliegt unabhängig von ihrem Inhalt dem Schutz des Art 8 EMRK. Ein **Verstoß** gegen das **Anwaltsgeheimnis** kann nicht nur das individuelle Vertrauensverhältnis, sondern das **gesamte Rechtssystem gefährden**. Die Durchsuchungen von Kanzleien sind einer besonders strengen Kontrolle zu unterwerfen. Diese setzt die Anwesenheit und **Mitwirkung** einer unabhängigen, **fachkundigen Person** voraus.

Die **Durchsuchung der Kanzlei** des Rechtsanwalts **samt** der **fast**

**fünfzehnmonatigen Beschlagnahme seines** Computers ist ein Eingriff in sein durch Art 8 EMRK geschütztes Recht. Die Dauer hatte **spürbare negative Auswirkungen** auf seine berufliche Tätigkeit.

Eine **gerichtliche ex-post-Überprüfung** der Rechtmäßigkeit der Durchsuchungen war nicht vorgesehen. Die Staatsanwaltschaft ist kein **unabhängiges Gericht** iSd Art 6 EMRK.

Ob **nur verfahrensrelevante Daten am Computer eingesehen wurden**, kann nicht festgestellt werden. Zudem fehlten nationale Regelungen, um vom **Anwaltsgeheimnis** betroffenes oder nicht verfahrensrelevantes Material zu schützen. Der Rechtsanwalt wurde sohin in seinen Rechten nach Art 8 EMRK verletzt.

EGMR 01.04.2025, 2799/16, Ships Waste Oil Collector B.V. and Others/the Netherlands

#### **Telefonabhörung, Datenweitergabe, Beweismittel**

- Mehrere niederländische Unternehmen standen im Fokus strafrechtlicher Ermittlungen wegen Urkundenfälschung und illegaler Entsorgung von Abfall. Im Rahmen dieser strafrechtlichen Untersuchung wurden **Telefonate von Mitarbeitern** abgehört, die Hinweise auf **Preisabsprachen** beinhalteten. Diese Daten wurden an die **niederländische Wettbewerbsbehörde weitergegeben**, die diese nutzte, um gegen wettbewerbsrechtliche Verstöße vorzugehen und schließlich Geldbußen gegen mehrere Unternehmen verhängte. Die Unternehmen erachteten sich ua in ihrem Recht auf Achtung ihres Privatlebens gemäß Art 8 EMRK verletzt und wendeten sich an den EGMR. Der EGMR entschied, dass die Übermittlung und Verwendung abgehörter Daten bei der Verfolgung gerichtlicher Straftaten an eine andere Behörde nicht gegen Art 8 EMRK verstoßen.

Der EGMR hat erwogen: Die **Übermittlung von abgehörten Daten** an eine andere Behörde ist ein **Eingriff in das Recht auf Achtung des Privatlebens** und der **Korrespondenz**. Ein solcher Eingriff muss gesetzlich vorgesehen sein, einem legitimen Ziel dienen und in einer demokratischen Gesellschaft notwendig sein.

Maßgeblich für den Ermessensspielraum der Staaten bei einem Grundrechtseingriff nach Art 8 EMRK ist der **Inhalt der betreffenden Daten**, nicht die physische oder rechtliche Natur oder der Status der Beschwerdeführenden. Um Willkür und Missbrauch zu verhindern, gelten die Mindestgarantien nach Art 8 EMRK für natürliche und **juristische Personen gleichermaßen**.

Die Übermittlung der Daten stützte sich auf eine gesetzliche Grundlage im niederländischen Recht. **Definiert** wurden sowohl die

**übermittelbaren Daten** (strafrechtliche Daten) als auch der **zulässige Zweck** (Durchsetzung von Rechtsvorschriften) sowie der **Kreis potenzieller Empfänger**. Die Umstände, unter denen die Übermittlung von rechtmäßig erlangtem **Abhörmaterial** an eine andere Strafverfolgungsbehörde genehmigt werden durfte, war sohin klar geregelt.

Das niederländische Recht verlangte von der Staatsanwaltschaft auch eine Prüfung der **Erforderlichkeit** und **Verhältnismäßigkeit** der Datenübermittlung. Die Datenübermittlungen dienten dem **legitimen Ziel**, das wirtschaftliche Wohl des Landes zu schützen und das Wettbewerbsrecht durchzusetzen. Die niederländischen Behörden haben die Interessen der Unternehmen mit dem öffentlichen Interesse abgewogen und haben ausreichende Gründe vorgebracht, um die Erforderlichkeit und Verhältnismäßigkeit der Datenübermittlung zum Zweck der Durchsetzung des Wettbewerbsrechts zu rechtfertigen.

Die betroffenen Unternehmen hatten auch die Möglichkeit, die Übermittlung der Daten vor Gericht anzufechten und eine **wirksame gerichtliche Überprüfung** zu erhalten. Eine Abhilfe in Form der Vernichtung übermittelter Daten oder einer finanziellen Entschädigung ist nicht zwingend erforderlich, um ein Rechtsmittel im Zusammenhang mit der Übermittlung von Abhördaten zu gewähren. Einschränkungen ihrer Nutzung, wie beispielsweise eine **Erklärung der Unzulässigkeit als Beweismittel**, können eine ausreichende Abhilfe darstellen. Zudem stand es den Unternehmen offen, die Übermittlungen in zivilrechtlichen Verfahren anzufechten.

### Rechtsprechung des EuGH

EuGH 03.04.2025, C-710/23, Ministerstvo zdravotnictví

#### **Vertreter juristischer Personen, personenbezogene Daten, Zugang zu amtlichen Dokumenten**

- Ein Auskunftswerber begehrte Auskunft über die Vertreter juristischer Personen, die Kaufverträge für COVID-19 Tests mit dem tschechischen Gesundheitsministerium unterzeichneten. Bei der erteilten Auskunft des Ministeriums wurden die **personenbezogenen Daten** dieser Personen, darunter Name, Kontaktdaten und Unterschrift sowie in einigen Fällen auch die Websites der juristischen Personen, **geschwärzt**. Gegen diese Vorgehensweise erhob der Auskunftswerber eine erfolgreiche Klage. Nach Ansicht des Gerichts hätte das Ministerium entsprechend der innerstaatlichen Rechtsprechung den Vertretern der juristischen Personen die Möglichkeit der Stellungnahme einzuräumen gehabt und es hätte zu prüfen gehabt, ob für

die Offenlegung der personenbezogenen Daten eine Rechtsgrundlage nach Art 6 DSGVO vorliegt. Das angerufene Höchstgericht legte dem EuGH die Fragen vor, (i) ob die verfahrensgegenständlichen Daten iSd Art 4 Z 1 DSGVO personenbezogene Daten sind und (ii) ob innerstaatliche Rechtsprechung, die einen Verantwortlichen verpflichtet, Betroffene vor der Datenübermittlung der Daten zu unterrichten, mit dem Unionsrecht vereinbar ist.

Der EuGH hat erwogen: Der Begriff **personenbezogener Daten** ist **weit** auszulegen und erfasst alle Arten von Informationen objektiver und subjektiver Natur einer identifizierten oder identifizierbaren natürlichen Person. Daten natürlicher Personen, die juristische Personen vertreten, **sind personenbezogene Daten**. Der berufliche Kontext begründet keine Ausnahme. Auch der Begriff "**Verarbeitung**" iSd Art 4 Z 2 DSGVO ist **weit** zu verstehen. Die in der Definition enthaltene Aufzählung an Verarbeitungstätigkeiten ist nur **beispielhaft**. Die Übermittlung von personenbezogenen Daten eines Vertreters einer juristischen Person ist eine Verarbeitung.

Mitgliedstaaten können nach Art 6 Abs 2 DSGVO Bestimmungen erlassen, die **spezifische Anforderungen für die Anwendung der Rechtfertigungsgründe** nach Art 6 Abs 1 lit c und e DSGVO festlegen, um eine rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung von Daten zu gewährleisten. Als **Rechtsgrundlage** für die Verarbeitung gemäß Art 6 Abs 1 lit c DSGVO iVm Art 6 Abs 3 DSGVO kann auch **innerstaatliche Rechtsprechung** herangezogen werden. Diese Rechtsgrundlage muss ein im **öffentlichen Interesse** liegendes Ziel verfolgen und in einem **angemessenen Verhältnis** zu dem verfolgten legitimen Zweck stehen. Solche Rechtsgrundlagen können auch spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO, darunter auch allgemeine Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung, enthalten.

Der **Zugang der Öffentlichkeit zu amtlichen Dokumenten** liegt im **öffentlichen Interesse**. Der **Transparenzgrundsatz** der Art 1, Art 10 EUV und Art 15 AEUV soll eine Beteiligung der Bürger am Entscheidungsprozess ermöglichen und Legitimität, Effizienz und Verantwortung der Verwaltung in einer Demokratie gewährleisten.

**Nationale Rechtsprechung**, die für den Zugang zu amtlichen Dokumenten eine Konsultation der von der Offenlegung betroffenen natürlichen Personen vorsieht, steht der DSGVO **nicht entgegen**. Die zusätzliche Verpflichtung darf eine Auskunft aber **nicht verunmöglichen**, einen **unverhältnismäßigen Aufwand** erfordern und nicht zu einer unverhältnismäßigen Einschränkung auf

Zugang zu amtlichen Dokumenten führen. Eine auskunftspflichtige Behörde hat den Zugang der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf **Schutz personenbezogener Daten in Einklang** zu bringen. Eine Behörde darf sich **nicht** systematisch auf die praktische Unmöglichkeit einer Informationserteilung stützen, ohne in irgendeiner Weise zu versuchen, die Interessen der DSGVO und des Öffentlichkeitsrechts miteinander in Einklang zu bringen.

### Rechtsprechung des VfGH

VfGH 25.02.2025, G20/2025

#### **SKY ECC, § 134 Z 3 StPO, Legaldefinition**

- Ein mutmaßlicher **Suchtgifthändler** wurde in erster Instanz (nicht rechtskräftig) zu einer Freiheitsstrafe verurteilt. Diese Verurteilung basierte insbesondere auf ursprünglich verschlüsselten Chatverläufen des Anbieters "**SKY ECC**", die von französischen Behörden entschlüsselt und an österreichische Strafverfolgungsbehörden übermittelt wurden. Der OGH erklärte die Verwertung derartiger Chatverläufe für zulässig. Der mutmaßliche Suchtgifthändler wendete sich mit einem **Parteiantrag** an den VfGH und beantragte, der VfGH möge § 134 Z 3 StPO als verfassungswidrig aufheben. Er brachte im Wesentlichen vor, dass (i) die Auffassung des OGH den Vorgaben des VfGH im Erkenntnis [VfSlg 20.356/2019](#) (Bundestrojaner) widerspricht, (ii) die Chatverläufe einem Beweismittelverbot unterliegen, und (iii) der OGH den § 134 Z 3 StPO verfassungswidrig auslegt. Der VfGH wies den Antrag zurück.

Der VfGH hat erwogen: Bei Gesetzesprüfungsverfahren ist der Anfechtungsumfang der Norm bei sonstiger Unzulässigkeit des Prüfungsantrags nicht zu eng zu wählen. Insbesondere darf der verbleibende Gesetzesteil nicht einen völlig veränderten Inhalt bekommen und es müssen auch die mit der aufzuhebenden Gesetzesstelle untrennbar zusammenhängenden Bestimmungen erfasst werden. Es sind also alle Normen anzufechten, die für die Beurteilung der allfälligen Verfassungswidrigkeit eine untrennbare Einheit bilden. **Legaldefinitionen** kommt **keine eigenständige normative Bedeutung zu**. Diese wird erst im Zusammenhang mit anderen Regelungen, die diesen Begriff verwenden, bewirkt. Die angefochtene Bestimmung ist eine Legaldefinition ohne eigenständige normative Wirkung (arg: Überschrift **§ 134 StPO** "Definitionen"), legt also lediglich fest, was eine "**Überwachung von Nachrichten**" iSd Gesetzes ist. Da lediglich die Legaldefinition des § 134 Z 3 StPO isoliert angefochten wird, ist der Prüfungsumfang zu eng gewählt und der Antrag ist zurückzuweisen. **Anm: Mit dem Fall "SKY ECC" haben wir uns im Schönherr Datenschutzmonitor bereits mehrfach beschäftigt.**

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Die Eintragung ins **Gewerbeinformationssystem Austria ("GISA")** ist **schlicht-hoheitliches Handeln**. Einzutragen sind ua die genaue Bezeichnung des Gewerbes, das Datum des Entstehens und der Beendigung der Gewerbeberechtigung, die Firma und die Firmenbuchnummer oder die ZVR-Zahl. Die Eintragung hat die zuständige Behörde vorzunehmen, das **Verwaltungsgericht** darf nur feststellen, dass die Eintragung vorzunehmen ist ([VwGH 27.02.2025, Ra 2024/04/0305](#)).

### Rechtsprechung der Justiz

Aus der Rechtsprechung der Justiz:

- Die bloße Wiederholung der an die zweite Instanz erstatteten Ausführungen ist keine gesetzmäßige Ausführung eines Rechtsmittels an ein Höchstgericht. Die Entscheidung des [OGH vom 28.06.2023, 9 ObA 51/22y](#), besagt nicht, dass **Einsichtsrechte des Betriebsrats** durch die DSGVO nicht beschnitten werden können ([OGH 27.02.2025, 8ObA61/24i](#)).
- Hat der Verantwortliche Zweifel an der Identität eines Betroffenen iSd Art 15 DSGVO, kann er nach Art 12 Abs 6 DSGVO weitere Informationen zu dessen **Identifizierung** einfordern. Mit der **bloßen Berufung eines Rechtsanwalts auf eine Vollmacht** gemäß § 8 Abs 1 RAO kann die Bevollmächtigung nur beim Einschreiten vor einer Behörde oder vor einem Gericht nachgewiesen werden. Eine Vollmacht bedarf einer **Unterschrift** oder **einer qualifizierten elektronischen Signatur** iSd § 4 Abs 1 S 1 Signatur- und Vertrauensdienstegesetzes. Fehlt eine entsprechende Unterschrift, hat der Verantwortliche keinerlei Grundlage dafür, von einer Bevollmächtigung auszugehen und darf die Auskunft verweigern. Bringt der Betroffene anschließend Klage ein und erteilt der Verantwortliche daraufhin die Auskunft, hat der Verantwortliche keinen Grund zur Klagsführung gegeben. Der Betroffene trägt – als Kläger – gemäß § 45 ZPO die Kosten des Verfahrens und hat dem Verantwortlichen **Kostenersatz** zu erstatten ([OLG Graz 17.01.2025, 5R205/24t](#)).

### Rechtsprechung des BVwG

BVwG 26.02.2025, W101 2284403-1

#### **Videoüberwachung, Geldbuße, Strafzumessung**

- Die Betreiberin einer Kfz-Werkstatt installierte in einem Zeitraum von knapp zwei Jahren eine **Videoüberwachungsanlage** im Bereich der straßenseitigen Einfahrt, um ihr Eigentum sowie das Eigentum ihrer Kunden

zu schützen. Der Aufnahmebereich der Anlage erfasste einen Teil des an die Werkstatt angrenzenden öffentlichen Gehsteigs sowie einen Teil der öffentlichen Gemeindestraße. Die Aufzeichnungen der Videoüberwachungsanlage wurden für einen **Zeitraum von 24 Stunden gespeichert** und in der Folge automatisch gelöscht. Die DSB stellte die Rechtswidrigkeit des Betriebs der Videoüberwachungsanlage sowie eine Verletzung der Informationspflichten fest und verhängte über die Werkstattbetreiberin eine Geldstrafe iHv EUR 3.190 zzgl EUR 319 als Beitrag zu den Kosten des Verwaltungsstrafverfahrens. Dagegen erhob die Werkstattbetreiberin Bescheidbeschwerde an das BVwG. Das BVwG gab der Bescheidbeschwerde dem Grunde nach keine Folge, setzte die Geldstrafe jedoch auf EUR 1.100 (zzgl EUR 110 Verfahrenskosten) herab.

Das BVwG hat erwogen: Die Werkstattbetreiberin hat zwar ein **rechtfertigendes Interesse** iSd Art 6 Abs 1 lit f DSGVO am Betrieb der Bildaufnahme vorgebracht (Schutz ihres Eigentums, Schutz des Eigentums ihrer Kunden, Ausforschung potenzieller Straftäter). Allerdings hat die Videokamera maßgebliche Bereiche des – vor der Werkstatt liegenden – **öffentlichen Raums** erfasst. Die diesen Bereich frequentierenden Passanten müssen vernünftigerweise nicht damit rechnen, im öffentlichen Raum gefilmt zu werden. Zur Zweckerfüllung war es nicht notwendig, (auch) diesen öffentlichen Raum zu überwachen, sodass den Grundsätzen der Datenminimierung nicht genüge getan wurde. Zudem hat die Werkstattbetreiberin die Videoüberwachungsanlage weder **gekennzeichnet** noch die betroffenen Personen in sonstiger Weise **informiert**.

Für die **Strafzumessung** ist jedoch zu berücksichtigen, dass die aufgenommenen Bilddaten automatisch **nach 24 Stunden gelöscht** wurden und es lediglich ein **einziges Mal zu einer "Nachschau" des Bildmaterials** – in Folge eines Parkschadens im Eingangsbereich der Werkstatt – kam. Ferner war die Werkstattbetreiberin **unbescholten** und sie hat nach Zustellung der Aufforderung zur Rechtfertigung die gegenständliche Verarbeitung **unverzüglich eingestellt**.

BVwG 03.02.2025, W292 2289286-1

### **Statistik Austria, Namensgleichheit, Register der statistischen Einheiten**

- Ein Landwirt führt einen landwirtschaftlichen Betrieb als Einzelunternehmer und wohnt mit seinem Vater an derselben Adresse. Beide tragen denselben Vor- und Nachnamen. Der Landwirt führt darüber hinaus die akademischen Titel "Dipl.-Ing." und "Dr.", sein Vater nicht. Im Rahmen einer agrarstatistischen Erhebung versendete die

Bundesanstalt Statistik Österreich (**Statistik Austria**) ein behördliches Schreiben mit Zugangsdaten (Anmeldennamen, Passwort, Aktivierungscode sowie Betriebsnummer) zu einem elektronischen Fragebogen. Die Sendung war korrekt an den Landwirt adressiert, enthielt jedoch nicht dessen akademische Titel. Sie wurde ohne Zustellnachweis übermittelt und von dem **namensgleichen Vater** entgegengenommen. Daraufhin brachte der Landwirt eine Datenschutzbeschwerde bei der DSB wegen Verletzung im Recht auf Geheimhaltung ein.

Die DSB stellte einen Verstoß gegen den Grundsatz des Art 5 Abs 1 lit f DSGVO (Integrität und Vertraulichkeit) fest, weil bei der Verfügung der Zustellung die akademischen Titel des Empfängers nicht als zusätzliches Identifikationskriterium verwendet wurden. Dagegen erhob die Statistik Austria eine (erfolgreiche) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die Statistik Austria ist gemäß § 22 Abs 1 Bundesstatistikgesetz 2000 eine Anstalt öffentlichen Rechts des Bundes. Sie ist als Verantwortliche des öffentlichen Bereichs und als staatliche Behörde iSd § 1 Abs 2 DSG zu qualifizieren. Gemäß **§ 4 Abs 1 Z 3 Bundesstatistikgesetz 2000** haben die Organe der Bundesstatistik die Statistiken zu erstellen und die statistischen Erhebungen durchzuführen, die durch eine Verordnung angeordnet sind. Gemäß **§ 5 Abs 1 Agrarstrukturstatistik-Verordnung 2023** hat die Statistik Austria für die Befragung einheitliche Erhebungsunterlagen (elektronischer Fragebogen samt Erläuterungen) zu erstellen und diese den Auskunftspflichtigen zur Verfügung zu stellen.

Die **Zustellung** hätte auch mit **Angabe der akademischen Titel** des Landwirts nicht verhindert werden können (§ 5 ZustG). Vielmehr wäre diese nur durch eine **Eigenhandzustellung** (§ 21 ZustG) auszuschließen gewesen.

Für die Rechte und Freiheiten des Landwirts war mit der Übersendung kein besonderes Risiko verbunden. **Art 5 Abs 1 lit f DSGVO** verlangt die Ergreifung von Maßnahmen, die ein dem Risiko **angemessenes Schutzniveau gewährleisten**. Die Statistik Austria hatte die Adressdaten zum Zweck der **Zustellverfügung** aus dem von ihr geführten **Register der statistischen Einheiten** gemäß § 25a Abs 1 Z 1 iVm § 25 Abs 1 Z 1 Bundesstatistikgesetz 2000 zu ermitteln, eine weitere Pflicht zur Abfrage öffentlicher Register bestand nicht.

Es gibt bundesweit kein öffentliches Register, aus welchem rechtssicher und aktuell hervorgeht, welche akademischen Titel von einer bestimmten Person geführt werden dürfen. Auch **besteht keine gesetzliche Verpflichtung**, akademische Titel in das

geführte Register einzutragen. Zudem sind **akademische Titel** rechtlich **kein Bestandteil eines Namens** einer natürlichen Person. Ein Verstoß gegen Art 5 Abs 1 lit f DSGVO bzw Art 32 DSGVO liegt somit nicht vor.

#### Aus der weiteren Rechtsprechung des BVwG:

- Eine Verantwortliche darf zur Wahrung ihres berechtigten Interesses (Art 6 Abs 1 lit f DSGVO) **drei Videokameras** betreiben, wenn dies zur **Verfolgung und Verteidigung von Rechtsansprüchen** iZm **Rechtsstreitigkeiten**, die zwischen dem Betroffenen und der Verantwortlichen sowie deren Vermieter **anhängig** sind, erforderlich und verhältnismäßig ist ([BVwG 11.03.2025, W292 2280453-2](#)).
- Bonitätsdaten (wie **historische Zahlungsinformationen**), die nicht aus dem Insolvenzregister stammen, sondern von einem **Inkassounternehmen** an eine **Kreditauskunftei** rechtmäßig offengelegt wurden, sind **ein Jahr** nach der **nachweislich positiven Erledigung** der Forderung zu **löschen** ([BVwG 24.02.2025, W298 2296144-1](#)).
- Ist der Sachverhalt von der DSB nur im Hinblick darauf ermittelt worden, dass die **Anzahl der bei der DSB** eingebrachten Datenschutzbeschwerden ermittelt wurde, ist eine Ermittlung des Sachverhalts anhand der Datenschutzbeschwerde komplett unterblieben. Nach dem Urteil des [EuGH vom 09.01.2025, C-416/23, Österreichische Datenschutzbehörde \(Demandes excessives\)](#), liegt der Tatbestand der **Exzessivität** nur vor, wenn eine **Missbrauchsabsicht** des Betroffenen nachgewiesen wird. Die Ermittlung der Anzahl der eingebrachten Datenschutzbeschwerden genügt nicht. Der Bescheid der DSB ist daher aufzuheben und die Angelegenheit ist zur Erlassung eines neuen Bescheides an die DSB **zurückverwiesen** ([BVwG 24.02.2025, W298 2280884-1](#)).

#### **Rechtsprechung der LVwG**

##### Aus der Rechtsprechung der LVwG:


- Die **Auswertung eines sichergestellten Datenträgers**, wie zB eines **Mobiltelefons**, ist eine eingriffsintensive und weitreichende Ermittlungsmaßnahme. Sämtliche auf einem Datenträger (lokal oder extern) gespeicherte Daten, einschließlich des Zugriffs auf **externe Speichermedien** (zB Netzwerksysteme oder Clouds), können ausgewertet werden. Die Strafverfolgungsorgane können dadurch (i) auf weit in der **Vergangenheit liegende Daten** des Betroffenen zugreifen, (ii) sie können **umfassende Verhaltens- und Bewegungsprofile** der Betroffenen erstellen, (iii) die eingesetzten **Algorithmen**

**oder Suchbegriffe** können sich auf das Ergebnis der Auswertung auswirken, (iv) die vorhandenen Daten können mit anderen Daten der Strafverfolgungsorgane **verknüpft werden** und (v) bei einer etwaigen **Veränderung von Daten** kann nur nachvollzogen werden, dass eine Veränderung stattgefunden hat. Bereits der **Versuch** von Polizeibehörden, ein Mobiltelefon für Zwecke der strafrechtlichen Ermittlung auszuwerten, fällt in den Anwendungsbereich der EU-DatenschutzRL für Polizei und Justiz 2016/680 (**DSRL-PJ**). Liegt kein begründeter Eilfall vor, ist ohne **vorangehende Kontrolle durch ein Gericht** sohin die gesamte **Sicherstellung des Mobiltelefons rechtswidrig** ([LVwG Tirol 26.03.2025, LVwG-2024/12/2583-3](#)).

#### **EU-Rechtsakte**

- Am **31.03.2025** sind die (i) "*Delegierte Verordnung (EU) 2025/300 der Kommission vom 10. Oktober 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch **technische Regulierungsstandards** für die zwischen **zuständigen Behörden auszutauschenden Informationen***", [ABI L 2025/300](#); (ii) "*Delegierte Verordnung (EU) 2025/305 der Kommission vom 31. Oktober 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch **technische Regulierungsstandards** zur Festlegung der in einen **Antrag auf Zulassung** als Anbieter von Krypto-Dienstleistungen aufzunehmenden **Angaben***", [ABI L 2025/305](#); (iii) "*Delegierte Verordnung (EU) 2025/413 der Kommission vom 18. Dezember 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch **technische Regulierungsstandards** zur Festlegung des **genauen Inhalts der Informationen**, die für die Beurteilung einer geplanten **Übernahme einer qualifizierten Beteiligung** an einem **Emittenten eines vermögenswertereferenzierten Tokens** erforderlich sind*", [ABI L 2025/413](#); (iv) "*Delegierte Verordnung (EU) 2025/414 der Kommission vom 18. Dezember 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch **technische Regulierungsstandards** zur Festlegung des **genauen Inhalts der Informationen**, die für die Beurteilung einer geplanten **Übernahme einer qualifizierten Beteiligung** an einem **Anbieter von Kryptowerte-Dienstleistungen** erforderlich sind*", [ABI L 2025/414](#); sowie die (v) "*Durchführungsverordnung (EU) 2025/306 der Kommission vom 31. Oktober 2024 zur Festlegung **technischer Durchführungsstandards** für die Anwendung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates im Hinblick*

auf **Standardformulare, Mustertexte und Verfahren** für die in einen Antrag auf Zulassung als **Anbieter von Krypto-Dienstleistungen** aufzunehmenden Angaben", [ABI L 2025/306](#); veröffentlicht worden. Die vier DelegiertenVOs ergänzen die KryptowerteVO [VO \(EU\) 2023/1114](#) (**MiCAR**) durch technische Regulierungsstandards zur Übermittlung bestimmter Informationen. Die DurchführungsVO enthält Standardformulare, Mustertexte und Verfahren zur MiCAR.



to the point

# Datenschutzmonitor. 15/2025 vom 16.04.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 08.04.2025, 22077/19, *Green/UK* (Datenoffenlegung, parlamentarische Immunität)

- **Rechtsprechung des EuGH**

EuGH 08.04.2025, C-292/23, *EUSTa* (Europäische Staatsanwaltschaft, Rechtsschutz, Zuständigkeit)

- **Rechtsprechung der Justiz**

OLG Linz 09.01.2025, 6R171/24w (Auskunft, Prozessposition, Rechtsmissbrauch)

OLG Innsbruck 29.01.2024, 10R87/24f (Auskunft, Vollmacht, Rechtsanwalt, Kostenersatz)

- **Rechtsprechung des BVwG**

BVwG 27.02.2025, W258 2230578-1 (Bürgerjournalismus, Medienfreiheit, Meinungsfreiheit)

BVwG 21.02.2025, W211 2288083-1 (Auskunft, konkrete Empfänger, zukünftige Empfänger, Erhebungspflicht)

BVwG 28.01.2025, W254 2284412-1 (Massenverfahren, Aussetzung)

- **Nationale Rechtsalte**

Verordnung über den "Elektronischen Rechtsverkehr im Bereich der Strafrechtspflege"



## To the Point:

### Rechtsprechung des EGMR

EGMR 08.04.2025, 22077/19, *Green/UK*

#### **Datenoffenlegung, parlamentarische Immunität**

- In einem bereits abgeschlossenen Zivilverfahren wurden gegen einen bekannten Geschäftsmann schwerwiegende Vorwürfe erhoben (ua rassistische Beleidigungen, sexuelle Belästigung). Um die Veröffentlichung der Vorwürfe zu verhindern, wurden in den Prozessen **Vertraulichkeitsvereinbarungen** geschlossen, weil sich die Offenlegung aus den Verfahren negativ auf den Ruf des Geschäftsmannes auswirken könnte. Über die Vorfälle wollte eine Zeitung berichten, gegen die der Geschäftsmann gerichtlich vorging und eine einstweilige Verfügung zur Verhinderung der Veröffentlichung seines Namens erwirkte. Die Zeitung veröffentlichte anschließend einen Artikel, der zwar auf die Hintergründe und Vorwürfe einging, jedoch den Namen des Geschäftsmannes nicht veröffentlichte.

In einer **parlamentarischen Debatte** veröffentlichte ein **Mitglied des House of Lords** unter Bezugnahme auf den Artikel den Namen des Geschäftsmannes. Der Geschäftsmann reichte eine Beschwerde gegen das Vereinigte Königreich wegen der Veröffentlichung seiner Identität beim EGMR ein, insb auch deshalb, weil die Offenlegung seiner Daten Verschwiegenheitsbemühungen gegen die Zeitung zunichtemachte. Der Geschäftsmann sah in der Vorgehensweise sein Recht auf Achtung seines Privatlebens gemäß Art 8 EMRK und sein Recht auf ein faires Verfahren gemäß Art 6 EMRK verletzt. Darüber hinaus sah er sein Recht auf wirksame Beschwerde gemäß Art 13 EMRK verletzt, weil gegen den Abgeordneten rechtlich nicht vorgegangen werden kann. Der EGMR stellte **keine Verletzung** von Art 8 EMRK fest und wies die Beschwerde hinsichtlich Art 6 und Art 13 EMRK zurück.

Der EGMR hat erwogen: Die **Offenlegung** der Daten einer Person, gegen die **schwerwiegende Vorwürfe** erhoben werden, ist eine **ernsthafte** Beeinträchtigung des **Rufs** und kann zu einer Verletzung des Rechts auf Achtung des Privatlebens gemäß Art 8 EMRK führen.

Die **parlamentarische Immunität** und die **Redefreiheit** sind **zentral** für die Rolle des Parlaments. Grundsätzlich wiegen das Recht auf **Privatsphäre** und das Recht auf Freiheit der **Meinungsäußerung gleich schwer**, im **parlamentarischen** Kontext wiegt das Recht auf freie **Meinungsäußerung** jedoch **schwerer**. Mitglieder des Parlaments müssen in der Lage sein, zu sprechen und zu kritisieren, **ohne** Angst vor Strafe zu haben. Die **parlamentarische Immunität**

**schützt** ua die **freie Rede** im Parlament und dient der Trennung der Legislative von der Judikative ("Gewaltenteilung"). Bei der Regulierung der **Redefreiheit** im parlamentarischen Kontext haben Mitgliedstaaten einen weiten **Ermessensspielraum**, wie und ob *ex-ante* und *ex-post* Kontrollen eingeführt werden. Die zusätzliche Einrichtung von Kontrollen, welche die Offenlegung von Informationen verhindern sollen, war nicht geboten.

Das Recht auf parlamentarische Immunität verstößt nicht gegen das Recht auf ein faires Verfahren. Ein Staat **muss keine** besonderen Maßnahmen zum Rechtsschutz implementieren, um die Offenlegung von Informationen zu verhindern. Dies auch dann nicht, wenn diese Informationen durch die einstweilige Verfügung eines Gerichts geschützt sind. Diese **Einschränkung** des gerichtlichen Rechtsschutzes ist **verhältnismäßig**, weil dadurch die **Redefreiheit** im Parlament und die **Gewaltenteilung geschützt werden**.

Eine eigene Beschwerdemöglichkeit bzw ein Rechtsbehelf ist gegen die **Offenlegungen im Parlament** nicht erforderlich.

### Rechtsprechung des EuGH

Aus der Rechtsprechung des EuGH:

- Mit der [VO \(EU\) 2017/1939](#) wurde die **Europäische Staatsanwaltschaft** errichtet ("**EUSTa**"). Die Zuständigkeit zur Überprüfung der Handlungen der EUSTa ist zwischen den nationalen Gerichten und den Unionsgerichten aufgeteilt. Die Zuständigkeit zur Überprüfung der Entscheidungen der EUSTa, die die **Rechte auf Datenschutz** der Betroffenen berühren, fällt in die **Zuständigkeit der Unionsgerichte** ([EuGH 08.04.2025, C-292/23, EUSTa](#)).

### Rechtsprechung der Justiz

OLG Linz 09.01.2025, 6R171/24w

#### **Auskunft, Prozessposition, Rechtsmissbrauch**

- Eine Spielerin war Kundin eines **Online-Glücksspielunternehmens**, welches über eine maltesische Glücksspiellizenz, nicht aber über eine Konzession nach dem österreichisches Glücksspielgesetz (GSpG) verfügt. Das Glücksspielunternehmen bietet ihre Website auf deutscher Sprache an und die Website ist in Österreich abrufbar. Die Spielerin stellte ein schriftliches Auskunftsersuchen an das Glücksspielunternehmen und verlangte eine Kopie ihrer Daten. Nachdem das Glücksspielunternehmen die Auskunft verweigerte, erhob die Spielerin eine Klage beim LG Steyr. Gegen das dem Klagebegehren stattgebende Urteil des Erstgerichts legte das Glücksspielunternehmen eine

(erfolglose) Berufung beim OLG Linz ein. Das Glücksspielunternehmen argumentierte, das Auskunftersuchen sei rechtsmissbräuchlich, weil die Spielerin damit bloß ein Beweismittel für einen Zivilprozess gegen das Unternehmen erlangen wolle.

Das OLG Linz hat erwogen: Das **Recht auf Auskunft** steht unter **keinen Voraussetzungen** und muss nicht mit einem **Rechtsschutzinteresse** begründet werden. Eine Auskunftspflicht besteht auch dann, wenn das Auskunftersuchen keinem der in **ErwGr 63 DSGVO** genannte Zwecke (Überprüfung der Rechtmäßigkeit, Bewusstsein der Verarbeitung) dient. Die Auskunftserteilung kann nicht bloß deshalb abgelehnt werden, weil damit primär die **Beweismittelbeschaffung** beabsichtigt wird. Ein Auskunftersuchen ist auch nicht offenkundig unbegründet oder rechtsmissbräuchlich, wenn damit **datenschutzfremde Ziele** verfolgt werden.

**Rechtsmissbrauch** liegt nur vor, wenn **zwischen den verfolgten eigenen Interessen** und den beeinträchtigten Interessen des anderen ein **krasses Missverhältnis** besteht. Die Geltendmachung von **erlittenen Spielverlusten** durch einen Kläger ist weder ein **unlauteres Verhalten** noch tritt das Auskunftsrecht hinter ein allenfalls berechtigtes Interesse des Beklagten. Es muss der **Schädigungszweck** bzw das **unlautere Motiv** der Rechtsausübung im Vordergrund stehen.

Die Geltendmachung von **erlittenen Spielverlusten** durch die Spielerin ist weder ein unlauteres Verhalten noch tritt das Auskunftsrecht hinter ein allenfalls berechtigtes Interesse des Glücksspielunternehmens. Auch lässt sich kein Schädigungszweck erkennen. Das Einklagen von einem allfälligen Saldo ist ein legitimes Interesse der Spielerin.

Ein **berechtigtes Geheimhaltungsinteresse** gemäß § 4 Abs 6 DSGVO iVm Art 15 Abs 4 DSGVO aufgrund der durch die Informationsherausgabe drohenden Schwächung ihrer **Prozessposition** (gemeint in einem zukünftigen Leistungsverfahren wegen Glücksspielverlusten) kommt dem Glücksspielunternehmen nicht zu. Denn die Spielerin ersucht nur um die Herausgabe von Daten aus gemeinsamen Geschäftsbeziehungen, sodass **kein Geheimnis** des Glücksspielunternehmens gegenüber der Klägerin besteht.

#### Aus der weiteren Rechtsprechung der Justiz:

- Mit der bloßen Berufung eines **Rechtsanwalts** auf die ihm erteilte **Vollmacht** gemäß § 8 Abs 1 RAO kann die Bevollmächtigung nur beim Einschreiten vor einer **Behörde** oder vor einem **Gericht** nachgewiesen werden. Stellt ein Dritter für einen Betroffenen

ein Auskunftersuchen an einen **Verantwortlichen des privaten Bereichs**, ist dem Auskunftersuchen eine **schriftliche Vollmacht** beizulegen. Fehlt die Vollmacht, hat der Verantwortliche keine Grundlage, um von einer Bevollmächtigung auszugehen und darf die **Auskunft verweigern**. Bringt der Betroffene anschließend Klage ein und erteilt der Verantwortliche daraufhin die Auskunft, hat der Verantwortliche **keinen Grund zur Klagsführung** gegeben. Der Betroffene trägt – als Kläger – gemäß **§ 45 ZPO** die Kosten des Verfahrens und hat dem Verantwortlichen Kostenersatz zu leisten ([OLG Innsbruck 29.01.2024, 10R87/24f](#)).

#### Rechtsprechung des BVwG

BVwG 27.02.2025, W258 2230578-1

#### **Bürgerjournalismus, Medienfreiheit, Meinungsfreiheit**

- Im Jahr 2018 dokumentierte ein **Tierschutzaktivist** zwei Jagdveranstaltungen in der Steiermark mittels Foto- und Videoaufnahmen. Ziel war es, die Öffentlichkeit über **Treibjagden** iZm Tierschutz zu informieren. Der Aktivist veröffentlichte die Aufnahmen auf sozialen Medien und stellte sie großen Medienhäusern zur Verfügung. Dabei wurde auch ein Jäger aufgenommen, der als Obmann eines Jagdvereins in der Jägerschaft bekannt war. Eine ausdrückliche Information des Jägers über die Datenverarbeitung unterblieb. Der Jäger erhob daraufhin Datenschutzbeschwerde bei der DSB. Er sah seine Rechte auf Geheimhaltung, Information und Auskunft verletzt.

Die DSB wies die Datenschutzbeschwerde hinsichtlich der behaupteten Verletzung des Rechts auf Geheimhaltung und Information ab, gab jedoch dem Auskunftersuchen statt. Sie stellte fest, dass sich der Tierschutzaktivist nicht auf das **Medienprivileg des § 9 Abs 1 DSGVO** berufen könne, seine Tätigkeit allerdings als **"Bürgerjournalismus"** zu qualifizieren sei. Bei einer Interessenabwägung des Grundrechts auf **freie Meinungsäußerung** des Tierschutzaktivisten und des Grundrechts auf Geheimhaltung des Jägers überwiege die Meinungsäußerungsfreiheit. Beide Verfahrensparteien erhoben eine Bescheidbeschwerde an das BVwG. Das BVwG gab der Bescheidbeschwerde des Jägers hinsichtlich des Rechts auf Information statt. Die Bescheidbeschwerde des Aktivisten wurde abgewiesen.

Das BVwG hat erwogen: Der österreichische Gesetzgeber hat die **Öffnungsklausel des Art 85 DSGVO** ursprünglich durch **§ 9 Abs 1 DSGVO idF BGBl I 2018/24 ("aF") umgesetzt**. Der Tierschutzaktivist versuchte durch seine Handlungen einen **Beitrag zur öffentlichen Debatte** rund um die Jagd iZm Tierschutz zu leisten. Durch die Auswahl geeigneter Aufnahmen und ihrer

textlichen Ergänzung ist ein **Mindestmaß an journalistischer Bearbeitung** gegeben.

Laut dem EuGH liegt eine **journalistische Tätigkeit** vor, wenn die Tätigkeit ua den Zweck hat, Informationen in der Öffentlichkeit zu verbreiten. Der Tierschutzaktivist war daher bei der Erstellung und Speicherung der Aufnahmen journalistisch tätig. Die Bestimmung des § 9 Abs 1 DSGVO aF war jedoch auf einen bestimmten Personenkreis beschränkt (zB Medieninhaber und Medienunternehmen), die den "Bürgerjournalismus" nicht umfasste.

Aufgrund der fehlenden Berücksichtigung des Bürgerjournalismus war die **Umsetzung** des Art 85 durch § 9 DSGVO aF **unvollständig**. Die **unmittelbare Anwendung** des Art 85 Abs 2 DSGVO scheidet jedoch aus, weil diese Bestimmung keine inhaltlichen Regelungen, sondern nur einen Auftrag an die Mitgliedstaaten enthält. Eine **analoge Anwendung** des § 9 DSGVO scheidet daran, dass keine planwidrige Lücke vorliegt. Der **Tierschutzaktivist** kann sich somit **nicht auf das Medienprivileg** des § 9 Abs 1 DSGVO aF berufen.

Der Aktivist darf sich hingegen auf die **Meinungsäußerungsfreiheit** nach Art 11 Abs 1 GRK berufen. Das Erfassen des Jägers erweist sich vor dem Hintergrund des Verarbeitungszwecks als unvermeidbar, wodurch der Grundsatz der **Datenminimierung** gewahrt bleibt (Art 5 Abs 1 lit c DSGVO). Auf den Aufnahmen und Videos ist der Jäger **unkennlich** gemacht worden, weshalb mangels personenbezogener Daten eine Verletzung seines **Rechts auf Geheimhaltung ausscheidet**. Trotz nicht störungsfreien Verhaltens **überwiegt das Interesse** des Tierschutzaktivisten an der **Dokumentation**, weil die Berichterstattung für die Diskussion über Tierschutz relevant ist und der Eingriff nur in die Sozialsphäre des Jägers erfolgte.

Das Medienprivileg ist in der Zwischenzeit novelliert worden. Hinsichtlich des **Medienprivilegs des § 9 Abs 1a S 5 DSGVO** in der neuen Fassung darf der Verantwortliche ua Auskunft über personenbezogene Daten, die zu journalistischen Zwecken verarbeitet werden und **noch nicht veröffentlicht wurden, verweigern**. Der Tierschutzaktivist hat jedoch die von ihm erfassten Daten bereits teilweise auf seiner "**Facebook Seite**" **veröffentlicht**. Er hätte dem Jäger daher bestimmte Informationen zu erteilen gehabt.

BVwG 21.02.2025, W211 2288083-1

### **Auskunft, konkrete Empfänger, zukünftige Empfänger, Erhebungspflicht**

- Ein Betroffener stellte im Jahr 2019 ein Auskunftersuchen an ein Unternehmen, das über eine Online-Applikation Webdienste zur kostenpflichtigen Abfrage öffentlich

zugänglicher Registerdaten betreibt. Das Unternehmen erteilte eine erste Auskunft. Der Betroffene erhob Datenschutzbeschwerde bei der DSB, weil die Auskunft seiner Ansicht nach unvollständig war. Die DSB setzte das Verfahren betreffend Art 15 Abs 1 lit c DSGVO aus, um eine Entscheidung des EuGH in der Rs [C-154/21, Österreichische Post](#), abzuwarten. Nach dem Urteil des EuGH ergänzte das Unternehmen im Jahr 2023 die Auskunft über die **konkreten Empfänger**. Gleichzeitig teilte es mit, dass seit dem Jahr 2022 keine Protokolle über Zugriffe mehr vorhanden seien, weil diese bereits gelöscht wurden. Die DSB **stellte** das Verfahren in der Folge mit Zustimmung des Betroffenen formlos **ein**.

Im selben Jahr erhob der Betroffene eine weitere Datenschutzbeschwerde. Er brachte vor, das Unternehmen habe während des vorhergehenden Verfahrens Daten zu Empfängern aus dem Jahr 2022 gelöscht, um der **Auskunftspflicht** aus dem ursprünglichen Auskunftersuchen von 2019 **zu entgehen**. Die DSB wies die Datenschutzbeschwerde ab. Sie stellte fest, dass die Auskunftspflicht nach Art 15 DSGVO nur Daten umfasst, die zum Zeitpunkt des Auskunftersuchens tatsächlich verarbeitet wurden. Daraufhin erhob der Betroffene (erfolglos) Beschwerde an das BVwG.

Das BVwG hat erwogen: Durch ein Auskunftersuchen wird eine **inhaltliche Auskunftspflicht** nur hinsichtlich solcher Daten ausgelöst, die vom Verantwortlichen **aktuell verarbeitet** werden. Löscht ein Verantwortlicher willkürlich die Daten nach Eingang eines Auskunftersuchens vor dessen Erledigung, so handelt er rechtswidrig. Der Umfang der Auskunftserteilung wird daher durch den **Zeitpunkt des Einlangens des Auskunftersuchens** bestimmt.

Nur konkrete **Empfänger iSd Art 15 Abs 1 lit c DSGVO** sind zu beauskunften, denen zum Zeitpunkt des Einlangens eines Auskunftersuchens bereits personenbezogene Daten übermittelt wurden. Eine Auskunftspflicht besteht zudem gegenüber jenen Empfängern, an die eine solche **Übermittlung in geplanter und vorhersehbarer Weise künftig erfolgt**.

Die Rechte der Betroffenen auf Information und Auskunft nach der DSGVO beziehen sich auf einen Zeitpunkt, der um bis zu drei Monate – die maximale Frist zur Beantwortung eines Auskunftersuchens – oder um die tatsächliche Bearbeitungsdauer in die Zukunft verschoben werden kann. Dies gilt jedoch nur für künftige Übermittlungen, die bereits laufend stattfinden, insofern Status quo sind, und deren **Eintreten sicher** ist.

Die Bestimmung des Art 15 Abs 1 lit c DSGVO verpflichtet nicht zur Auskunft über zukünftige Verarbeitungen, die während eines anhängigen Verfahrens zur

Auskunftserteilung erfolgen. Es gibt auch keine nachträgliche **Erhebungspflicht**. Das Unternehmen hat vor dem Jahr 2022 keine **Zuordnung von Empfängern** gespeichert, weshalb eine derartige Auskunft für den zeitgegenständlichen Zeitraum gar nicht möglich war.

Aus der weiteren Rechtsprechung des BVwG:

- Sind vor dem BVwG eine **erhebliche Anzahl** von Verfahren anhängig, in welchen dieselbe(n) Rechtsfrage(n) zu beantworten sind, die über eine Revision auch beim VwGH anhängen, kann das BVwG diese **Verfahren** mit Beschluss **aussetzen** ([BVwG 28.01.2025, W254 2284412-1](#)).

### **Nationale-Rechtsakte**

- Am **08.04.2025** wurde die Verordnung des Bundesministers für Inneres über den elektronischen Rechtsverkehr im Bereich der Strafrechtspflege ("**Elektronischer Rechtsverkehr im Bereich der Strafrechtspflege**"), [BGBl II 2025/63](#), kundgemacht. Die Verordnung enthält Regelungen zum elektronischen Rechtsverkehr mit Gerichten, Staatsanwaltschaften und Vollzugsbehörden.

to the point

# Datenschutzmonitor. 16/2025 vom 24.04.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des VwGH**

VwGH 29.01.2025, Ra 2023/04/0002 (Rechtsmissbrauch, Exzess, Auskunft)

VwGH 29.01.2025, Ra 2022/04/0049 (Rechtsmissbrauch, offenkundige Unbegründetheit, Berichtigung)

VwGH 29.01.2025, Ro 2023/04/0018;  
Ro 2022/04/0016; Ro 2022/04/0022  
Ra 2020/04/0084 (Rechtsmissbrauch, Exzess)

VwGH 20.03.2025, Ro 2022/01/0010 (Passgesetz, personenbezogene Daten)

- **Rechtsprechung der Justiz**

OLG Linz 02.04.2025, 4R29/25z (Auskunft, Identitätsnachweis, Vollmacht)

- **Rechtsprechung des BVwG**

BVwG 14.03.2025, W252 2259204-3 (Wiederaufnahme)

- **Rechtsprechung der LVwG**

LVwG Steiermark 10.12.2024, LVwG 413.9-2959/2024 (Verwaltungsgericht, Beweisverfahren)

LVwG Kärnten 23.08.2022, KLVwG-1400/3/2022 (Smart Meter, IME-VO)

- **Rechtsprechung der DSB**

DSB 17.03.2025, 2025-0.192.907 (Parkraum, Videoüberwachung, Mitwirkung, Liquidation, Untersagung, aufschiebende Wirkung)

DSB 04.02.2025, 2025-0.021.375 (Pflegedienst, Videoüberwachung)

- **Leitlinien**

EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies<sup>1.1</sup> (2025) (Blockchain, Datenschutz)

## To the Point:

### Rechtsprechung des VwGH

VwGH 29.01.2025, Ra 2023/04/0002

#### **Rechtsmissbrauch, Exzess, Auskunft**

- Ein Betroffener erhob in weniger als zwei Jahren insgesamt 77 Datenschutzbeschwerden bei der DSB. Er machte in 46 Fällen das Recht auf Löschung und in 29 Fällen das Recht auf Auskunft geltend. Oftmals erhob der Betroffene seine Datenschutzbeschwerden wenige Tage nach Ablauf der "Ein-Monats-Frist", wenn er innerhalb eines Monats keine Antwort erhielt.

Die DSB **lehnte** die Behandlung einer auf das Recht auf Auskunft gerichteten Datenschutzbeschwerde des Betroffenen mit der Begründung **ab**, dass die 77 Datenschutzbeschwerden als exzessive Inanspruchnahme des Beschwerderechts nach Art 57 Abs 4 DSGVO anzusehen seien. Der Betroffene brachte Bescheidbeschwerde beim BVwG ein, dass den **Ablehnungsbescheid** der DSB als **Zurückweisungsbescheid** wertete und der Bescheidbeschwerde stattgab. Begründend führte das BVwG ua aus, dass "**Exzessivität**" iSd Art 57 Abs 4 DSGVO nur dann vorliege, wenn Datenschutzbeschwerden einen offensichtlich **schikanösen bzw rechtsmissbräuchlichen Charakter** haben. Weiters sei nach Art 57 Abs 4 DSGVO bei "exzessiven Anträgen" **vorrangig** eine **angemessene Gebühr** zu verlangen. Eine Ablehnung der Behandlung komme nur in Ausnahmefällen in Betracht.

Die DSB erhob Amtsrevision an den VwGH, der das Verfahren aussetzte und dem EuGH drei Fragen zu "exzessiven Anträgen" iSd Art 57 Abs 4 DSGVO vorlegte. Nachdem der EuGH diese Fragen mit Urteil vom [09.01.2025, C-416/23, Österreichische Datenschutzbehörde \(Exzessive Anfragen\)](#), beantwortete, setzte der VwGH das Verfahren fort und behob das Erkenntnis des BVwG.

Der VwGH hat erwogen: Die DSB ist nur berechtigt, die Behandlung einer Datenschutzbeschwerde abzulehnen, wenn sie das Vorliegen einer **Missbrauchsabsicht** des Beschwerdeführers **nachweist**. Allein die Zahl der eingebrachten Datenschutzbeschwerden durch eine Person reicht nicht als Nachweis. Die Häufung von Datenschutzbeschwerden kann jedoch ein **Indiz** für die Missbrauchsabsicht sein.

Eine Missbrauchsabsicht ist dann anzunehmen, wenn die entscheidenden Gründe des Beschwerdeführers für die Einbringung einer Vielzahl von Datenschutzbeschwerden nicht **in der Verfolgung der ihm aus der DSGVO zukommenden Rechte liegen** und der Beschwerdeführer ohne diese **sachfremden Gründe** die Vielzahl an Datenschutzbeschwerden nicht erhoben hätte.

Ein **Indiz** dafür, dass der Beschwerdeführer nicht oder nicht entscheidend den Schutz der ihm **aus der DSGVO zukommenden Rechte verfolgt**, ist etwa, wenn der Beschwerdeführer zu den Verantwortlichen, gegen die sich seine Datenschutzbeschwerden richten, keinen Bezug hat und keine Anhaltspunkte für die Verarbeitung personenbezogener Daten des Beschwerdeführers durch die Verantwortlichen bestehen.

**Veranlasst** ein Beschwerdeführer **nur deshalb** eine Verarbeitung seiner personenbezogenen Daten durch einen Verantwortlichen, um anschließend die ihm aus der DSGVO zukommenden Rechte, wie etwa das Auskunftsrecht, gegenüber dem Verantwortlichen geltend machen zu können, und besteht nur deswegen eine Beziehung zwischen dem Beschwerdeführer und dem Verantwortlichen, ist in Bezug auf eine spätere Datenschutzbeschwerde ebenso **Missbrauchsabsicht** des Beschwerdeführers anzunehmen.

Die DSB hat die **Wahl** zwischen der Einhebung einer **angemessenen Gebühr** für die Bearbeitung einer exzessiven Datenschutzbeschwerde und der **Weigerung**, aufgrund einer solchen Datenschutzbeschwerde **tätig zu werden**. Sie hat jedoch unter Berücksichtigung aller relevanten Umstände auf die Eignung, Erforderlichkeit und Verhältnismäßigkeit beider Handlungsoptionen Bedacht zu nehmen.

Das Verfahren über Bescheidbeschwerden gegen Entscheidungen der nationalen Aufsichtsbehörden richtet sich nach dem jeweiligen **mitgliedstaatlichen Verfahrensrecht**.

Lehnt die DSB die Behandlung einer Datenschutzbeschwerde ab, trifft sie keine inhaltliche Entscheidung. Die "Sache" des Beschwerdeverfahrens vor dem BVwG ist daher – wie bei der Zurückweisung – nur die Frage der **Rechtmäßigkeit der Ablehnung**. Das BVwG hat jedoch den von der DSB herangezogenen Ablehnungsgrund umfassend und abschließend zu beurteilen und dafür den maßgeblichen Sachverhalt amtswegig selbst zu erheben. **Anm: Dieses Erkenntnis des VwGH könnte große praktische Auswirkungen entfalten. Insb das Geschäftsmodell, Websites nur deshalb aufzurufen, um den Verantwortlichen anschließend abzumahnen, gegen ihn Datenschutzbeschwerde einzubringen oder ihn auf Unterlassung- und/oder auf Schadenersatz zu klagen, könnte unter Druck geraten.**

**Ob der Betroffene tatsächlich 77 Datenschutzbeschwerden eingebracht hat, ist unklar. Denn die DSB zählt die von ihr vergebenen Aktenzahlen und nicht die tatsächliche Anzahl der Datenschutzbeschwerden.**

### Rechtsmissbrauch, offenkundige Unbegründetheit, Berichtigung

- Ein Betroffener brachte insg 29 Datenschutzbeschwerden bei der DSB ein, mit welchen er die Berichtigung iSd Art 16 DSGVO bzw die "Richtigstellung" eines Sachverständigengutachtens über seinen Gesundheitszustand verlangte. Die DSB lehnte die Behandlung der verfahrensgegenständlichen Datenschutzbeschwerden wegen "offenkundiger Unbegründetheit" und "Exzessivität" ab. Das BVwG behob den Ablehnungsbescheid der DSB, wogegen sich die (erfolgreiche) Amtsrevision der DSB richtete.

Der VwGH hat erwogen: Über die Weigerung der Behandlung einer Datenschutzbeschwerde hat die DSB in **Bescheidform** abzusprechen.

Das Vorliegen einer **offenkundigen Unbegründetheit** ist aus objektiver Sicht zu beurteilen. Eine Datenschutzbeschwerde ist dann offenkundig unbegründet, wenn sie ohne nähere Prüfung der Angriffs- oder Verteidigungsmittel als erfolglos erkannt werden kann. Eine offenkundige Unbegründetheit kann somit angenommen werden, wenn eine Datenschutzbeschwerde keinen Bezug zu datenschutzrechtlichen Fragestellungen aufweist. Das Berichtigungsrecht ist nur bei Tatsachenangaben anwendbar, nicht aber bei Werturteilen. Die auf Tatsachenangaben beruhenden Schlussfolgerungen eines Sachverständigen in einem Gutachten sind subjektiver Natur. Sie sind die Meinung eines Gutachters und sind dem Berichtigungsrecht nicht zugänglich. Die "Richtigstellung" einer gutachterlichen Meinung kann daher keinen Gegenstand einer auf **Berichtigung** gerichteten Datenschutzbeschwerde bilden. Einer solchen Datenschutzbeschwerde kommt **ohne nähere Prüfung keine Erfolgchance** zu, weshalb eine offenkundige Unbegründetheit vorliegen kann.

Die Behandlung einer Datenschutzbeschwerde darf nur dann als **exzessiv** abgelehnt werden, wenn eine **nachgewiesene Missbrauchsabsicht** vorliegt. Das Einbringen einer Datenschutzbeschwerde ist ua dann missbräuchlich, wenn (i) der Beschwerdeführer die Datenschutzbeschwerde zur Erzielung eines durch die datenschutzrechtlichen Bestimmungen nicht geschützten Zwecks erhebt (zB Publicity, Feindseligkeit, Sensationslust), (ii) der Beschwerdeführer sich der Unrichtigkeit seines Rechtsstandpunkts bewusst sein muss, etwa weil er dieselbe – oder ähnliche – Datenschutzbeschwerden bereits erfolglos erhoben hat, (iii) eine Person die Ressourcen der DSB in Anspruch nimmt, obwohl sich bereits aus dem Beschwerdevorbringen ergibt, dass mit der betreffenden Datenschutzbeschwerde

offenkundig andere Ziele als die Durchsetzung des Datenschutzrechts verfolgt werden.

Aus der weiteren Rechtsprechung des VwGH:

- Die DSB ist nur berechtigt, die Behandlung einer Datenschutzbeschwerde als **exzessiv** abzulehnen, wenn sie das Vorliegen einer **Missbrauchsabsicht** des Beschwerdeführers nachweist. Eine Missbrauchsabsicht ist dann anzunehmen, wenn die entscheidenden Gründe des Beschwerdeführers für die Einbringung einer Vielzahl von Datenschutzbeschwerden nicht **in der Verfolgung der ihm aus der DSGVO zukommenden Rechte liegen** und der Beschwerdeführer ohne diese **sachfremden Gründe** die Vielzahl an Datenschutzbeschwerden nicht erhoben hätte. Das Einbringen einer Datenschutzbeschwerde ist ua dann missbräuchlich, wenn der Beschwerdeführer die Datenschutzbeschwerde zur Erzielung eines durch die datenschutzrechtlichen Bestimmungen nicht geschützten Zwecks erhebt (zB Publicity, Feindseligkeit, Sensationslust) ([VwGH 29.01.2025, Ro 2023/04/0018](#); [Ro 2022/04/0016](#); [Ro 2022/04/0022](#); [Ra 2020/04/0084](#)).
- Die Passversagung kann nicht auf § 22a Passgesetz gestützt werden, weil diese Bestimmung nur die **Verarbeitung personenbezogener Daten** anlässlich der Antragstellung und in lokalen Anwendungen regelt ([VwGH 20.03.2025, Ro 2022/01/0010](#)).

### Rechtsprechung der Justiz

Aus der Rechtsprechung der Justiz:

- Beauftragt eine Betroffene einen Rechtsanwalt mit der Durchsetzung ihres Betroffenenrechts auf Auskunft, muss der Verantwortliche die **Vollmacht** und Identität der betroffenen Person prüfen. Weitere Informationen zur Bestätigung der Identität dürfen nur bei begründeten Zweifeln an der Identität verlangt werden. Eine **Ausweiskopie** ist ein **geeigneter Identitätsnachweis**. Für den Bevollmächtigungsvertrag gibt es keine besonderen Formvorschriften, auch Art 12 Abs 6 DSGVO enthält keine speziellen Formfordernisse. Wenn der Verantwortliche lediglich mitteilt, keine elektronischen Vollmachten zu akzeptieren, ohne Zweifel an der Echtheit der Unterschrift zu äußern, ist für den Betroffenen nicht ersichtlich, ob berechtigterweise weitere Nachweise zur Erfüllung des Auskunftersuchens erforderlich sind. Da der Verantwortliche die allenfalls bestehenden Zweifel iSd Art 12 Abs 6 DSGVO nicht einzelfallbezogen dargelegt hat, wurde die **Klageerhebung** durch den Verantwortlichen **veranlasst**. Die Bestimmung des § 45 ZPO findet keine Anwendung ([OLG Linz 02.04.2025, 4R29/25z](#)).

## Rechtsprechung des BVwG

Aus der Rechtsprechung des BVwG:

- Aufgrund einer späteren Entscheidung des EuGH entsteht **keine Berechtigung zur Wiederaufnahme von rechtskräftig abgeschlossenen Verfahren** (BVwG [14.03.2025, W252 2259204-3](#)).

## Rechtsprechung der LVwG

LVwG Steiermark 10.12.2024, LVwG 413.9-2959/2024

### **Verwaltungsgericht, Beweisverfahren**

- Beim LVwG Steiermark war ein Verfahren anhängig, bei welchem der Bruder des Betroffenen einen Bescheid nach der Bundesabgabenordnung (**BAO**) bekämpfte. Nach einer erfolglosen Berufung an den Gemeinderat erhob der Bruder eine Bescheidbeschwerde an das LVwG Steiermark, wo eine **öffentliche, mündliche Verhandlung** durchgeführt wurde. Der Betroffene wurde zu dieser Verhandlung als Zeuge geladen. Weiters wurden in der mündlichen Verhandlung Beweismittel vorgelegt, die sich neben dem Bruder auch auf den Betroffenen bezogen. Diese Beweismittel wurden zuvor vom Rechtsanwalt des Bruders an das Gericht übermittelt. Der Betroffene brachte eine Datenschutzbeschwerde beim LVwG Steiermark ein und behauptete, durch die Offenlegung dieser Beweismittel in seinem Recht auf Datenschutz verletzt worden zu sein.

Das LVwG Steiermark hat erwogen: Gemäß Art 130 Abs 2a B-VG sind natürlichen Personen berechtigt, sich über die Handhabung der DSGVO durch die Verwaltungsgerichte zu beschweren. Das LVwG Steiermark ist gemäß Art 130 Abs 2a B-VG iVm § 29a Abs 3 StLVwGG für Beschwerden von Personen zuständig, die durch das LVwG Steiermark in Ausübung seiner gerichtlichen Zuständigkeiten in ihren Rechten gemäß der DSGVO verletzt zu sein behaupten.

Das LVwG Steiermark ist Verantwortlicher für die Verarbeitung von personenbezogenen Daten, unabhängig davon, ob es im Rahmen der justiziellen Tätigkeit oder der Justizverwaltung agiert. Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn sie auf einen Erlaubnistatbestand des Art 6 DSGVO gestützt werden kann. Gemäß Art 6 Abs 1 lit e DSGVO ist die Verarbeitung rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in **Ausübung öffentlicher Gewalt** erfolgt. Die **Staatsfunktion Gerichtsbarkeit** erfolgt in **Ausübung öffentlicher Gewalt**. Rechtsgrundlage für die Verarbeitung iSd Art 6 Abs 3 DSGVO durch das LVwG Steiermark ist Art 129 B-VG iVm § 1 StLVwGG sowie Art 130 B-VG. Die Verarbeitung der personenbezogenen Daten des Betroffenen erfolgte während einer

öffentlichen **mündlichen Verhandlung**, die ein zentraler **Pfeiler der Verwaltungsgerichtsbarkeit** ist.

Die **Entgegennahme und Würdigung von Beweismitteln** ist eine zentrale und grundlegende Aufgabe eines Gerichts und steht in direktem Zusammenhang mit der Gerichtsbarkeit. Gemäß § 166 BAO ist im Abgabungsverfahren alles als Beweismittel geeignet, was zur Feststellung des maßgebenden Sachverhalts geeignet und zweckdienlich ist.

Die Vorlage der Beweismittel erfolgte durch eine Partei des Verfahrens. Das LVwG muss vorgelegte Beweismittel, sofern sie nicht zurückgewiesen werden, zum Akt nehmen und in Folge würdigen, um den Sachverhalt festzustellen. Die Entgegennahme und Würdigung eines Beweismittels kann zwar eine Verarbeitung personenbezogener Daten sein, jedoch entspricht dies dem Zweck des **Beweisverfahrens** und ist dazu geeignet, festzustellen, ob das Beweismittel zur Klärung des Sachverhalts verwertbar sein kann.

Die Verarbeitung der personenbezogenen Daten des Betroffenen ohne dessen Einwilligung war **erforderlich** und **verhältnismäßig**. Die Verarbeitung ist somit vom Rechtmäßigkeitsgrund nach Art 6 Abs 1 lit e DSGVO gedeckt.

Aus der weiteren Rechtsprechung der LVwG:

- Gemäß § 2 Abs 1 der Intelligente Messgeräte-Einführungsverordnung (**IME-VO**) haben **Netzbetreiber** der **E-Control** die aktuellen Projektpläne über die Einführung von intelligenten Messgeräten sowie jeweils zum 31.03. eines Kalenderjahres einen Bericht insb über den Fortschritt der Installationen von intelligenten Messgeräten, zu den angefallenen Kosten, zu den bei der Installation gemachten Erfahrungen, zum **Datenschutz**, zur **Verbrauchsentwicklung** bei den Endverbrauchern und zur Netzsituation in einer von der E-Control vorzugebenden Form zu übermitteln. Der **Bundesministerin** für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie ist jederzeit Einsicht in die an die E-Control übermittelten Projektpläne zu gewähren und Auskunft über die Anzahl der bereits eingereichten Projektpläne zu erteilen ([LVwG Kärnten 23.08.2022, KLVwG-1400/3/2022](#)).

## Rechtsprechung der DSB

DSB 17.03.2025, 2025-0.192.907

**Parkraum, Videoüberwachung, Mitwirkung, Liquidation, Untersagung, aufschiebende Wirkung**

- Eine **Parkraumbewirtschaftungsgesellschaft** verfügte über mehr als 350 Stell- und Garagenplätze in Europa, größtenteils in Wien. Diese Stellplätze wurden mit einer



unbekannten Anzahl von Videokameras überwacht. Die Parkraumbewirtschaftungsgesellschaft verschickte Abmahnschreiben einschließlich Bildaufnahmen an KFZ-Halter, denen **Besitzstörungen** vorgeworfen wurden.

Bei der DSB sind eine Vielzahl von Datenschutzbeschwerden bzw Anzeigen eingelangt. Das Verhalten der Parkraumgesellschaft ist auch medial bekannt. Die DSB leitete daher Verfahren gegen die Parkraumbewirtschaftungsgesellschaft ein. Die Gesellschaft reagierte nicht. Selbst nach Einleitung mehrerer Verwaltungsstrafverfahren wegen Verletzung der **Mitwirkungspflicht** (Art 31 DSGVO), in welchen auch Geldbußen verhängt wurden, erfolgte keine Reaktion. Der einzelvertretungsbefugte Geschäftsführer erschien trotz ordentlicher Ladung zu keiner mündlichen Verhandlung. Das Recht auf Akteneinsicht wurde jedoch ausgeübt.

Die DSB **untersagte** der Parkraumbewirtschaftungsgesellschaft jegliche Datenverarbeitung durch Videokameras auf Park- und Stellflächen im **gesamten Staatsgebiet** der Republik Österreich und schloss die **aufschiebende Wirkung** einer allfälligen Bescheidbeschwerde aus.

Die DSB hat erwogen: Die **nicht gehörige Mitwirkung** einer Partei im Beweisverfahren unterliegt der **freien Beweiswürdigung** gemäß § 45 Abs 2 und § 46 AVG. Der Behörde steht es frei, aus der mangelnden Mitwirkung einer Partei im Ermittlungsverfahren eventuell auch für die Partei **negative Schlüsse** zu ziehen.

Die **Liquidation** der Parkraumbewirtschaftungsgesellschaft ändert nichts an der Identität der Gesellschaft oder an ihrer **Rechtsfähigkeit**, denn sie erlischt erst mit ihrer (Voll-)Beendigung, nicht schon mit dem Eintritt der Liquidation. Parteifähige Kapitalgesellschaften verlieren ihre Parteifähigkeit erst mit ihrer **Vollbeendigung**. Selbst wenn man dies in Abrede stellen würde, kommt es bei der Verarbeitung personenbezogener Daten nicht darauf an, ob Verantwortliche iSd Art 4 Z 7 DSGVO eine **Rechtspersönlichkeit** und eine eigene Rechtsfähigkeit haben oder nicht.

Die Parkraumbewirtschaftungsgesellschaft konnte – mangels Mitwirkung – trotz der **Rechenschaftspflicht** und der deshalb sie treffenden **Beweislast** gemäß Art 5 Abs 2 DSGVO nicht darlegen, dass die Datenverarbeitung rechtmäßig erfolgt ist. Aufgrund der fehlenden Mitwirkung und der Vielzahl der von der Vorgehensweise der Gesellschaft betroffenen Personen war ein **sofortiges Verbot** der Datenverarbeitung auszusprechen.

Der Ausschluss der **aufschiebenden Wirkung** war auszusprechen, weil ohne Ausschluss dieser Wirkung erhebliche Nachteile für das öffentliche Wohl bzw für Dritte eintreten könnten, die schwerer wiegen als

mögliche Nachteile für die Parkraumbewirtschaftungsgesellschaft. Außerdem liegt **Gefahr in Verzug** vor, weil davon auszugehen ist, dass die Parkraumbewirtschaftungsgesellschaft weiterhin eine unrechtmäßige Videoüberwachung betreibt.

DSB 04.02.2025, 2025-0.021.375

### **Pflegedienst, Videoüberwachung**

- Ein **Erwachsenenvertreter** installierte in der **Wohnung** zum Schutz seines **Pflegebefohlenen**, der unter Angststörungen litt und zu Selbstgefährdung neigte, **zwei Kameras**. Diese erfassten das **Pflegepersonal** beim Betreten und Verlassen der Wohnung. Eine weitere Kamera installierte der Erwachsenenvertreter im Garten, wobei das Pflegepersonal vom Aufnahmebereich nicht erfasst wurde. Eine Einwilligung von Seiten des Pflegepersonals in die Videoaufzeichnung lag für keine Kamera vor. Eine der Pflegerinnen brachte eine auf Verletzung im Recht auf Geheimhaltung gestützte Datenschutzbeschwerde gegen den Erwachsenenvertreter bei der DSB ein.

Die DSB hat erwogen: Da der Aufnahmebereich jener Kamera, die **im Garten** des Pflegebefohlenen installiert wurde, so gewählt worden war, dass er das Pflegepersonal nicht erfasste, schied eine Verletzung im Recht auf Geheimhaltung *a priori* aus.

Die beiden im **Wohnzimmer** angebrachten **Kameras** sind anders zu beurteilen. Der mit der Installation der Videokameras intendierte Schutz des Pflegebefohlenen mag auf die Wahrnehmung eines berechtigten Interesses gestützt werden können. Die Videoüberwachung des Pflegebefohlenen entsprach jedoch nicht dem **Grundsatz der Datenminimierung**, weil sie auf Dauer angelegt war. Die Kameras filmten auch in jenen Zeiträumen, in denen das **Pflegepersonal** anwesend war.

Das **ununterbrochene Überwachen** der Wohnung war zur Zweckerreichung (dem Schutz des Pflegebefohlenen) **nicht erforderlich**, weil das Pflegepersonal vor Ort in der Lage war, auf etwaige Gesundheitsveränderungen des Pflegebefohlenen reagieren zu können. Die Videoüberwachung verletzte sohin die Pflegerin in ihrem Geheimhaltungsrecht. Die Aufnahmezeiten der installierten Kameras sind daher derart einzuschränken, dass sie während der Anwesenheit des **Pflegedienstes** außer Betrieb gesetzt sind.

## **Leitlinien**

EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies<sup>1.1</sup> (2025)

### **Blockchain, Datenschutz**

- Der europäische Datenschutzausschuss ("EDSA") hat einen Entwurf der Leitlinien zur Verarbeitung personenbezogener Daten durch Blockchain-Technologien zur öffentlichen Konsultation veröffentlicht. Bis 09.06.2025 können Kommentare, Anmerkungen und Vorschläge an den EDSA übermittelt werden.

Die vorgeschlagenen Leitlinien enthalten einen allgemeinen Rahmen für Fragen betreffend die Beachtung der DSGVO, wenn die Verarbeitung personenbezogener Daten ganz oder teilweise auf der sogenannten Blockchain-Technologie basiert. Der EDSA hält fest, dass manche grundlegende Merkmale von Blockchains nur schwer mit den Anforderungen der DSGVO in Einklang zu bringen sind, bemüht sich jedoch, geeignete Wege zur Einhaltung der Vorschriften vorzuschlagen. In einigen Fällen stellt er aber fest, dass der Einsatz dieser Technologie unter datenschutzrechtlichen Gesichtspunkten schlichtweg ausgeschlossen werden muss. Einige Elemente des Datenschutzes stehen der Blockchain-Technologie bereits konzeptionell konträr gegenüber. Das sind insb (i) der Grundsatz der Speicherbegrenzung und der Grundsatz der Datenminimierung, denn in einer Blockchain werden Daten sequenziell hinzugefügt und gespeicherte Daten können prinzipiell nicht mehr gelöscht werden, (ii) darauf basierend das Recht auf Löschung oder Berichtigung, (iii) die Zuordnung der Akteure, weil durch den dezentralisierten Ansatz bei der Blockchain die Identifizierung der datenschutzrechtlichen Rollenverteilungen wesentlich erschwert wird, und (iv) Fragen der internationalen Datenübermittlung.

Der EDSA empfiehlt eine Reihe von Maßnahmen, um dieses Spannungsverhältnis aufzulösen. Empfohlen wird zB die Prüfung der Erforderlichkeit, ob eine Blockchain wirklich zwingend eingesetzt werden muss. Beim Bejahen dieser Frage wird die Wahl eines möglichst datenschutzfreundlichen Modells empfohlen, das etwa (i) Lese- und Schreibrechte auf eine begrenzte Anzahl identifizierter Akteure beschränkt, (ii) die Verschlüsselung von Daten in der Blockchain vorsieht, (iii) die wirksame Ausübung der Betroffenenrechte sicherstellt und (iv) die Durchführung einer DSFA beinhaltet. Weiters empfiehlt der EDSA (v) die Schaffung eines robusten Governance-Systems, das klare technische, organisatorische und rechtliche Vorgaben macht, Verantwortliche und Auftragsverarbeiter klar benennt und Zugriffs-, Vorfalls- und Aktualisierungs-Überwachungen bietet.

to the point

# Datenschutzmonitor. 17/2025 vom 30.04.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des VwGH**

VwGH 20.03.2025, Ro 2023/04/0050 (Informationspflicht, Feststellungskompetenz)

- **Rechtsprechung der Justiz**

OGH 26.03.2025, 6Ob50/24g (eCommerce, Herkunftslandprinzip, DSA)

OLG Graz 14.03.2025, 5R28/25i (Auskunft, Vollmacht, Kostenersatz)

OLG Graz 13.03.2025, 2R32/25f (Auskunft, Identifizierung)

- **Rechtsprechung des BVwG**

BVwG 05.03.2025, W211 2291833-1 (Medienprivileg, Bürgerjournalismus)

BVwG 06.03.2025, W292 2289837-1 (Auskunft, Identifizierung, Zurückverweisung)

BVwG 11.03.2025, W211 2293097-1 (Hackerangriff, Benachrichtigung, Präklusion)

BVwG 10.03.2025, W287 2286005-1 (Geldbuße, Mitwirkungspflicht, Anweisung, Selbstbeziehung, Strafbemessung)

BVwG 10.02.2025, W176 2285593-1 (Auskunft, Vollmacht, Korrespondenz, Datenkopie, Löschung)

BVwG 11.03.2025, W137 2305838-1 (Exzess, Rechtsmissbrauch, unzumutbarer Aufwand)

BVwG 11.03.2025, W211 2288587-1 (Beweislast, Datenoffenlegung)

- **Rechtsprechung der LVwG**

LVwG NÖ 25.03.2025, LVwG-AV-1248/002-2024 (Amtsgeheimnis, Steuergeheimnis, Besitzstörung, Hundehaltung)

- **Beschlüsse der EK**

EK Pressemitteilung 23.04.2025, IP/25/1085 (Apple, Meta, Facebook Marketplace, "Consent or Pay")

- **Nationale Rechtsakte**

Einzelentgeltnachweisverordnung 2025

## To the Point:

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Betroffene haben ein **Recht auf Feststellung** einer Verletzung der **Informationspflicht** gemäß Art 14 DSGVO, auch wenn die Information bis zum Abschluss des Verfahrens vor der DSB vollständig erteilt wird. Da die Rechtsverletzung in der Unterlassung der antraglos zu erteilenden Information liegt, kann diese Verletzung – anders als beim auf Antrag zu erteilenden Auskunft – rückwirkend **nicht beseitigt** werden. Auch fehlt es nicht an der **Beschwer** zum Entscheidungszeitpunkt ([VwGH 20.03.2025, Ro 2023/04/0050](#)).

### Rechtsprechung der Justiz

[OGH 26.03.2025, 6Ob50/24g](#)

#### **eCommerce, Herkunftslandprinzip, DSA**

- Ein österreichischer Bauunternehmer, der auch Geschäftsführer einer GmbH war, hat ein in der Slowakei ansässiges Unternehmen mit Arbeiten beauftragt, aber aufgrund Differenzen über die Rechnungslegung die aushaftende Summe nicht beglichen. Ein slowakisches Inkassounternehmen hat ihn daraufhin auf ihrer Website unter der Überschrift "Betrüger" in eine "Schuldnerliste", die auch mehrere andere Personen enthielt, aufgenommen und ihm vorgeworfen, für sein Unternehmen Personal geleast und die Rechnung nicht bezahlt zu haben, wodurch er sich unberechtigt bereichert haben soll. Der OGH hat den Antrag zur Vorlage der Frage an den EuGH, ob diese Äußerungen ein Abgehen vom Herkunftslandprinzip ermöglichen, abgewiesen und die Sache zur Erhebung des anwendbaren slowakischen Rechts an das Erstgericht zurückverwiesen.

Der OGH hat erwogen: Eine den **Hostprovider** treffende Verpflichtung zur Unterlassung der Verbreitung von Persönlichkeitsrechte verletzenden Inhalten fällt in den **koordinierten Bereich** von Art 2 lit h sublit i **eCommerceRL 2000/31/EG** bzw § 3 Z 8 ECG (4 Ob 191/23a [ErwGr 3.1. und 3.3.]; 6 Ob 166/22p [ErwGr 2.2.]; 6 Ob 180/21w [ErwGr 2.1.2.]). Im koordinierten Bereich stellt Art 3 Abs 2 der eCommerceRL das **grundsätzliche Verbot** auf, dass der Anbieter eines Dienstes des elektronischen Geschäftsverkehrs strengerer Anforderungen unterliegt, als sie das im Sitzmitgliedstaat dieses Anbieters – hier die Slowakei – geltende Sachrecht vorsieht ("**Herkunftslandprinzip**"; EuGH 25. 10. 2011, verb Rs C-509/09 und C-161/10, eDate Advertising ua, Rz 63–68). Gerichte können im Einzelfall zum Schutz taxativ genannter Rechtsgüter – wie dem Schutz der Würde einzelner Menschen – und unter Wahrung des

Verhältnismäßigkeitsgrundsatzes abweichend vom Herkunftslandprinzip Maßnahmen treffen. Diese Bestimmung ist als Ausnahmeregelung aber grundsätzlich eng auszulegen.

Nicht jede **ehrenrührige** oder **kreditschädigende Äußerung** rechtfertigt bereits eine Abweichung vom Herkunftslandprinzip (vgl 6 Ob 221/23b [ErwGr 2.4.]). Ehrverletzungen, die den Kernbereich der Persönlichkeitsrechte betreffen (die Gesundheit, das Sexualleben und das Leben in und mit der Familie) sind regelmäßig als ausreichend schwerer Eingriff anzusehen (6 Ob 166/22p [ErwGr 2.5.2.]). Bei inhaltlicher Unrichtigkeit oder Fehlen eines ausreichenden diesbezüglichen wahren Tatsachenkerns sind die vorliegenden Äußerungen zwar als ehrenbeleidigend und/oder kreditschädigend iSd § 1330 ABGB anzusehen. Sie erreichen aber nicht einen Schweregrad, der ein Abgehen vom Herkunftslandprinzip zum Schutz der Menschenwürde des Klägers als verhältnismäßig erscheinen lässt.

Auf eine allfällige **Rechtsänderung** durch das während des Rechtsmittelverfahrens in Kraft getretene **Digital Services Act (DSA)** ist nicht näher einzugehen. Zwar ist eine Rechtsänderung bei einem in die Zukunft gerichteten Unterlassungstitel während des Rechtsmittelverfahrens beachtlich, weil die Berechtigung des angestrebten Gebots seinem Wesen nach ein in der Zukunft liegendes Verhalten erfassen soll. Mangels Feststellung des slowakischen Rechts fehlen aber noch Feststellungen zur Rechtswidrigkeit des Eingriffs ins Persönlichkeitsrecht.

#### Aus der weiteren Rechtsprechung der Justiz:

- Mit der **bloßen Berufung** eines Rechtsanwalts auf die ihm erteilte Vollmacht gemäß § 8 Abs 1 RAO kann die Bevollmächtigung nur beim Einschreiten vor einer Behörde oder vor einem Gericht nachgewiesen werden. Beauftragt eine Betroffene einen Rechtsanwalt mit der Durchsetzung ihres Betroffenenrechts auf Auskunft, muss der Verantwortliche die Vollmacht und Identität der Betroffenen prüfen. Eine **Vollmacht** bedarf einer Unterschrift oder einer qualifizierten elektronischen Signatur iSd § 4 Abs 1 S 1 Signatur- und Vertrauensdienstegesetzes. Fehlt eine entsprechende Unterschrift, hat der Verantwortliche keinerlei Grundlage dafür, von einer Bevollmächtigung auszugehen und darf die Auskunft verweigern. Bringt der Betroffene anschließend Klage ein und erteilt der Verantwortliche daraufhin die Auskunft, hat der Verantwortliche keinen Grund zur Klagsführung gegeben. Der Betroffene trägt – als Kläger – gemäß § 45 ZPO die Kosten des Verfahrens und hat dem Verantwortlichen **Kostenersatz** zu erstatten ([OLG Graz 14.03.2025, 5R28/25i](#)).

- Hat der Verantwortliche **Zweifel an der Identität** eines Betroffenen, kann er nach Art 12 Abs 6 DSGVO weitere Informationen zu dessen **Identifizierung** einfordern. Der Verantwortliche darf nicht generell einen **Identitätsnachweis** verlangen, sondern muss im Einzelfall prüfen und entscheiden. Der Verantwortliche kann sich weigern, der **Betroffenen-anfrage** nachzukommen, wenn er den Betroffenen nicht identifizieren kann. In einem solchen Fall muss er jedoch glaubhaft machen, nicht in der Lage zu sein, den Betroffenen zu identifizieren. Erstattet der Verantwortliche kein Vorbringen zum Grund seines Verlangens auf Vorlage eines Lichtbildausweises zur Identifizierung, **veranlasst** er eine **Klagsführung** durch den Betroffenen und § 45 ZPO kommt nicht zur Anwendung ([OLG Graz, 13.03.2025, 2R32/25f](#)).

### Rechtsprechung des BVwG

[BVwG 05.03.2025, W211 2291833-1](#)

#### **Medienprivileg, Bürgerjournalismus**

- Ein Websitebetreiber veröffentlichte eine Strafverfügung gegen einen Beamten, ohne dessen Namen zu anonymisieren. Die DSB gab der Datenschutzbeschwerde des Beamten statt und stellte fest, dass der Websitebetreiber ihn in seinem Recht auf Geheimhaltung verletzt hat (Spruchpunkt 1). Zudem trug sie dem Websitebetreiber auf, sämtliche personenbezogene Daten des Beamten von der Website zu löschen (Spruchpunkt 2). In der Folge wurde der Beitrag entfernt und eine geschwärzte Version der Strafverfügung online gestellt. Der Websitebetreiber erhob Bescheidbeschwerde beim BVwG. Dieses bestätigte die Entscheidung der DSB hinsichtlich der Verletzung der Geheimhaltungspflicht (Spruchpunkt 1), behob jedoch den Löschungsauftrag (Spruchpunkt 2).

Das BVwG hat erwogen: Der zu beurteilende Verstoß gegen das Recht auf Geheimhaltung war mit der Entfernung der ungeschwärzten Strafverfügung abgeschlossen. In vergleichbaren Fällen sprach der VwGH aus, dass bei der Beurteilung der Rechtmäßigkeit eines **abgeschlossenen Vorgangs** einer möglichen Datenschutzverletzung die **zu diesem Zeitpunkt geltende Rechtslage anzuwenden** ist. Da jedoch nicht festgestellt werden konnte, ob die Löschung vor oder nach Inkrafttreten des § 9 DSG (neu) erfolgte und dies auf das Ergebnis keinen Einfluss hat, konnten dahingehende Ermittlungen unterbleiben.

Das **Medienprivileg** des § 9 Abs 1 DSG (alt) ist nicht anwendbar, weil die Website kein Medienunternehmen iSd MedienG ist. Ein Medieninhaber wird erst dann zum Medienunternehmer, wenn über den Zweck der bloßen Verbreitung von Inhalten hinaus ein

Unternehmen mit einem Mindestmaß an **unternehmerischen Strukturen** betrieben wird, dessen Unternehmenszweck die inhaltliche Gestaltung der Website ist, die von einer Redaktion vorgenommen wird. Die Website beinhaltet zwar redaktionelle Beiträge, stellt aber auch eine Plattform für selbständig agierende Mitgliedsgruppen und zur Verbreitung von Informationen über geplante Aktionen dar, wobei Mitgliedsgruppen auch teilweise selbständig Beiträge hochladen können. **Bürgerjournalismus** ist von § 9 Abs 1 DSG (alt) nicht umfasst.

Eine unmittelbare Anwendung des **Art 85 Abs 2 DSGVO** scheidet aus, da diese Bestimmung keine inhaltlichen Regelungen enthält, sondern Mitgliedstaaten verpflichtet, Regelungen zu erlassen.

Auch **§ 9 Abs 1 DSG (neu)** referenziert als Zielgruppe für die entsprechenden Privilegierungen auf Medienunternehmen nach dem MedienG, weshalb diese Bestimmung ebenfalls nicht anwendbar ist. Da auch § 9 Abs 1 DSG (neu) den Bürgerjournalismus nicht ausreichend berücksichtigt, ist auf die DSGVO zurückzugreifen.

Daten sind **nicht allgemein verfügbar**, wenn sie nicht einem unbestimmten Personenkreis zugänglich sind. Die Strafverfügung war im Rechtsinformationssystem des Bundes (**RIS**) nicht abrufbar, sodass das personenbezogene Datum des Beamten nicht allgemein verfügbar war.

Der Websitebetreiber hat zwar ein berechtigtes Interesse daran, über Einschränkungen von Grundrechten und behördlichen Entscheidungen zu informieren, die Veröffentlichung des Namens des Beamten war jedoch **nicht erforderlich**, um dieses Ziel zu erreichen. Die Kritik an der behördlichen Entscheidung kann auch ohne Nennung des Namens des Beamten geäußert werden, sodass die Nennung des Beamten nicht durch Art 6 Abs 1 lit f DSGVO gerechtfertigt war.

Mit der **Entfernung der ungeschwärzten Strafverfügung** entsprach der Websitebetreiber dem Auftrag der DSB. Zum Entscheidungszeitpunkt des BVwG war daher der geforderte Zustand hergestellt, sodass der **Leistungsauftrag aufzuheben** war.

[BVwG 06.03.2025, W292 2289837-1](#)

#### **Auskunft, Identifizierung, Zurückverweisung**

- Ein Deutscher begehrte Auskunft von einem österreichischen Inkassounternehmen, das eine unselbständige Zweigniederlassung in Deutschland betreibt. Der Deutsche übermittelte dem Inkassounternehmen eine teilweise geschwärzte Kopie seines Personalausweises. Während Vor- und Nachname des Betroffenen lesbar waren, wurden weitere Angaben, darunter insb das Geburtsdatum,

geschwärzt. Nachdem das Inkassounternehmen dem Auskunftersuchen des Deutschen nicht nachgekommen war, erhob dieser Datenschutzbeschwerde an den **Landesbeauftragten für den Datenschutz Niedersachsen**. Über Anregung des in weiterer Folge involvierten **Bayerischen Landesamts für Datenschutzaufsicht** zog die **DSB** als **federführende Aufsichtsbehörde** die Rechtssache an sich. Die DSB gab der Datenschutzbeschwerde des Deutschen folge. Dagegen erhob das Inkassounternehmen eine erfolgreiche Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Da sich die **Hauptniederlassung** des Verantwortlichen, nämlich des Inkassounternehmens, in Österreich befand, ging die DSB zu Recht von ihrer **Zuständigkeit** aus.

Das Inkassounternehmen teilte der DSB mit, dass es zur Zuordnung des Auskunftersuchens genauere Informationen zur **Identität** des Deutschen benötige, weil sich unter dessen Namen mehrere Datensätze in der Forderungskartei des Inkassounternehmens befänden. Dennoch übermittelte das Inkassounternehmen jedoch ein an die E-Mailadresse des Deutschen gerichtetes E-Mail, welches Informationen zu Geldforderungen gegen einen **unbeteiligten Dritten** enthielt. Dies deshalb, weil die E-Mailadresse des Deutschen irrtümlich mit dem unbeteiligten Dritten verknüpft worden war.

Obwohl die DSB das Inkassounternehmen auf diese Personenverwechslung hingewiesen hat, verabsäumte sie es in weiterer Folge dahingehend zu ermitteln, ob das Inkassounternehmen **begründete Zweifel** an der Identität des Deutschen **haben durfte**. Da die DSB insofern zum maßgeblichen Sachverhalt bestenfalls bloß ansatzweise ermittelt hat, war die Angelegenheit zur Feststellung der eindeutigen Identität des Deutschen an sie **zurückzuverweisen**.

BVwG 11.03.2025, W211 2293097-1

### **Hackerangriff, Benachrichtigung, Präklusion**

- Im Jahr 2019 ereignete sich ein **Hackerangriff** auf die elektrische Datenbank einer Bücherei. Die Datenbank wurde kopiert und samt personenbezogenen Daten der Nutzer auszugsweise auf den anonymen Filehostingdienst **Anonfiles** veröffentlicht. Die Bücherei informierte die Öffentlichkeit über den Vorfall durch eine Bekanntmachung auf ihrer Webseite und verschickte eine E-Mail an alle betroffenen Nutzer mit einem Hinweis auf einen erforderlichen Passwortwechsel. Darüber hinaus fand eine mediale Berichterstattung betreffend des Hackerangriffs statt, über welche die Nutzer zumindest eine allgemeine Kenntnis erlangten. Im Jahr 2021 erhob ein Nutzer

Datenschutzbeschwerde bei der DSB. Er erachtete sich in seinem Recht auf Geheimhaltung gemäß § 1 Abs 1 DSGVO und in Bezug auf die Informationspflichten gemäß Art 13 und 14 DSGVO verletzt.

Die DSB stellte fest, dass die Bücherei mangels geeigneter technischer und organisatorischer Maßnahmen gemäß Art 32 DSGVO das Recht auf Geheimhaltung verletzt habe. Hinsichtlich der behaupteten Verletzung im Recht auf Information wurde die Datenschutzbeschwerde abgewiesen. Die DSB führte zudem aus, dass keine Präklusion gemäß § 24 Abs 4 DSG eingetreten sei. Die Bücherei erhob daraufhin (erfolgreich) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Eine bloß **beiläufige Kenntnisnahme** eines Ereignisses, das potenziell iZm einer (unrechtmäßigen) Verarbeitung personenbezogener Daten steht, **löst die subjektive Präklusivfrist des § 24 Abs 4 DSG nicht aus**. Gemäß Art 34 Abs 1 DSGVO hat der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten die Betroffenen **unverzüglich zu benachrichtigen**.

Nach Bekanntwerden des Hackerangriffs erstattete die Bücherei umgehend eine Meldung gemäß Art 33 Abs 1 DSGVO an die DSB. Weiters informierte die Bücherei mittels **öffentlicher Bekanntmachung auf der eigenen Webseite** über den Hackerangriff. Eine persönliche Betroffenheit war aus dieser Information zwar nicht mit an Sicherheit grenzender Wahrscheinlichkeit abzuleiten. Zusätzlich nahm die Bücherei aber auch eine **individuelle Benachrichtigung der Betroffenen via E-Mail** vor, wobei die öffentliche Bekanntmachung direkt verlinkt war.

Die versendete E-Mail verfolgte hauptsächlich den Zweck, die Betroffenen zu einem **Passwortwechsel** zu bewegen. Dies genügte in der konkreten Konstellation den Anforderungen an eine klare und einfache Sprache nach Art 34 Abs 2 DSGVO.

Der Nutzer musste somit **spätestens aufgrund der persönlichen Verständigung** – über den ihm bereits allgemein bekannten Vorfall – einen **begründeten Verdacht** seiner persönlichen Betroffenheit iSd § 24 Abs 4 DSG haben. Die **einjährige subjektive Präklusivfrist** betreffend die Möglichkeit der Erhebung einer Datenschutzbeschwerde war daher im Jahr 2020 abgelaufen.

### **Geldbuße, Mitwirkungspflicht, Anweisung, Selbstbeziehung, Strafbemessung**

- Die **Medieninhaberin** und Herausgeberin einer Tageszeitung sowie Betreiberin eines Online-Nachrichtendienstes verarbeitete personenbezogene Daten zahlreicher Privatpersonen. Zwischen 2020 und 2022 führte die DSB mehrere Beschwerdeverfahren, in deren Rahmen sie die Medieninhaberin wiederholt aufforderte, Stellungnahmen abzugeben. Trotz mehrfacher und teils per RSb-Brief zugestellter Aufforderungen reagierte die Medieninhaberin in mehreren Verfahren nicht oder nur verspätet auf die Anfragen der DSB. Die Medieninhaberin wurde jeweils ausdrücklich auf ihre Mitwirkungspflicht nach Art 31 DSGVO sowie auf die Möglichkeit der Einleitung eines Verwaltungsstrafverfahrens hingewiesen. In einem der Verfahren wurde der Medieninhaberin aufgetragen, einem Betroffenen binnen vier Wochen eine Auskunft gemäß **Art 15 DSGVO zu erteilen**. Dieser Verpflichtung kam die Medieninhaberin erst zehn Tage **nach Ablauf der gesetzten Frist** nach.

Während des relevanten Zeitraums war die interne Organisation der Medieninhaberin erheblich beeinträchtigt. Aufgrund der **COVID-19 Pandemie** kam es zu einem erheblichen Anstieg von Betroffenenanfragen sowie zu strukturellen Veränderungen, wie Kurzarbeit, Homeoffice und einem Einstellungsstopp. Die Medieninhaberin war bewusst gegen die Inanspruchnahme externer Unterstützung.

Die DSB leitete ein Verwaltungsstrafverfahren gegen die Medieninhaberin ein. Im Jahr 2022 setzte sie dieses Verfahren bis zur rechtskräftigen Entscheidung durch den EuGH in der Rechtssache C-807/21, *Deutsche Wohnen*, ausgesetzt. Nach Fortsetzung des Verfahrens verhängte die DSB gegen die Medieninhaberin eine Geldbuße wegen Verletzung der **Mitwirkungspflicht** und Nichtbefolgung einer **Anweisung der DSB**. Dagegen erhob die Medieninhaberin eine teilweise erfolgreiche Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: **Art 31 DSGVO** legt dem Verantwortlichen eine **verwaltungsrechtliche Kooperationspflicht** auf. Diese Verpflichtung besteht unabhängig davon, welche Fragen die DSB stellt oder wie das Verfahren ausgeht. Sie hängt auch nicht von der eigenen Beurteilung des Sachverhalts durch die Medieninhaberin ab.

**Mitwirkungspflichten** stehen in einem **Spannungsverhältnis** zum nemo tenetur-Grundsatz ("**Selbstbelastungsverbot**"). Zwar besteht die Garantie des Selbstbeziehungsverbots bereits im Vorfeld eines Verwaltungsstrafverfahrens, sie **gilt jedoch nicht absolut** und kann eingeschränkt

werden, solange der Grundkern dieses Verfahrensrechts erhalten bleibt. Melde- oder Auskunftspflichten, die nicht intentional auf eine Informationsbeschaffung zum Zwecke strafrechtlicher Verfolgung des Verpflichteten gerichtet sind, gelten als zulässig. Ein **Verstoß gegen Art 6 EMRK** liegt nur dann vor, **wenn eine Selbstauskunft die Gefahr** einer (verwaltungs-)strafrechtlichen Verfolgung mit sich bringt und einer Selbstbeziehung gleichkommt. Das **Recht zu schweigen** darf jedoch nicht dazu führen, dass jegliche Zusammenarbeit mit einer Behörde verweigert wird.

Die Medieninhaberin konnte sich über die **Rechtswidrigkeit ihres Verhaltens nicht im Unklaren sein**. Wie sich aus den jeweiligen behördlichen Aufforderungen klar und eindeutig ergibt, hat die DSB jeweils auf die Bestimmung des Art 31 DSGVO sowie den Umstand hingewiesen, dass im Falle der Nichtmitwirkung eine Geldbuße iSd Art 83 DSGVO verhängt werden könne.

Da der Konzernumsatz zwischen EUR 50.000.000 und EUR 100.000.000 liegt, hatte nach den **Leitlinien des EDSA** eine Anpassung der Geldbuße anhand der Größe der Medieninhaberin zu erfolgen. Zumal der Unternehmensumsatz am unteren Ende der angegebenen Spanne liegt, ist der von der DSB herangezogene Prozentsatz von 15% zu hoch. Neben den Herausforderungen durch die COVID-19-Pandemie ist als **mildernd** zu berücksichtigen, dass die Auskunft nur zehn Tage nach Ablauf der Leistungsfrist erteilt wurde. Als **erschwerend** ist zu berücksichtigen, dass die Medieninhaberin auch nach Zustellung der ersten Aufforderung zur Rechtfertigung, weiter gegen ihre Mitwirkungspflicht verstoßen hat.

### **Auskunft, Vollmacht, Korrespondenz, Datenkopie, Löschung**

- Eine Kundin buchte zwei Flugtickets für sich und ihren Ehemann bei einer Fluggesellschaft. Aufgrund geänderter Reisepläne wollte sie die Flüge umbuchen und kontaktierte hierfür die Fluggesellschaft telefonisch. Das Telefonat wurde mit Einverständnis der Kundin aufgezeichnet. Da die Kundin aufgrund des Telefonats davon ausging, dass eine Stornierung und Erstattung des Ticketpreises möglich sei, stornierte sie die Flüge telefonisch. Nach Erhalt einer Bestätigungsemail, die eine Rückerstattung von nur USD 5,60 pro Flug auswies, forderte ihr Ehemann per E-Mail – unter Hinweis auf seine Tätigkeit als Rechtsanwalt – die vollständige Rückerstattung sowie die Herausgabe der Telefonaufzeichnung. Der Ehemann gab an, die Kundin rechtsfreundlich zu vertreten, ein Nachweis der Bevollmächtigung wurde jedoch nicht beigefügt.

Nachdem die Fluggesellschaft die Herausgabe trotz mehrfacher Aufforderung ablehnte, erhob die Kundin eine Datenschutzbeschwerde bei der DSB wegen Verletzung ihres Auskunftsrechts. Die Fluggesellschaft argumentierte, dass kein **formelles Auskunftersuchen** gemäß Art 15 DSGVO gestellt wurde und die Aufzeichnung aufgrund der internen Löschrfrist von zwei Wochen bereits **gelöscht** wurde. Nachdem die DSB die Stellungnahme der Fluggesellschaft an die Kundin weiterleitete, änderte diese ihren Antrag und begehrte die Feststellung, dass die **Löschung der Aufzeichnung** nach Stellung eines Auskunftersuchens ihr Recht nach Art 15 DSGVO **verletzte**. Gegen den abweisenden Bescheid der DSB erhob die Kundin eine (erfolglose) Beschwerde an das BVwG.

Das BVwG hat erwogen: Das Auskunftsrecht ist ein höchstpersönliches und damit ein subjektives Recht, das an eine bestimmte Person gebunden ist. Ein Auskunftersuchen kann jedoch auch durch einen rechtlichen Vertreter gestellt werden. Mit der **bloßen Berufung** eines Rechtsanwalts auf die ihm erteilte Vollmacht gemäß § 8 Abs 1 RAO kann die Bevollmächtigung nur beim Einschreiten vor einer Behörde oder vor einem Gericht nachgewiesen werden.

Beauftragt eine Betroffene einen Rechtsanwalt mit der Durchsetzung ihres Auskunftsrechts, muss der Verantwortliche die **Vollmacht** und **Identität** der Betroffenen prüfen. Da die Fluggesellschaft wochenlang mit dem Ehemann **korrespondierte**, ohne den Nachweis der Bevollmächtigung zu verlangen, kann sie sich jedoch nicht **nachträglich** darauf berufen, dass ihr die Vollmacht nicht vorgelegt wurde.

Die DSGVO sieht **keine Formvorschriften** oder Mindestinhalte für Auskunftersuchen vor. Das Ersuchen ist auf seinen Inhalt zu prüfen, wobei der Maßstab anzulegen ist, wie der Empfänger das Ersuchen nach Wortlaut und Geschäftszweck objektiv verstehen konnte. Die Kundin forderte zunächst lediglich die **Herausgabe der Aufzeichnung**, was kein Auskunftersuchen iSd Art 15 DSGVO ist. Erst mit einer späteren E-Mail, die nach Löschung der Aufzeichnung an die Fluggesellschaft geschickt wurde, verwies die Kundin auf ihr Ersuchen gemäß Art 15 Abs 3 DSGVO und gab der Fluggesellschaft zu erkennen, dass sie Auskunft über ihre verarbeiteten personenbezogenen Daten verlangt.

Das Recht auf **Erhalt einer Datenkopie** gemäß Art 15 Abs 3 DSGVO regelt lediglich die **Form der Auskunftserteilung** und begründet kein zusätzliches eigenständiges Recht. Wird die Zurverfügungstellung einer Datenkopie gefordert, kann darauf geschlossen werden, dass implizit auch um eine generelle Auskunftserteilung ersucht wird.

Unter Berufung auf Art 15 Abs 3 DSGVO steht jedoch keine über das nach Art 15 Abs 1 DSGVO vorgesehene Maß hinausgehende Auskunftserteilung zu. Da die Aufzeichnung zum Zeitpunkt der Stellung des Auskunftersuchens bereits **gelöscht** war, konnte die Entscheidung darüber, ob die Zurverfügungstellung einer Datenkopie zur Ausübung der Betroffenenrechte unerlässlich gewesen wäre dahingestellt bleiben.

Der **Umfang** der zu erteilenden Auskunft richtet sich nach dem Zeitpunkt, in dem das Auskunftersuchen gestellt wird. Wenn der Verantwortliche keine personenbezogenen Daten mehr verarbeitet, ist er zur Erteilung einer **Negativauskunft** verpflichtet. Verantwortliche haben gemäß **§ 24 Abs 6 DSGVO** bis zum Abschluss des Verfahrens vor der DSB die Möglichkeit, die behauptete Rechtsverletzung **nachträglich zu beseitigen**, in dem sie den Anträgen entsprechen. Da im Zeitpunkt der Löschung noch kein Auskunftersuchen vorlag, hat die Fluggesellschaft nicht gegen Art 15 DSGVO verstoßen. Zudem hat die Fluggesellschaft, während des Verfahrens, die DSB über die automatische Löschung der Aufzeichnung informiert und hat somit **nachträglich Auskunft erteilt**. **Anm: Der Unterscheid zum oben zusammengefassten Urteil des OLG Graz (OLG Graz 14.03.2025, 5R28/25i) besteht darin, dass die Fluggesellschaft sich trotz Fehlen der Vollmacht auf eine Korrespondenz eingelassen hat.**

#### Aus der weiteren Rechtsprechung des BVwG:

- Befasst sich die DSB nicht mit einer Datenschutzbeschwerde können Betroffene das **BVwG befassen** (§ 24 Abs 8 DSG). Die DSB lehnte die Behandlung der Datenschutzbeschwerde ab und verweigerte damit die Sachentscheidung, weil die Datenschutzbeschwerde exzessiv gewesen sei. Das "Kernanliegen" der Datenschutzbeschwerde war den Kontakt zum minderjährigen Kind des nichtmehr zur Obsorge berechtigten Vaters – unter Umgehung eines gerichtlichen Kontaktverbots – herzustellen. Die Datenschutzbeschwerde erwies sich aber schon aufgrund ihrer **Struktur und Ausführung** als **exzessiv** und **rechtsmissbräuchlich** (700 Seiten). Denn bereits die Durchsicht von 700 Seiten zur Identifizierung allfälliger Mängel bewirkt einen **unzumutbaren Aufwand** ([BVwG 11.03.2025, W137 2305838-1](#)).
- Kann die behauptete Offenlegung personenbezogener Daten **nicht festgestellt** werden, liegt **keine Verletzung** des Rechts auf Geheimhaltung vor ([BVwG 11.03.2025, W211 2288587-1](#)). **Anm: Die Beweislast für die monierte Datenverarbeitung trägt der Betroffene.**



## Rechtsprechung der LVwG

Aus der Rechtsprechung der LVwG:

- Die Tatsache, wer abgabenrechtlicher Halter eines Hundes ist, unterliegt der **Amtsverschwiegenheit** gemäß Art 20 Abs 3 B-VG, sofern diese Tatsache **geheim** ist. Wird der Name einer Hundehalterin der Abgabenbehörde wegen der **Meldung** einer **Hundehaltung** auf der Grundlage eines Abgabengesetzes bekannt, unterliegt der Name der Hundehalterin auch dem **Steuergeheimnis** gemäß § 48a BAO. Die Abgabenbehörde darf den Namen einer Hundehalterin an eine Person, die gestützt auf ein Auskunftsgesetz, die Herausgabe dieses Namens zur Verfolgung eines rechtlichen Interesses (Einbringung einer **Besitzstörungsklage**) verlangt, **nicht herausgeben** ([LVwG NÖ 25.03.2025, LVwG-AV-1248/002-2024](#)).

## Beschlüsse der EK

- Am **23.04.2025** veröffentlichte die EK eine Pressemitteilung, in der sie ua mitteilte gegen Apple und Meta auf das Digital Markets Act (**DMA**) gestützte Geldbußen verhängt zu haben. Gegen Apple wurde wegen Nichteinhaltung der **Lenkungsregeln** des DMA eine Geldbuße iHv **EUR 500 Mio** verhängt. Gegen Meta wurde wegen eines bereits abgeänderten binären **"Consent or Pay"-Modells** eine Geldbuße iHv EUR 200 Mio verhängt. Weiters stellte die EK fest, dass **Facebook Marketplace** nicht mehr als **Online-Vermittlungsdienst** iSd DMA benannt werden sollte ([EK Pressemitteilung 23.04.2025, IP/25/1085](#)).

## Nationale Rechtsakte

- Am **23.04.2025** wurde die Verordnung der Rundfunk und Telekom Regulierungs-GmbH, mit der der Detaillierungsgrad und die Form der Bereitstellung des Entgeltnachweises festgelegt werden (**Einzelentgeltnachweisverordnung 2025; EEN-V 2025**), [BGBl II 2025/75](#), kundgemacht. Die Einzelentgeltnachweisverordnung 2025 regelt die **Rechnungslegung** für die Erbringung eines **nummerngebundenen interperso-nellen Kommunikationsdienstes** oder eines **Internetzugangsdienstes**. **Anm:** Nummerngebundene interpersonelle Kommunikationsdienste sind Festnetz- und Mobiltelefonie sowie Dienste, die den Anruf einer Telefonnummer ermöglichen (zB [noch] Skype und Viber). Internetzugangsdienste stellen die Verbindung zum Internet her (zB A1, Magenta und Hutchison Drei).

to the point

# Datenschutzmonitor. 18/2025 vom 07.05.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 29.04.2025, 49617/22, *Kavecansky/Slovakia* (Notariat, Hausdurchsuchung, Rechtsstaatsprinzip)

- **Rechtsprechung des EuGH**

EuGH 30.04.2025, C-313/23, *Inspektorat kam Visshia* (Datenschutz-Aufsicht, Gerichtsbarkeit, Rollenverteilung)

- **Rechtsprechung des VwGH**

VwGH 01.04.2025, Ro 2024/04/0005; Ro 2023/04/0051 (Kohärenzverfahren, Aussetzung)

VwGH 03.04.2025, Ra 2025/01/0073 (Berichtigung, Melderegister, Zuständigkeit)

- **Rechtsprechung des BVwG**

BVwG 27.02.2025, W298 2305443-1 (Rechtsanwalt, Auskunft, Reaktionspflicht, Geldbuße)

BVwG 13.03.2025, W137 2253556-1 (AuskunftspflichtG, Grundrecht auf Informationen)

BVwG 10.03.2025, W211 2272691-1; 24.02.2025, W211 2272785-1 (Beschwerdegegner, *res iudicata*)

- **EU-Rechtsakte**

DurchführungsVO zur Transparenz und Targeting politischer Werbung samt Anhang

## To the Point:

### Rechtsprechung des EGMR

EGMR 29.04.2025, 49617/22, Kavecansky/Slowakei

#### **Notariat, Hausdurchsuchung, Rechtsstaatsprinzip**

- Gegen einen slowakischen **Notar** wurde ein Strafverfahren wegen schwerer Unterschlagung eingeleitet, weil er – so der Verdacht der Ermittler – mehrere hunderttausende Euro von seinen Einlagenkonten nicht freigegeben haben soll. Der ermittelnde Beamte erließ Durchsuchungsbefehle für die **Durchsuchung der Notariatskanzlei** sowie der Wohnung des Notars auf Grundlage der slowakischen Strafprozessordnung. Die Durchsuchungsbefehle enthielten keine näheren Angaben, wie mit Material umzugehen sei, welches nicht dem laufenden Strafverfahren zugeordnet werden könne oder dem notariellen Berufsgeheimnis unterliege. Beide Durchsuchungsbefehle wurden von der Staatsanwaltschaft genehmigt.

Der Notar wandte sich an den EGMR und machte eine Verletzung seines Rechts auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK geltend. Die Beschwerde an den EGMR begründete der Notar ua damit, dass der slowakischen Strafprozessordnung die Möglichkeit einer Überprüfung der Rechtmäßigkeit einer solchen Ermittlungsmaßnahme im Vorfeld durch eine unabhängige Richterschaft fremd sei. Eine wirksame Überprüfung der Rechtmäßigkeit der betreffenden Ermittlungsmaßnahme wäre umso notwendiger gewesen, als die zu beschlagnahmenden Gegenstände und Unterlagen zu keinem Zeitpunkt im Vorfeld konkretisiert worden seien. Der Notar forderte EUR 5.000 als Ersatz für seinen immateriellen Schaden. Der EGMR stellte eine Verletzung von Art 8 EMRK fest und sprach dem Notar EUR 5.000 an immateriellem Schaden zu.

Der EGMR hat erwogen: Im Zusammenhang mit Durchsuchungen und Beschlagnahmen muss das innerstaatliche Recht dem Einzelnen Schutz vor willkürlichen Eingriffen in die Rechte nach Art 8 EMRK bieten. Maßnahmen wie **Hausdurchsuchungen** und **Beschlagnahmen** stellen einen **schwerwiegenden Eingriff** in das Privatleben, die Wohnung und den Schriftverkehr dar. Aus diesem Grund haben derartige Maßnahmen auf **besonders präzisen Gesetzen** zu beruhen. Klare und detaillierte Regelungen zu diesem Thema sind unerlässlich. Hinsichtlich des Verfahrensschutzes im Rahmen von Art 8 EMRK hat der EGMR dem Berufsgeheimnis von **rechtspflegenden Berufen** besondere Bedeutung beigemessen. Die Staatsanwaltschaft hat nach slowakischem Recht keinen unabhängigen Status, der mit dem eines unabhängigen Gerichts vergleichbar wäre. Das

Recht des Notars auf Achtung seines Privatlebens und seiner Wohnung wurde verletzt, weil weder ein vorheriger **richterlicher Beschluss** vorlag noch die Möglichkeit bestand, die Entscheidung über die Anordnung der Durchsuchungen oder die Art und Weise ihrer Durchführung **nachträglich wirksam gerichtlich überprüfen** zu lassen. Die Situation wurde dadurch erschwert, dass die Durchsuchungen in den **Räumlichkeiten eines Notars** stattfanden. Dem Notar wurde dadurch jener Mindestschutz vorenthalten, auf den er nach dem **Rechtsstaatsprinzip** in einer demokratischen Gesellschaft Anspruch gehabt hätte.

### Rechtsprechung des EuGH

EuGH 30.04.2025, C-313/23, Inspektorat kam Visshia

#### **Datenschutz-Aufsicht, Gerichtsbarkeit, Rollenverteilung**

- Durch eine Verfassungsänderung wurde in Bulgarien beim Obersten Justizrat eine **Aufsichtsbehörde** zur Überwachung der Tätigkeit der Justiz eingerichtet. Zu den Aufgaben dieser Aufsichtsbehörde gehört ua die Überwachung der **Integrität** und des **Fehlens von Interessenkonflikten** bei Richtern, Staatsanwälten und Strafrechtspflegern (im Folgenden: **Justizangehörige**). Nach Ablauf der Frist zur Abgabe der Vermögensklärungen dieser Justizangehörigen beantragte die Aufsichtsbehörde eine richterliche Genehmigung zur Aufhebung des Bankgeheimnisses für die Konten mehrerer Justizangehörigen sowie deren Familienangehörigen. Das angerufene Gericht legte dem EuGH daraufhin mehrere Fragen zur Vorabentscheidung vor, ua (i) zur Fortführung der Amtsgeschäfte durch die Aufsichtsbehörde, obwohl die Amtszeit einzelner Mitglieder abgelaufen war, (ii) zum Anwendungsbereich der DSGVO sowie (iii) zur Rollenverteilung zwischen Aufsichtsbehörde und Gericht.

Der EuGH hat erwogen: Der **Grundsatz der richterlichen Unabhängigkeit** steht der Praxis eines Mitgliedstaats entgegen, wonach die Mitglieder eines Justizorgans nach Ablauf ihrer **verfassungsmäßigen Amtszeit** im Amt bleiben, wenn es dafür keine gesetzliche Grundlage und keine zeitliche Begrenzung gibt.

Eine Datenverarbeitung, die dazu dient, bei **Justizangehörigen** die Integrität und das Bestehen etwaiger Interessenkonflikte zu überwachen, fällt in den **sachlichen Anwendungsbereich** der DSGVO – auch wenn diese Daten dem **Bankgeheimnis** unterliegen.

Nach bulgarischem Recht ist die Aufsichtsbehörde ua dafür zuständig, bei Justizangehörigen die **Integrität** und das **Fehlen von**

**Interessenkonflikten** zu überwachen und die Erklärung über die **Vermögensverhältnisse** zu überprüfen. Stimmen die betreffenden Justizangehörigen oder deren Familienangehörige dem Zugang zu ihren Daten nicht zu, kann die Aufsichtsbehörde eine richterliche Genehmigung auf Zugang zu den personenbezogenen Daten beantragen.

Für diese Datenverarbeitung **Verantwortlicher** iSd Art 4 Z 7 DSGVO ist die **Aufsichtsbehörde** und nicht das Gericht. Die Kontrolle des Gerichts hat nach dem nationalen Recht rein formal zu sein und beschränkt sich bei der Aufhebung des Bankgeheimnisses auf die Frage, ob die zu überprüfenden Personen erklärungs-pflichtig sind. Das Gericht wird nur auf Antrag der Aufsichtsbehörde tätig. Der Kreis der Personen und die Daten, die Gegenstand der Verarbeitung sein können, die Zwecke der Verarbeitung und das für deren Erreichung zuständige Organ werden durch nationales Gesetz bestimmt. Die Personen, zu deren Daten die Aufsichtsbehörde Zugang haben will, bestimmt die Aufsichtsbehörde. Das Gericht bestimmt daher weder den Zweck der Verarbeitung noch die betroffenen Personen und Daten.

Ein **Gericht**, das lediglich die Offenlegung personenbezogener Daten genehmigt, ist **keine Aufsichtsbehörde** iSd Art 51 DSGVO, wenn es nicht ausdrücklich damit beauftragt wurde, die Anwendung der DSGVO zu überwachen.

Ein **nationales Gericht** muss die **Einhaltung der DSGVO nicht von Amts wegen überprüfen**, wenn kein konkreter Rechtsbehelf nach Art 78 oder 79 DSGVO vorliegt oder das nationale Recht ihm nicht ausdrücklich Kontrollbefugnisse gibt. Dies auch dann nicht, wenn allgemein bekannt ist, dass die Aufsichtsbehörde in der Vergangenheit gegen die DSGVO verstoßen hat.

## Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Das **Recht auf Berichtigung** personenbezogener Daten im **Melderegister** ist auf dem in Art 77 und 49 DSGVO und § 24 DSG vorgesehenen **Rechtsweg** geltend zu machen ([VwGH 03.04.2025, Ra 2025/01/0073](#)).
- Steht die **federführende Aufsichtsbehörde** noch nicht fest, regelt § 24 Abs 10 Z 2 DSG lediglich eine Hemmung des Fristenlaufs, enthält aber keine Grundlage für eine **Verfahrensaussetzung**. Gegenstand des Beschwerdeverfahrens vor dem BVwG ist nur die **Rechtmäßigkeit der beschneidmässigen Aussetzung** durch die DSB. Eine **Umdeutung** der Bescheidbeschwerde in eine Säumnisbeschwerde ist **ausgeschlossen** ([VwGH 01.04.2025, Ro 2024/04/0005](#); [Ro 2023/04/0051](#)).

## Rechtsprechung des BVwG

BVwG 27.02.2025, W298 2305443-1

### **Rechtsanwalt, Auskunft, Reaktionspflicht, Geldbuße**

- Ein **Rechtsanwalt** reichte im Auftrag des Bruders einer Erbin eine Pflichtteilsergänzungsklage ein. Die Erbin beschuldigte den Rechtsanwalt im Zuge dessen, unbefugt eine Namensabfrage gemäß §§ 5 und 6a Grundbuchsumstellungsgesetz durchgeführt zu haben, was zu einem Disziplinarverfahren führte. Dieses wurde mangels Nachweises einer solchen Abfrage jedoch eingestellt. Später stellte die Erbin ein Auskunftersuchen gemäß § 44 DSG mittels eines Formulars der DSB an den Rechtsanwalt, dem er nicht nachkam. Die DSB gab der Datenschutzbeschwerde der Erbin statt und stellte fest, dass der Rechtsanwalt gegen das Recht auf Auskunft verstoßen hatte. Sie hielt fest, dass die Auskunftspflicht nach Art 12 und 15 DSGVO unabhängig von der Nennung des Artikels oder der Verwendung eines bestimmten Formulars besteht. Gegen den Bescheid der DSB erhob der Rechtsanwalt zunächst Bescheidbeschwerde an das BVwG, das diese abwies. Daraufhin verhängte die DSB mit Straferkenntnis eine Geldbuße iHv EUR 400. Dagegen erhob der Rechtsanwalt erneut (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Das Recht auf Auskunft steht unter **keinen Voraussetzungen**. Es ist weder inhaltlich noch in Bezug auf die Form an bestimmte Anforderungen gebunden. Es ist lediglich notwendig, dass der Verantwortliche überhaupt erkennen kann, worauf sich das Auskunftersuchen des Auskunftswerbers richtet. Weiters ist ein **Auskunftersuchen an keinerlei Formvoraussetzungen geknüpft**, was auch eine falsche Bezeichnung miteinschließt – *falsa demonstratio non nocet*.

Nach **§ 9 Abs 4 RAO** besteht **keine gänzliche Ausnahme** von der **Auskunftspflicht für Rechtsanwälte**. Die Auskunftspflicht entfällt nur insoweit, als dies zur Sicherstellung des Schutzes der Partei, der Rechte und Freiheiten anderer Personen oder der Durchsetzung zivilrechtlicher Ansprüche erforderlich ist. Die RAO modifiziert nur die inhaltliche Ausgestaltung einer datenschutzrechtlichen Auskunft, indem sie eine **spezielle Verschwiegenheitspflicht** berücksichtigt. Das Auskunftsrecht bleibt jedoch bestehen. Der Rechtsanwalt muss daher auf ein Auskunftersuchen **reagieren**. Das völlige Unbeantwortet lassen des Auskunftersuchens ist daher jedenfalls rechtswidrig.

Da eine Auskunft auch dann zu erteilen ist, wenn der Verantwortliche keine Daten der Betroffenen verarbeitet ("**Negativauskunft**"), ist auch darüber zu informieren,

### **warum die Auskunft nicht erteilt werden kann.**


Der Rechtsanwalt handelte **vorsätzlich**. Die DSB erteilte einen ausdrücklichen Hinweis auf die Auskunftspflicht gemäß Art 15 DSGVO und die drohende Sanktion. Die von der DSB festgesetzte Strafe iHv EUR 400 erscheint daher unter Berücksichtigung des Tatunwerts und der grundsätzlichen Strafandrohung tat- und schuldangemessen.

#### Aus der weiteren Rechtsprechung des BVwG:

- Im Hinblick darauf, dass Auskünfte nach § 1 Abs 1 **AuskunftspflichtG** auch personenbezogene Daten betreffen können, greift diese Bestimmung in das Grundrecht auf Datenschutz nach § 1 Abs 1 DSG ein. Ebenso greift sie in Art 10 Abs 1 EMRK ein, weil die Verweigerung der Auskunft aufgrund von Verschwiegenheitspflichten das **Recht auf Zugang zu Informationen** beschränken kann. Im Hinblick auf § 1 Abs 2 DSG muss die gesetzliche Grundlage ausreichend präzise sein. Diese Anforderung ist durch § 1 Abs 1 AuskunftspflichtG erfüllt, weil diese Bestimmung die **gebotene Interessenabwägung** zwischen dem **Grundrecht auf Information** und jenem **auf Datenschutz** und damit einen **angemessenen Ausgleich** zwischen diesen beiden Grundrechtspositionen ermöglicht ([BVwG 13.03.2025, W137 2253556-1](#)).
- Führt die DSB das Datenschutzverfahren gegen den falschen **Beschwerdegegner** als Verantwortlichen, der nicht vom Rechtsschutzantrag umfasst ist, ist der Bescheid ersatzlos zu beheben. Wird ein Sachverhalt sowohl von einem Betroffenen als auch von der DSB aufgegriffen, um in einem Verfahren überprüft zu werden, führt dies zu **keiner res iudicata** (BVwG [10.03.2025, W211 2272691-1](#); [24.02.2025, W211 2272785-1](#)).

#### EU-Rechtsakte

- Am **30.04.2025** hat die Europäische Kommission den [Entwurf einer DurchführungsVO zur Verordnung \(EU\) 2024/900](#) über die **Transparenz und das Targeting politischer Werbung** samt **Anhang** veröffentlicht. Rückmeldungen sind binnen vier Wochen möglich. Mit der DurchführungsVO sollen das Format, die Vorlage und die technischen Spezifikationen der **Kennzeichnungen** und **Transparenzbekanntmachungen** politischer Anzeigen geregelt werden.



to the point

# Datenschutzmonitor. 19/2025 vom 14.05.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuG**

**NACHTRAG**

EuG 29.04.2025, T-319/24, *Meta/EDPB* (Meta, EDSA, unverbindliche Stellungnahme)

- **Rechtsprechung der Justiz**

OGH 28.03.2025, 8Ob14/25d (Smart Meter, Aussetzung)

OLG Wien 28.02.2025, 16R161/24z (Datenkopie, Fernzugriff)

OLG Wien 02.11.2025, 4R133/24v (Zuständigkeit, Klauselkontrolle, Speicherfrist, Drittlandtransfer)

OLG Innsbruck 27.03.2025, 7Bs64/25g (Trennung des Ermittlungsverfahrens, § 27 StPO)

- **Rechtsprechung des BVwG**

BVwG 11.03.2025, W211 2280469-1 und 24.04.2025, W211 2272439-1 (Beschwerdegegner, *res iudicata*)

- **EU-Rechtsakte**

DurchführungsVOs zur eIDAS (europäische Brieftaschen)

## To the Point:

### Rechtsprechung des EuG

#### NACHTRAG

EuG 29.04.2025, T-319/24, Meta/EDPB

#### **Meta, EDSA, unverbindliche Stellungnahme**

- Meta Platforms Ireland (**Meta**) bietet Nutzern ein "Consent or Pay"-Modell an, bei dem diese entweder der Verarbeitung ihrer personenbezogenen Daten für verhaltensbasierte Werbung zustimmen oder eine Gebühr zahlen, um den Dienst ohne diese Datenverarbeitung zu nutzen. Auf Anfrage dreier Datenschutzbehörden gab der EDSA eine **unverbindliche Stellungnahme** "*Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*" ab, in der er Kriterien für die Bewertung der Freiwilligkeit und Wirksamkeit der Einwilligung solcher Modelle festlegte. Meta beantragte beim EuG die Aufhebung dieser Stellungnahme und forderte Schadenersatz aufgrund wirtschaftlicher Nachteile. Das EuG wies die Klage teilweise zurück und teilweise ab und legte Meta die Verfahrenskosten auf.

Das EuG hat erwogen: Ob ein **Rechtsakt**

rechtlich **bindend** ist, hängt von seinem Inhalt, dem Kontext und den Befugnissen der ausstellenden Stelle ab. In seiner Stellungnahme betont der EDSA, dass die Bewertung der Freiwilligkeit und Wirksamkeit der Einwilligung stets im Einzelfall zu erfolgen hat. Zwar weist er darauf hin, dass **kostenpflichtige Alternativen** ohne kostenlose Option idR zur **Unwirksamkeit der Einwilligung** führen, dies hängt jedoch von mehreren Faktoren ab, etwa von der Bedeutung des Dienstes oder dem Preis der Alternative.

Die Stellungnahme enthält keine verbindlichen Vorgaben und entfaltet keine rechtlich bindende Wirkung. Formulierungen wie "sollte" oder "in den meisten Fällen" unterstreichen den **Empfehlungscharakter**. Zudem beruht die Stellungnahme auf Art 64 Abs 2 DSGVO, der dem EDSA lediglich erlaubt, zu allgemeinen Fragen Stellung zu nehmen. Auch wenn Meta oder die irische Datenschutzbehörde den Empfehlungen folgen, tun sie dies freiwillig.

Die Aufforderung der irischen Datenschutzbehörde, wonach Meta die Stellungnahme einhalten möge, verleiht dieser keine rechtliche Bindung. Selbst eine spätere verbindliche Entscheidung, die sich auf die Stellungnahme stützt, macht diese nicht rückwirkend verbindlich. Auch ein möglicher Widerspruch zur EuGH-Rechtsprechung ändert nichts an der **fehlenden Bindungswirkung** und begründet keinen Verstoß gegen das Recht auf effektiven Rechtsschutz. Dieser wäre dann eröffnet, wenn eine behördliche oder gerichtliche Entscheidung auf der

Stellungnahme basiert. Unterschiedliche Auslegungen sind kein Grund, eine unverbindliche Stellungnahme angreifbar zu machen. Solche Unterschiede sind systembedingt und durch Verfahren wie das **Vorabentscheidungsverfahren** oder das **Streitbeilegungsverfahren** abgesichert.

Ein **Schadenersatzanspruch** setzt voraus, dass ein rechtswidriges Verhalten eines Unionsorgans vorliegt, ein tatsächlicher Schaden entstanden ist und ein unmittelbarer Kausalzusammenhang zwischen Handlung und Schaden besteht. Diese Voraussetzungen sind nicht erfüllt. Die Stellungnahme des EDSA ist nicht rechtswidrig, weil sie keine verbindlichen Rechtswirkungen entfaltet. Ein Schaden ist nicht nachgewiesen, da sich die behaupteten wirtschaftlichen Einbußen auf hypothetische und zukünftige Entwicklungen stützen. Auch ein unmittelbarer Kausalzusammenhang liegt nicht vor. Da die Stellungnahme nicht bindend ist, kann sie nicht als unmittelbare Ursache für den behaupteten **Einnahmerückgang** von Meta angesehen werden. Die behaupteten Einnahmeverluste könnten allenfalls auf freiwillige Anpassungen durch Meta selbst oder auf noch nicht ergangene Entscheidungen zurückgehen – nicht aber auf die unverbindliche Stellungnahme des EDSA.

### Rechtsprechung der Justiz

OGH 28.03.2025, 8Ob14/25d

#### **Smart Meter, Aussetzung**

Eine **Strom-Verteilernetzbetreiberin** verlangte von einer Endverbraucherin die Duldung des Ausbaus eines veralteten Strommessgeräts. Die Endverbraucherin verweigerte dies und verwies zudem auf ihr Wahlrecht, einen mechanischen Zähler zu wählen. Das BG Krems gab der Klage der Strom-Verteilernetzbetreiberin statt. Das LG Krems hob infolge Berufung der Endverbraucherin dieses Urteil zur Verfahrensergänzung auf. Es stellte fest, dass ihre Vorbringen – insb mögliche Gesundheitsgefahren und Datenschutzbedenken – durch Sachverständigengutachten zu prüfen sind. Den Rekurs an den OGH ließ das Berufungsgericht im Hinblick auf ein anhängiges Vorabentscheidungsverfahren (C-468/24, *Netz Niederösterreich*) zu.

Der OGH hat erwogen: Das Verfahren ist bis zur Entscheidung des EuGH über das vom LG St. Pölten beim EuGH eingebrachten Vorabentscheidungsersuchen **zu unterbrechen** (C-468/24, *Netz Niederösterreich*). Das LG St. Pölten legte in einem Parallelverfahren dem EuGH ua die Fragen vor, ob (i) Netzbetreiber verpflichtet sind, dem Wunsch nach einem **konventionellen statt eines intelligenten Zählers** zu entsprechen, (ii) unionsrechtliche Vorgaben nationalen Regelungen entgegenstehen, die keine konkreten Anforderungen an die Datensicherheit von Messgeräten enthalten, (iii) der Begriff "**elektronisches**

**Kommunikationsnetz**" in Art 5 Abs 3 der Richtlinie 2002/58/EG auch **Stromnetze** umfasst, über die Daten zu Zwecken der Richtlinie 2019/944 übertragen werden, (iv) die EU-Grundrechte-Charta (**GRC**) einer nationalen Regelung entgegensteht, die keine Information über vorzeitige Datenabrufe im begründeten Einzelfall verlangt und (v) bei der Auslegung der einschlägigen Bestimmungen der Richtlinie 2019/944 die Rechtsprechung des EGMR zu Art 8 EMRK zu berücksichtigen ist.

#### Aus der weiteren Rechtsprechung der Justiz:

- Die auf das Erkenntnis des [BVwG vom 23.09.2020, W101 2132039-1](#), gestützte Ansicht des Beklagten, wonach kein Auskunftsanspruch besteht, wenn der Auskunftswerber über seinen Account **elektronischen Zugriff** auf seine Daten hat, **ist überholt**. Denn gemäß dem Urteil des [EuGH vom 04.05.2023, C-487/21, Österreichische Datenschutzbehörde](#), ist das in Art 15 Abs 3 S 1 DSGVO verankerte Recht auf Erhalt einer **"Kopie"** so zu verstehen, dass der betroffenen Person eine **originalgetreue und verständliche Reproduktion** all ihrer personenbezogenen Daten auszufolgen ist ([OLG Wien 28.02.2025, 16R161/24z](#)). **Anm:** Dieses Urteil könnte zu einer Divergenz zwischen der Rechtsprechung der Berufungsinstanzen im Verwaltungs- und Zivilrechtsweg führen. Denn, wie im Urteil auch angeführt, erachtete das BVwG es für zulässig, einem Auskunftersuchen durch Gewährung eines **Fernzugriffs** zu entsprechen. Auch der **EDSA** hält in seinen Guidelines zum Auskunftsrecht das Erteilen einer Auskunft via Fernzugriff für zulässig. Das OLG Wien meint, dass diese Rechtsprechung bzw Rechtsansicht überholt sei, weil laut dem EuGH eine "Kopie" der personenbezogenen Daten auszufolgen sei. Der EuGH sprach über die Frage, ob diese "Kopie" personenbezogener Daten über Fernzugang ausgefolgt werden könnte, jedoch nicht ab. Es bleibt daher abzuwarten, ob das BVwG dem OLG Wien folgen wird.
- Die **Zuständigkeit der DSB** schließt nicht aus, dass Zivilgerichte zur Auslegung von Datenschutzerklärung berufen sind. Eine Datenschutzerklärung in den AGB, die Vertragsbestandteil ist, unterliegt einer **Klauselkontrolle**. Nach Art 13 Abs 1 DSGVO muss der Verantwortliche bei der Datenerhebung klar benannt und mit Kontaktdaten angegeben werden, die **Nennung des Datenschutzbeauftragten** allein **reicht nicht** aus. Nach Art 6 DSGVO ist die Rechtsgrundlage für die Datenverarbeitung genau anzugeben. Ein allgemeiner Verweis auf Art 6 DSGVO genügt nicht. Auch die **Speicherdauer** personenbezogener Daten muss gemäß Art 13 Abs 2 lit a DSGVO genau oder anhand klarer Kriterien angegeben werden.

Pauschale Hinweise auf gesetzliche Fristen oder unternehmensinterne Abwägungen sind unzureichend. Werden Daten in **Dritt-länder** übermittelt, müssen Zielstaat, **Angemessenheitsbeschluss und Garantien** gemäß Art 13 Abs 1 lit f DSGVO konkret benannt werden ([OLG Wien 02.11.2025, 4R133/24v](#)).

- Der Staatsanwaltschaft ist gemäß **§ 27 StPO** von Amts wegen oder auf Antrag die **getrennte Führung** des **Ermittlungsverfahrens** gegen einzelne Beschuldigte oder wegen einzelner Straftaten gestattet, insbesondere um Verzögerungen zu vermeiden, **schutzwürdige Geheimhaltungsinteressen (§ 1 DSG)** eines Beschuldigten zu wahren oder die Haft des Beschuldigten zu verkürzen ([OLG Innsbruck 27.03.2025, 7Bs64/25g](#)).

#### Rechtsprechung des BVwG

##### Aus der Rechtsprechung des BVwG:

- Führt die DSB das Datenschutzverfahren gegen den **falschen Beschwerdegegner** als Verantwortlichen, der nicht vom Rechtschutzantrag umfasst ist, ist der Bescheid ersatzlos zu beheben. Wird ein Sachverhalt sowohl von einem Betroffenen als auch von der DSB aufgegriffen, um in einem Verfahren überprüft zu werden, führt dies zu **keiner res iudicata** (BVwG [11.03.2025, W211 2280469-1](#); [24.04.2025, W211 2272439-1](#)).

#### EU-Rechtsakte

- Am **07.05.2025** wurden die (i) "*Durchführungsverordnung (EU) 2025/846 der Kommission vom 6. Mai 2025 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf den grenzüberschreitenden Identitätsabgleich natürlicher Personen*", [ABI L 2025/846](#), (ii) "*Durchführungsverordnung (EU) 2025/847 der Kommission vom 6. Mai 2025 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Reaktion auf Sicherheitsverletzungen europäischer Brieftaschen für die digitale Identität*", [ABI L 2025/847](#), (iii) "*Durchführungsverordnung (EU) 2025/848 der Kommission vom 6. Mai 2025 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Registrierung von auf Brieftaschen vertrauenden Beteiligten*", [ABI L 2025/848](#), und (iv) "*Durchführungsverordnung (EU) 2025/849 der Kommission vom 6. Mai 2025 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des*



Europäischen Parlaments und des Rates in Bezug auf die **Übermittlung von Informationen an die Kommission und die Kooperationsgruppe für die Liste der zertifizierten europäischen Brieftaschen für die digitale Identität**", [ABI L 2025/849](#), veröffentlicht. Mit diesen vier DurchführungsVOs werden Anforderungen und Pflichten betreffend die **europäischen Brieftaschen** iSd [eIDAS](#) festgelegt bzw präzisiert.

to the point

# Datenschutzmonitor. 20/2025 vom 21.05.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Leitlinien veröffentlicht:

- **Rechtsprechung des EuGH / EuG**

EuGH SA 15.05.2025, Rs C-327/24, *Lolach* (Telekommunikation, Wettbewerb, Zugangsverpflichtung)

EuG 14.05.2025, T-36/23, *Stevi und The New York Times* (Dokumentenzugang, Richtigkeitsvermutung, Beweislast)

- **Rechtsprechung des VwGH**

VwGH 31.03.2025, Ra 2022/04/0143 (Exzess, Missbrauchsabsicht)

- **Rechtsprechung der Justiz**

OLG Graz 19.03.2025, 4R52/25m (Auskunft, Datenkopie, Bestimmtheit)

OLG Wien 12.02.2025, 33R23/25g (Beweisbeschaffung, Prozessstandpunkt, kein Rechtsmissbrauch)

OLG Wien 20.02.2025, 4R191/24y (routinemäßige Identitätsprüfung, Vollmacht)

- **Rechtsprechung des BVwG**

BVwG 27.03.2025, W298 2285480-1 (Erleichterungsgebot, Geldbuße, VStG, Anwendungsvorrang)

BVwG 04.03.2025, W176 2285563-1 (Arzt, Rolle, Gesundheitsdaten, Weiterverarbeitung)

BVwG 05.09.2024, W211 2287218-1 (Videoüberwachung, Personenbezug, Interessenabwägung, statistische Zwecke)

BVwG 06.03.2025, W292 2284288-2 (Betroffenheit, Amtswegigkeit, Mitwirkungspflicht)

BVwG 05.03.2025, W211 2272384-1 (Betroffenheit, Mitwirkungspflicht)

BVwG 03.10.2024, W137 2261950-1 ua (gekürzte Ausfertigung)

BVwG 10.03.2025, W137 2280882-2 (Exzess, Missbrauch)

- **Europäische Kommission**

Leitlinien zum Schutz Minderjähriger im Internet nach dem Gesetz über digitale Dienste (Schutz Minderjähriger, Online-Plattformen)

## To the Point:

### Rechtsprechung des EuGH / EuG

EuGH SA 15.05.2025, Rs C-327/24, *Lolach*

#### **Telekommunikation, Wettbewerb, Zugangsverpflichtung**

- Die deutsche Regulierungsbehörde für den Sektor der elektronischen Kommunikation verpflichtete eine Telekommunikationsanbieterin, anderen Betreibern Zugang zu bestimmten baulichen Anlagen zu gewähren, die nicht Teil des relevanten Markts sind. Die Regulierungsbehörde stützte ihren Beschluss auf die zur Umsetzung der RL (EU) 2018/1972 über den **europäischen Kodex für die elektronische Kommunikation (EKEK)** erlassenen nationalen Vorschriften. Die Telekommunikationsanbieterin erhob Klage und beantragte die Aufhebung der **Zugangsverpflichtung**. Eine solche Verpflichtung sei nur zulässig, wenn sowohl der Wettbewerb als auch die Interessen der Endnutzer beeinträchtigt seien. Die Regulierungsbehörde hielt dem entgegen, sie könne bei der Abwägung auch weitere Ziele des EKEK berücksichtigen und dürfe das Ziel der Entwicklung eines nachhaltig wettbewerbsorientierten Endkundenmarkts verfolgen.

Das vorliegende Gericht ersuchte den EuGH um Vorabentscheidung, ob die Regulierungsbehörde bei der Auferlegung einer Zugangsverpflichtung zu baulichen Anlagen, die nicht Teil des relevanten Markts sind, ausschließlich die in Art 72 EKEK genannten Voraussetzungen prüfen muss, oder ob sie gleichrangig auch die weiteren Ziele des Art 3 EKEK berücksichtigen darf.

Der Generalanwalt hat erwogen: Die Bestimmung des Art 72 Abs 2 EKEK ermächtigt die nationale Regulierungsbehörde, **Unternehmen mit beträchtlicher Marktmacht** zu verpflichten, Zugang zu baulichen Anlagen zu gewähren, auch wenn diese nicht Teil des relevanten Markts sind. Treffen beide Umstände zusammen, ist die nationale Regulierungsbehörde ermächtigt, eine Zugangsverpflichtung aufzuerlegen.

Die Bestimmung des Art 68 Abs 4 lit c EKEK regelt die Auferlegung von Verpflichtungen, die dann ua in den Art 72 und 73 EKEK präzisiert werden und sieht dabei vor, dass diese Verpflichtungen im Hinblick auf die Ziele des Art 3 EKEK gerechtfertigt sein müssen. Dementsprechend sind die nationalen Regulierungsbehörden befugt, sämtliche in den Art 69 bis 74 und 76 bis 81 EKEK festgelegten Verpflichtungen aufzuerlegen, wenn eine solche Auferlegung im Hinblick auf die in Art 3 EKEK genannten Ziele gerechtfertigt werden kann. Daraus folgt, dass die Zugangsverpflichtungen nach Art 72 Abs 2 EKEK durch die Ziele des Art 3 gerechtfertigt sein können.

Die Regulierungsbehörde darf die Zugangsverpflichtung zu baulichen Anlagen, die nicht Teil des relevanten Markts sind, auferlegen, wenn diese Verpflichtung zur Erreichung der in Art 3 EKEK genannten Ziele notwendig und verhältnismäßig ist.

EuG 14.05.2025, T-36/23, *Stevi und The New York Times*

#### **Dokumentenzugang, Richtigkeitsvermutung, Beweislast**

- Eine Journalistin der New York Times beantragte Zugang zu sämtlichen Textnachrichten zwischen der Kommissionspräsidentin Ursula von der Leyen und dem CEO des Pharmaunternehmens Pfizer im Zeitraum 2021 und 2022. Die Kommission teilte mit, sie könne dem Antrag nicht entsprechen, weil sie nicht im Besitz von Dokumenten sei, die mit der Beschreibung des Antrags übereinstimmten. Nach weiteren Anträgen der Journalistin erließ die Kommission im November 2022 die Entscheidung "C(2022) 8371 final". Darin hielt sie erneut fest, dass sie nicht im Besitz von Dokumenten sei, die dem Antrag entsprechen. Die Journalistin und The New York Times Company erhoben eine erfolgreiche **Nichtigkeitsklage** nach Art 263 AEUV an das EuG.

Das EuG hat erwogen: Erklärt ein Organ der Union im Rahmen eines Zugangsantrags, ein Dokument existiere nicht, gilt dieses Dokument aufgrund der **Vermutung der Richtigkeit** der Erklärung als nicht existent. Wird diese Vermutung entkräftet, kann sich die Kommission nicht mehr auf diese Vermutung berufen. Sie hat die Nichtexistenz oder den Nichtbesitz der angeforderten Dokumente durch plausible Erklärungen zu beweisen.

Die Klägerinnen haben **relevante Anhaltspunkte** vorgelegt, ua **Artikel und Interviews**. Diese beschreiben einen wiederholten mündlichen und schriftlichen Austausch, insb Textnachrichten, iZm dem Impfstoffkauf durch die Kommission während der COVID-19-Pandemie. Somit ist den Klägerinnen gelungen, die **Vermutung der Nichtexistenz** der angeforderten Dokumente zu **entkräften**.

Die Kommission hat sich auf den Hinweis beschränkt, dass sie trotz erneuter eingehender Nachforschungen kein entsprechendes Dokument habe identifizieren können, **jedoch ohne den Umfang oder die Einzelheiten dieser Nachforschungen zu präzisieren**. Sie hat nämlich weder angegeben, welche Arten von Nachforschungen durchgeführt, noch welche Dokumentenspeicherorte eingesehen wurden. Mangels genauer Erläuterungen dazu, wie die angeforderten Dokumente gesucht wurden, verstößt die Kommission gegen ihre **Pflicht, plausible Erklärungen für den Nichtbesitz von Dokumenten** zu geben.

Es ist unmöglich nachzuvollziehen, ob die angeforderten **Textnachrichten noch existieren** oder ob sie gelöscht wurden. Weiters bleibt auch offen, ob die **Mobiltelefone der Kommissionspräsidentin ersetzt** wurden und, wenn ja, was mit diesen Geräten geschehen ist – und ob sie Gegenstand der Nachforschungen waren, die infolge der Anträge durchgeführt wurden. Unter diesen Umständen können die Erläuterungen der Kommission, die auf Vermutungen beruhen, nicht als plausibel angesehen werden.

Das **Recht auf Zugang zu Dokumenten** verpflichtet das betreffende Organ, Dokumente, die sich in deren Besitz befinden, so **aufzubewahren**, dass der Zugang auch über einen längeren Zeitraum möglich bleibt. Die Organe dürfen dieses Recht **nicht dadurch aushöhlen**, dass sie Unterlagen zu ihren Tätigkeiten nicht **registrieren**. Die Kommission gibt nicht eindeutig an, ob die angeforderten Dokumente nicht registriert wurden, weil sie unwichtig waren und keiner Folgemaßnahmen seitens der Kommission oder einer ihrer Dienststellen bedurften. Weiters legt die Kommission auch nicht dar, weshalb die Textnachrichten nicht als **relevante**, dauerhaft aufzubewahrende Informationen eingestuft wurden.

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Die DSB ist nur berechtigt, die Behandlung einer Datenschutzbeschwerde als **exzessiv** abzulehnen, wenn sie das Vorliegen einer **Missbrauchsabsicht** des Beschwerdeführers nachweist. Eine Missbrauchsabsicht ist dann anzunehmen, wenn die entscheidenden Gründe des Beschwerdeführers für die Einbringung einer Vielzahl von Datenschutzbeschwerden nicht **in der Verfolgung der ihm aus der DSGVO zukommenden Rechte liegen** und der Beschwerdeführer ohne diese **sachfremden Gründe** die Vielzahl an Datenschutzbeschwerden nicht erhoben hätte ([VwGH 31.03.2025, Ra 2022/04/0143](#)).

### Rechtsprechung der Justiz

OLG Graz 19.03.2025, 4R52/25m

#### **Auskunft, Datenkopie, Bestimmtheit**

- Ein Spieler erstellte auf der Website eines estnischen **Online-Glücksspielunternehmens** ein **Spielerkonto**, auf welches er Beträge in Euro einzahlte. Nachdem sein Konto im Jahr 2023 gesperrt wurde, beantragte er die Freischaltung seines gesperrten Spielerkontos. Das Online-Glücksspielunternehmen kam dem nicht nach. Daraufhin übermittelte der Rechtsvertreter des Spielers ein Schreiben an das Online-Glücksspielunternehmen

und forderte dieses zur Übermittlung einiger Daten auf (etwa wie viel Geld der Spieler gewonnen oder verloren hat, mit welcher Gesellschaft das Vertragsverhältnis zustande gekommen ist, etc). Es konnte nicht festgestellt werden, ob das Schreiben dem Online-Glücksspielunternehmen tatsächlich zugegangen ist.

Da das Online-Glücksspielunternehmen dem Aufforderungsschreiben des Anwalts nicht nachkam, reichte der Spieler eine Klage gestützt auf Art 15 DSGVO ein und begehrte die digitale Übermittlung einer Kopie seiner Daten. Gegen das abweisende Urteil des Erstgerichts erhob der Spieler eine (erfolgreiche) Berufung an das OLG Graz.

Das OLG Graz hat erwogen: Die DSGVO schützt alle Arten von personenbezogenen Daten, wobei der **Begriff der personenbezogenen Daten** weit zu verstehen ist. Der Spieler gab bei der Erstellung seines Spielerkontos personenbezogene Daten wie seinen Namen, Geburtsdatum und Adresse ein. Der Spieler begehrte im Prozess keine Auskunft, sondern eine digitale Übermittlung seiner verarbeiteten Daten gemäß Art 15 Abs 3 DSGVO.

Es schadet nicht, dass der Spieler **zuvor bereits Zugriff** auf die Daten auf elektronischem Weg hatte. Da der Spieler zuvor lediglich ein Auskunftersuchen an das Online-Glücksspielunternehmen gerichtet hat, kann auch von **keinem exzessiven** Auskunftersuchen die Rede sein. Zudem hat das Online-Glücksspielunternehmen im Hinblick auf die Höchstpersönlichkeit des Auskunftsrechts **keine Zweifel an der Identität** des Spielers vorgebracht. Die Vorlage einer Vollmacht und eines Ausweises durch den Rechtsvertreter genügte zur Legitimation.

Der Spieler hat sein Begehren schlüssig aus Art 15 Abs 3 DSGVO abgeleitet. Das Klagebegehren ist **hinreichend bestimmt**, weil klar ist, dass der Spieler eine Kopie seiner von dem Online-Glücksspielunternehmen im Zusammenhang mit seinem Glücksspiel verarbeiteten Daten digital übermittelt haben will. Es ist ausreichend spezifiziert, dass es sich um den Datensatz des Spielers handelt und nicht um jenen irgendeines sonstigen Spielers. Das Online-Glücksspielunternehmen kann bei einer großen Datenmenge grundsätzlich eine Konkretisierung verlangen, dies ist hier aber nicht erforderlich. Daher war das erstinstanzliche Urteil aufzuheben. Das Online-Glücksspielunternehmen muss dem Spieler eine **Kopie der verarbeiteten Daten** digital übermitteln und die Kosten des Verfahrens ersetzen.

Aus der weiteren Rechtsprechung der Justiz:

- Ein auf Art 15 Abs 1 und 3 DSGVO gestütztes Auskunftersuchen dient auch dann einem **legitimen Zweck**, wenn es darauf

abzielt, **Beweismaterial** für eine **spätere Prozessführung** zu beschaffen. Ein Auskunftersuchen, das mit dem **Motiv** gestellt wird, einen späteren Prozess vorzubereiten, ist **nicht rechtsmissbräuchlich** ([OLG Wien 12.02.2025, 33R23/25g](#)).

- Stellt eine Person ein Auskunftersuchen, darf der Verantwortliche nur bei **begründeten Zweifeln** an der Identität der Person zusätzliche Informationen anfordern. Eine **rountinemäßige Identitätsprüfung** ist unzulässig. Äußert der Verantwortliche in seinem vorprozessualen Antwortschreiben keine hinreichend deutlichen Zweifel an der Identität der Person, wird die Klage vom Verantwortlichen veranlasst ([OLG Wien 20.02.2025, 4R191/24y](#)).

### **Rechtsprechung des BVwG**

[BVwG 27.03.2025, W298 2285480-1](#)

#### **Erleichterungsgebot, Geldbuße, VStG, Anwendungsvorrang**

- Ein Kunde stellte ein Lösungsersuchen an die in der Datenschutzerklärung eines Reisebüros angegebene E-Mail-Adresse. Da die Adresse inaktiv war, erreichte das Ersuchen das Unternehmen nicht, sodass darauf nicht reagiert wurde. Der Kunde erhob daraufhin Datenschutzbeschwerde bei der DSB. Die DSB forderte das Reisebüro mehrmals zur Stellungnahme auf, erhielt jedoch keine Antwort. Nach Einleitung eines Verwaltungsstrafverfahrens und der Einvernahme des Geschäftsführers löschte das Reisebüro die Daten des Kunden und teilte dies der DSB mit. Mangels Bekanntgabe des Reisebüros zu seinen Einkommens- und Vermögensverhältnissen schätzte die DSB anhand des jährlichen Bilanzgewinns den Umsatz und verhängte eine Geldstrafe iHv EUR 15.000. Gegen dieses Straferkenntnis erhob das Reisebüro Beschwerde an das BVwG. Das BVwG bestätigte das Straferkenntnis und schrieb dem Reisebüro einen zusätzlichen Kostenbeitrag iHv EUR 3.000 vor.

Das BVwG hat erwogen: Die Angabe einer nicht existenten oder inaktiven E-Mail-Adresse verhindert oder erschwert die Ausübung der Betroffenenrechte und verstößt gegen den **Erleichterungsgrundsatz** des Art 12 Abs 2 DSGVO. Die fehlende Reaktion auf das Lösungsbegehren verstößt gegen Art 12 Abs 3 iVm Art 17 DSGVO. Zudem hat das Reisebüro gegen die Mitwirkungspflicht gemäß Art 31 DSGVO verstoßen.

Die Bemessung der Geldbuße erfolgt ausschließlich nach den Kriterien des Art 83 Abs 1 bis 6 DSGVO. Im Anwendungsbereich der DSGVO bleibt daher kein Raum für die Anwendung nationaler Bestimmungen wie **§ 11 DSG (Verwarnung)** oder **§ 33a VStG (Beratung)**, die zusätzliche Tatbestandserfordernisse hinsichtlich des behördlichen

Ermessens normieren, wenn die DSB nach Art 58 DSGVO handelt. Das Verfahrensrecht der Mitgliedstaaten kommt nur insoweit zur Anwendung, als es nicht der Durchsetzung des Unionsrechts widerspricht.

Auch **Ermessensbeschränkungen** des § 5 VStG sind nicht anzuwenden. Das Verschulden des Verantwortlichen ist ausschließlich anhand der Bestimmungen des Art 83 Abs 1 und 2 DSGVO zu beurteilen. Die Strafbarkeit juristischer Personen und eingetragener Personengesellschaften richtet sich ausschließlich nach der Systematik des Art 4 Z 7 iVm Art 83 DSGVO und kann deren Haftung nicht auf zur Vertretung nach außen Berufene oder auf einen verantwortlichen Beauftragten einschränken. Auch betreffend § 19 VStG ist die **Bemessung der Geldbuße** ausschließlich anhand der von Art 83 Abs 1 bis 6 DSGVO normierten Kriterien durchzuführen. Die **Erschwernis- und Milderungsgründe** ergeben sich abschließend aus Art 83 Abs 2 DSGVO. Die § 20 VStG (außerordentliche Milderung der Strafe) und § 22 Abs 2 VStG (Kumulationsprinzip) bleiben daher im Anwendungsbereich des Art 83 Abs 3 DSGVO unangewendet.

Ein Unternehmen, das trotz mehrfacher Aufforderung nicht mit der DSB kooperiert, handelt **vorsätzlich**. Die Angabe einer inaktiven E-Mail-Adresse in der Datenschutzerklärung und die unterlassene Reaktion auf ein Lösungsersuchen begründen zumindest Fahrlässigkeit.

**Mildernd** ist zu berücksichtigen, dass die Daten im Laufe des Verfahrens nachträglich gelöscht wurden und eine erstmalige Verletzung der DSGVO vorliegt. Die fehlende Mitwirkung im Verwaltungs(straf)verfahren und der Umstand, dass die Datenschutzerklärung noch immer nicht geändert wurde, wirken sich **erschwerend** aus.

Die Erleichterung der Ausübung der Betroffenenrechte und die Kooperation mit der Aufsichtsbehörde sind ein Kernstück der datenschutzrechtlichen Pflichten nach der DSGVO. Ein solcher Verstoß ist daher nicht als geringfügig anzusehen. Um den **Unwertgehalt** der Tat zu verdeutlichen und eine zukünftige Kooperation mit Behörden und die Einhaltung datenschutzrechtlicher Pflichten sicherzustellen, scheint die Geldbuße erforderlich.

Auch **generalpräventive Gründe** sprechen für die Geldbuße, um zu verhindern, dass Verantwortliche durch verzögerte Mitwirkung die Ermittlungstätigkeit der Aufsichtsbehörde erschweren.

[BVwG 04.03.2025, W176 2285563-1](#)

#### **Arzt, Rolle, Gesundheitsdaten, Weiterverarbeitung**

- Eine Versicherte war in einen Verkehrsunfall verwickelt und litt nach eigener Angabe

seitdem an einem Tinnitus. Ihre Versicherung beauftragte daraufhin einen HNO-Facharzt mit der Erstellung eines Gutachtens. Bei einer persönlichen Untersuchung übergab die Versicherte dem Facharzt einige medizinische Befunde. Der Facharzt attestierte die Verletzungen als nicht unfallkausal (**Erstgutachten**). Die Haftpflichtversicherung des Unfallgegners erteilte dem Facharzt den Auftrag zur Erstellung eines weiteren Gutachtens. Der Facharzt griff dabei ua auf die ihm im Rahmen des Erstgutachtens übergebenen medizinischen Befunde der Versicherten zurück. Eine entsprechende Einwilligung der Versicherten lag nicht vor. Die gegnerische Haftpflichtversicherung legte das **Zweitgutachten** im Zivilprozess gegen die Versicherte vor.

Die DSB gab der Datenschutzbeschwerde der Versicherten statt. Sie stellte fest, dass der Facharzt gegen das Recht auf Geheimhaltung verstoßen habe, indem er Gesundheitsdaten der Versicherten, ohne deren Wissen und Einwilligung für das Zweitgutachten verarbeitet hatte. Der Facharzt erhob daraufhin (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Der **Facharzt** war iZm dem Zweitgutachten eigenständiger **Verantwortlicher iSd Art 4 Z 7 DSGVO**. Er erstellte das Zweitgutachten zwar im Auftrag der Haftpflichtversicherung, entschied jedoch selbst über Zwecke und Mittel der Verarbeitung.

Die medizinischen Befunde und das Erstgutachten sind **Gesundheitsdaten iSd Art 4 Z 15 DSGVO** und somit auch gemäß Art 9 Abs 1 DSGVO besonders geschützte Daten. Gemäß **Art 9 Abs 2 lit a DSGVO** ist die Verarbeitung von Gesundheitsdaten zulässig, wenn die Betroffene in die Verarbeitung ausdrücklich einwilligt. Die Versicherte hatte jedoch **keine Einwilligung** für die Verarbeitung ihrer Gesundheitsdaten für das Zweitgutachten erteilt.

Der Ausnahmetatbestand des **Art 9 Abs 2 lit f DSGVO** erlaubt die Verarbeitung von Gesundheitsdaten, wenn dies ua zur **Geltendmachung von Rechtsansprüchen** erforderlich ist. Die Verarbeitung muss jedoch mit den Grundsätzen des Art 5 DSGVO, darunter dem **Zweckbindungsgrundsatz**, vereinbar sein. Danach müssen die Zwecke der Verarbeitung bereits vor Beginn eindeutig feststehen. Die Gesundheitsdaten dürfen nur in einer mit dem Zweck, für den sie erhoben wurden, vereinbaren (kompatiblen) Weise verwendet werden. Durch die **Zweckänderung** – der Arzt verwendete die Gesundheitsdaten für das Zweitgutachten – war der Facharzt nicht mehr im Auftrag der Versicherung der Versicherten tätig, sondern für die Haftpflichtversicherung des Unfallgegners.

Der Facharzt hat somit für das Zweitgutachten die Gesundheitsdaten der Versicherten **unzulässig weiterverarbeitet**, weil der neue Verarbeitungszweck mit dem ursprünglichen nicht vereinbar war.

BVwG 05.09.2024, W211 2287218-1

### **Videoüberwachung, Personenbezug, Interessenabwägung, statistische Zwecke**

- Ein Unternehmen beauftragte eine Auftragsverarbeiterin mit der Errichtung eines **videobasierten Personenzählsystems**, um Besuchermengen zu ermitteln. Hierfür wurden 27 Videokameras im öffentlichen Raum einer Stadt montiert, wobei keine Kennzeichnung erfolgte. In Folge wurde die Personenzählung zu einer **Frequenzmessung** umgebaut. Die Kameras nahmen in **Echtzeit** auf und generierten digitales Bildmaterial, das an ein Computersystem eines externen Technologieunternehmens weitergeleitet und dort durch spezielle Software in Echtzeit analysiert und in Textdaten umgewandelt wurde. Die Bilddaten wurden dabei nach maximal **50 Millisekunden** im Arbeitsspeicher **gelöscht**, eine (weitere) Speicherung des Bildmaterials erfolgte nicht. Die **Livebilder** konnten von der Auftragsverarbeiterin und dem Technologieunternehmen betrachtet werden, der Zugriff war jedoch beschränkt, weil zunächst ein Port freigeschalten werden musste. Zudem wurden solche Zugriffe protokolliert. Die durch die Besucherstromanalyse bzw Frequenzanalyse gewonnenen Daten sollten der Planung, Organisation und Durchführung von Events und Marketingmaßnahmen dienen.

Nachdem die DSB ein **amtswegiges Prüfverfahren** durchführte, **untersagte** sie die Datenverarbeitung durch die Kameras mit sofortiger Wirkung. Daraufhin erhob das Unternehmen eine (erfolglose) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: **Personenbezogene Daten** liegen vor, wenn eine identifizierte oder identifizierbare natürliche Person betroffen ist. Auch wenn Betroffene erst nachträglich identifiziert werden können, kann es sich bei Bilddaten um personenbezogene Daten handeln. Für die **Identifizierbarkeit** muss nicht der Verantwortliche einen Personenbezug herstellen können, es reicht bereits aus, dass irgendeine dritte Person einen Bezug herstellen kann.

Die Daten wurden zweifelsfrei erhoben, erfasst und anschließend übermittelt, womit eine **Verarbeitung** iSd Art 4 Z 2 DSGVO vorliegt. Das Unternehmen ließ die Videokameras zu Zwecken der Personenzählung errichten und betrieb diese anschließend zu Zwecken der Frequenzzählung weiter. Damit ist das Unternehmen **Verantwortliche** iSd Art 4 Z 7 DSGVO.

Das Unternehmen hat ausgeführt, dass sie ein **berechtigtes Interesse** an der Erfassung und Auswertung habe. **Marketinginteressen** können grundsätzlich ein berechtigtes Interesse iSd Art 6 Abs 1 lit f DSGVO sein. Die Verarbeitung muss jedoch erforderlich sein, auf das notwendigste beschränkt sein und die Grundrechte und Grundfreiheiten der Betroffenen dürfen nicht überwiegen. Die 27 Videokameras erfassten 24 Stunden täglich alle Zu- und Abgänge zu drei zentralen Orten. Dies führte zu einer **lückenlosen Dokumentation** aller Passanten ohne Unterscheidung von Personengruppen (etwa Kinder, Touristen, Anwohner oder Zufallsanwesende). Zudem wurden die Kameras **nicht gekennzeichnet**. Damit handelt es sich jedenfalls um eine **exzessive und unverhältnismäßige Datenverarbeitung**. Dem Unternehmen standen **weniger eingriffsintensive Alternativen** zur Verfügung, wie zB analoge Zählsysteme oder Laserscanner. Passanten dürfen erwarten, dass sie in öffentlich zugänglichen Bereichen nicht dauerhaft überwacht werden, insb wenn diese Bereiche der Erholung und Freizeit dienen. Das **Geheimhaltungsinteresse** der Betroffenen **überwiegt** damit das Marketinginteresse des Unternehmens.

Die Privilegierung nach § 7 DSG dient ua der Ermittlung und Verarbeitung von personenbezogenen Daten für **statistische Zwecke**. Diese Privilegierung umfasst jedoch nur die Verarbeitung **pseudonymisierter Daten**. Da es dem Verantwortlichen möglich war, durch Betrachtung der Livebilder vor der Umwandlung in eine Textdatei allfällige Identifizierungen durchzuführen, greift die Privilegierung des § 7 DSG nicht.

#### Aus der weiteren Rechtsprechung des BVwG:

- Die Feststellung einer Verletzung im Recht auf Geheimhaltung setzt die Verarbeitung personenbezogener Daten des Betroffenen voraus. Kann nicht festgestellt werden, dass an der in Rede stehenden Örtlichkeit eine zur Aufzeichnung personenbezogener Bilddaten geeignete **Videokamera** betrieben wird, kann keine Verletzung im Recht auf Geheimhaltung festgestellt werden. Das **Amtswegigkeitsprinzip** wird im Verfahren vor der DSB durch § 24 Abs 2 DSG eingeschränkt. Den Beschwerdeführer trifft eine **Mitwirkungspflicht** ([BVwG 06.03.2025, W292 2284288-2](#)).
- Eine Verletzung des Rechts auf Geheimhaltung kann nur vorliegen, wenn tatsächlich Daten des Betroffenen verarbeitet wurden. Zum **Nachweis der Betroffenheit** trifft den Betroffenen eine **Mitwirkungspflicht** ([BVwG 05.03.2025, W211 2272384-1](#)).
- Das Erkenntnis des BVwG kann in **gekürzter Form ausgefertigt** werden, wenn von den Parteien auf die Revision beim VfGH und die

Beschwerde beim VfGH verzichtet oder nicht innerhalb von zwei Wochen nach Zustellung der Niederschrift eine Ausfertigung des Erkenntnisses beantragt wird ([BVwG 03.10.2024, W137 2261950-1 ua](#)).

- Der **Missbrauch** bzw die **exzessive Ausübung** des Rechts auf Erheben einer Datenschutzbeschwerde besteht nicht in der schieren Anzahl der eingebrachten Datenschutzbeschwerden, sondern liegt darin, dass die Datenschutzbeschwerde sich nicht auf Rechte bezieht, die die DSGVO dem Betroffenen verleiht ([BVwG 10.03.2025, W137 2280882-2](#)).

#### Europäische Kommission

##### [Leitlinien zum Schutz Minderjähriger im Internet nach dem Gesetz über digitale Dienste](#)

#### **Schutz Minderjähriger, Online-Plattformen**

- Die **Kommission** hat am **13.05.2025** die von ihr erarbeiteten Leitlinien zum **Schutz von Minderjährigen im Internet** zur öffentlichen Konsultation veröffentlicht. Bis zum **10.06.2025** können Interessenträger, einschließlich Kinder, Eltern und Erziehungsberechtigte, nationale Behörden, Anbieter von Online-Plattformen und Sachverständige Rückmeldungen einbringen. Die Veröffentlichung der Leitlinien wird für den Sommer 2025 erwartet. Gemäß **Art 28 Digital Services Act** ("Online-Schutz Minderjähriger") haben **Online-Plattformen**, die für Minderjährige zugänglich sind, geeignete und verhältnismäßige Maßnahmen zu ergreifen, um für ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen innerhalb ihres Dienstes zu sorgen. Konkret zu ergreifende Maßnahmen schreibt der DSA nicht vor, allerdings ermöglicht es Art 28 Abs 4 DSA der Kommission, Leitlinien zu veröffentlichen, die die Anbieter von Online-Plattformen "*bei der Umsetzung der Maßnahmen unterstützen*."

Die nun veröffentlichten Guidelines greifen den **risikobasierten Ansatz** auf, der dem DSA zugrunde liegt. Sie berücksichtigen überdies, dass verschiedene Plattformen unterschiedliche Risikoniveaus für Minderjährige aufweisen. Es sollen angemessene Schutzmaßnahmen erreicht werden, die sich anhand der Gefährdung durch den jeweiligen Dienst bestimmen, ohne dabei die Rechte von Kindern auf Teilhabe, Information und Meinungsfreiheit übermäßig einzuschränken.

Folgende Schutzmaßnahmen werden empfohlen: (i) **Altersverifikationsmaßnahmen** umsetzen, um das Risiko zu verringern, dass Kinder mit pornografischen oder anderweitig altersunangemessenen Inhalten in Kontakt kommen; (ii) **Accounts von Kindern/Jugendlichen** standardmäßig auf "**privat**" **setzen**, um das Risiko

unerwünschter Kontakte durch Fremde zu senken; (iii) **Empfehlungssysteme** anpassen und dabei eindeutige Signale von Nutzern – etwa, ob ihnen Inhalte gefallen oder nicht – priorisieren, um zu verhindern, dass Minderjährige in sog "**Rabbit Holes**" mit schädlichen Inhalten geraten; (vi) Möglichkeiten für Minderjährige vorsehen, andere Nutzer zu **blockieren** oder **stummzuschalten**; und sicherstellen, dass sie nicht ohne ihre ausdrückliche Zustimmung zu Gruppen hinzugefügt werden können.



to the point

# Datenschutzmonitor. 21/2025 vom 28.05.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Leitlinien veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH 22.05.2025, C-213/23, *Kommission/Niederlande*; C-215/23, *Kommission/Belgien*; C-237/23, *Kommission/Bulgarien*; C-238/23, *Kommission/Lettland* (PSI-II-RL, Vertragsverletzungsverfahren)

- **Rechtsprechung der Justiz**

OGH 24.04.2025, 10Ob5/25w; 10Ob18/25g (Smart Meter, einstweilige Verfügung)

- **Rechtsprechung des BVwG**

BVwG 24.03.2025, W101 2269148-1 (Datenschutzbeauftragte, Aussageverweigerungsrecht, Rechtsirrtum)

BVwG 01.04.2025, W252 2297124-1 (Anwendungsbereich, Paketzustellung, Rollenverteilung)

BVwG 10.02.2025, W287 2265979-1 (Online-Handel, Zustellbenachrichtigung, Rollenverteilung)

BVwG 28.03.2025, W287 2301192-1; 31.03.2025, W137 2289435-1 (Zurückziehung der Bescheidbeschwerde)

- **Rechtsprechung der LVwG**

LVwG Innsbruck 14.05.2025, LVwG-2024/27/1150-1 (Amtssignatur, Bescheid, Verifizierung)

LVwG Wien 13.01.2025, VGW-101/042/17553/2024 (Liegenschaftsadresse, Interessenabwägung)

- **Rechtsprechung der DSB**

DSB 13.01.2022, 2021-0.450.072 (Berufsemailkonto, Löschung, Datenübertragung, Informationspflicht, Einschränkung)

## To the Point:

### Rechtsprechung des EuGH

Aus der Rechtsprechung des EuGH:

- Der **EuGH** hat die **Niederlande, Belgien, Bulgarien** und **Lettland** wegen der nicht fristgerechten Umsetzung der "RL (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors" (**PSI-II-RL**) verurteilt. Die **Niederlande** haben an die Kommission einen Betrag iHv **EUR 10 Mio** zu entrichten. **Belgien** wurde eine Geldzahlung iHv **EUR 2,1 Mio** auferlegt. **Bulgarien** wurde die Zahlung von **EUR 900.000** vorgeschrieben und **Lettland** hat **EUR 250.000** zu bezahlen ([EuGH 22.05.2025, C-213/23, Kommission/Niederlande](#); [C-215/23, Kommission/Belgien](#); [C-237/23, Kommission/Bulgarien](#); [C-238/23, Kommission/Lettland](#)).

### Rechtsprechung der Justiz

OGH 24.04.2025, 10Ob5/25w; 10Ob18/25g

#### **Smart Meter, einstweilige Verfügung**

- Eine Netzbetreiberin wollte **eichfällige Zähler** gegen intelligente Messgeräte ("**Smart Meter**") austauschen und auf Wunsch der Netzbenutzer entsprechend § 1 Abs 6 IME-VO konfigurieren ("Opt-Out-Konfiguration"). Dennoch lehnten die Netzbenutzer den Austausch unter Verweis auf die Gefahr von "Elektrosmog" und datenschutzrechtlichen Bedenken ab. Die Netzbetreiberin drohte an, den Strom abzuschalten, wogegen die Netzbenutzer Anträge auf einstweilige Verfügungen stellten.

Der OGH hat erwogen: Die **Weigerung eines Netzbenutzers**, der Netzbetreiberin Zugang zu seinem Objekt (Wohnung) zu gewähren, damit die Netzbetreiberin einen (grundsätzlich funktionsfähigen) Stromzähler austauschen kann, ist qualitativ den Fällen des Zahlungsverzugs und der Verweigerung einer Vorauszahlung oder Sicherheitsleistung nicht gleichzuhalten. Diese Weigerung des Netzbenutzers rechtfertigt daher die Androhung der Stromabschaltung nicht. Weigert sich der Netzbenutzer jedoch, Zutritt zum Objekt zu gewähren, um einen der Eichpflicht unterliegenden **eichfälligen Zähler** auszutauschen, könnte das als Verletzung "wesentlicher anderer Pflichten" aus dem Netzzugangsvertrag zu werten sein. Ein solcher Verstoß ist hier aber deshalb nicht zu prüfen, weil der Netzbenutzer nur den Austausch des eichfälligen Stromzählers auf eine bestimmte andere Zählerart, nämlich auf einen **Smart Meter**, verweigert.

Nach § 1 IME-VO besteht **keine Verpflichtung** zum Einbau eines intelligenten

Messgeräts bei diesem konkreten Netzbenutzer. Die Netzbetreiberin ist laut dieser Bestimmung zwar verpflichtet, bis Ende 2024 mindestens 95% der an ihrem Netz angeschlossenen Zählerpunkte als intelligente Messgeräte auszugestalten. Da laut dem eigenen Vorbringen der Netzbetreiberin bereits 99,97% ihrer Strommessgeräte Smart Meter sind, ist sie dieser Zielverpflichtung bereits nachgekommen und ist ihr der Einbau eines Smart Meters beim konkreten Netzbenutzer somit gesetzlich nicht vorgeschrieben.

Zur Abwehr der Androhung der Stromabschaltung steht dem Netzbenutzer eine **einstweilige Verfügung** gegen den Netzbetreiber zu. Dem Netzbetreiber steht es aber offen, selbst gerichtliche Hilfe bei der Durchsetzung seines Interesses auf Tausch des Stromzählers in Anspruch zu nehmen.

### Rechtsprechung des BVwG

BVwG 24.03.2025, W101 2269148-1

#### **Datenschutzbeauftragte, Aussageverweigerungsrecht, Rechtsirrtum**

- Im Zuge eines datenschutzrechtlichen **Verwaltungsstrafverfahrens** gegen eine GmbH sowie gegen deren Geschäftsführerin vor der DSB wurde die **Datenschutzbeauftragte** als Zeugin einvernommen. Aufgrund dieser Einvernahme weitete die DSB das Verwaltungsstrafverfahren auf weitere aus ihrer Sicht infrage kommende Verwaltungsübertretungen nach der DSGVO aus. In der darauffolgenden ergänzenden Zeugeneinvernahme berief sich die bereits zuvor einvernommene Datenschutzbeauftragte auf die **Aussageverweigerungsgründe** nach § 5 Abs 2 DSG sowie auf das **Selbstbeziehungsverbot**. Daraufhin verhängte die DSB eine **Ordnungsstrafe**, weil sie nicht davon ausging, dass die Aussageverweigerungsgründe einschlägig seien. Die Bestimmung des § 5 Abs 2 DSG gelte laut den Erläuterungen zur Bestimmung nicht gegenüber der DSB und beziehe sich darüber hinaus lediglich auf personenbezogene Daten, über die die Datenschutzbeauftragte im Rahmen ihrer Tätigkeit als solche Kenntnis erlangt habe. Die Bescheidbeschwerde der Datenschutzbeauftragten an das BVwG war erfolgreich.

Das BVwG hat erwogen: Für Fälle der ungerichtfertigten Aussageverweigerung kann gemäß § 49 Abs 5 AVG eine **Ordnungsstrafe** über einen **Zeugen** verhängt werden. Zwar hat die DSB die Bestimmung des **§ 5 Abs 2 DSG**, wonach dieser Aussageverweigerungsgrund nicht gegenüber der DSB gilt, rechtskonform angewendet. Die Kann-Bestimmung des § 49 Abs 5 AVG zur Verhängung einer Ordnungsstrafe wendete die DSB hingegen zu Unrecht an. Die Bestimmung des § 5 Abs 2 DSG kann nämlich von einer **nicht rechtskundigen Person** durchaus in

einer solchen Weise bzw Lesart interpretiert werden, die eine darauf begründete Aussageverweigerung auch gegenüber der DSB rechtfertigt. Die Umstände, wonach eine Berufung auf § 5 Abs 2 DSG gegenüber der DSB nicht möglich ist, können nämlich nur in den Erläuterungen zur Bestimmung nachgelesen werden. Einer nicht rechtskundigen Person kann nicht zugemutet werden, sich neben der Sichtung einer Gesetzesbestimmung noch zusätzlich mit den Materialien vertraut machen zu müssen. Die Datenschutzbefugte ist einem **nicht vorwerfbaren Rechtsirrtum** über die Interpretation des § 5 Abs 2 DSG unterlegen, der eine Verhängung einer Ordnungsstrafe nicht rechtfertigt.

BVwG 01.04.2025, W252 2297124-1

#### **Anwendungsbereich, Paketzustellung, Rollenverteilung**

- Eine Braut bestellte bei einem Unternehmen Hochzeitseinladungen, die personenbezogene Daten ihres künftigen Ehemannes enthielten, darunter ua Name, Telefonnummer und Ort der Hochzeitsfeier. Ein beauftragtes Versandunternehmen übergab das Paket einem Frächter zur Zustellung. Der Frächter stellte das Paket jedoch ohne Abstellgenehmigung vor der Wohnung des Brautpaares ab. Diese fanden das Paket aufgerissen und geleert vor.

Die DSB gab der Datenschutzbeschwerde des Bräutigams gegen das Versandunternehmen statt. Sie stellte fest, dass das Versandunternehmen den Bräutigam durch das Abstellen des Pakets ohne entsprechende Genehmigung in seinem Recht auf Geheimhaltung verletzt habe. Dadurch seien personenbezogene Daten des Bräutigams Dritten offengelegt worden. Es habe durch die **unzureichende Zustellung** nicht für eine geeignete Sicherheit der Verarbeitung gesorgt und damit auch den Grundsatz der Integrität und Vertraulichkeit verletzt. Das Versandunternehmen erhob daraufhin (erfolgreich) Beschwerde an das BVwG.

Das BVwG hat erwogen: Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten. Sie gilt auch für eine **nichtautomatisierte Verarbeitung**, wenn die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Die DSGVO unterscheidet weder hinsichtlich der Intensität oder Dauer der jeweiligen Verarbeitung noch wird iZm der für die Verarbeitung eingesetzten Technik eine Differenzierung vorgenommen. Die **Datenverarbeitung umfasst den gesamten Vorgang**, dh vom Zeitpunkt der Online-Bestellung von Hochzeitseinladungen durch die Braut, der Eingabe der persönlichen Daten des Bräutigams, der Produktion der Hochzeitseinladungen, bis zum Versand.

Gemäß Art 4 Z 7 DSGVO ist "**Verantwortlicher**" derjenige, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Das Versandunternehmen hatte weder auf den Zweck noch auf die Mittel der Verarbeitung Einfluss. Erstellung und Druck der Hochzeitseinladungen erfolgen gänzlich außerhalb dessen Sphäre. Ein allfälliges **Eigeninteresse** des Versandunternehmens bzw eine Verarbeitung in dessen Namen bezieht sich ausschließlich auf die **Versanddaten** des Pakets, aber **nicht auf dessen Inhalt**. Folglich wird dadurch ebenfalls keine Verantwortlichkeit begründet.

Eine **Datenschutzbeschwerde ist abzuweisen**, wenn sie sich unzweifelhaft gegen eine Person oder Stelle richtet, die **nicht Verantwortlicher** der betreffenden Datenverarbeitung ist.

BVwG 10.02.2025, W287 2265979-1

#### **Online-Handel, Zustellbenachrichtigung, Rollenverteilung**

- Ein international tätiger Versanddienstleister übernahm die Zustellung eines Pakets, das eine Kundin bei einem Online-Händler bestellt hatte. Der Händler beauftragte die Übermittlung eines **Terminavisos** (elektronische Zustellbenachrichtigung) an eine bestimmte E-Mail-Adresse. Dabei kam es zur irrtümlichen Verwendung der E-Mail-Adresse eines Mitbewohners der Kundin. Dieser erhielt daraufhin Informationen über die bevorstehende Zustellung des Pakets und konnte Verfügungen darüber treffen. Die Kundin erachtete sich dadurch in ihrem Recht auf Geheimhaltung verletzt. Die DSB gab der Datenschutzbeschwerde statt und stellte fest, dass eine Verarbeitung **fehlerhafter Daten** weder vertraglich noch durch ein berechtigtes Interesse gedeckt sei. Dagegen erhob der Versanddienstleister erfolgreiche Beschwerde an das BVwG.

Das BVwG hat erwogen: Als "**Auftragsverarbeiter**" wird jemand angesehen, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (**Art 4 Z 8 DSGVO**). Der Auftragsverarbeiter darf die Daten nicht anders als nach den Anweisungen des Verantwortlichen verarbeiten.

Der Händler hat den Auftrag zum Versand des Pakets sowie zur Versendung eines Terminavisos an die Kundin erteilt und die Mittel selbst bestimmt. Eine maßgebliche eigenverantwortliche Entscheidungsgewalt des Versanddienstleisters ist somit nicht hervorgekommen. Dieser hat somit weder über den Zweck noch über die Mittel der Datenverarbeitung entschieden und kann für sie daher nicht Verantwortlicher iSd Art 4 Z 7 DSGVO sein. Der Versanddienstleister agierte nur als Auftragsverarbeiter des Händlers. Dem Versanddienstleister kann als bloßer

Auftragsverarbeiter **nicht die Fehlerhaftigkeit** der im Auftrag der Versenderin verarbeiteten Daten **zugerechnet werden**.

Aus der weiteren Rechtsprechung des BVwG:

- Die **Zurückziehung einer Bescheidbeschwerde** führt zum Erlöschen der Entscheidungspflicht und damit aus der Sicht des Beschwerdeführers, der die Bescheidbeschwerde zurückgezogen hat, zum Verlust des Erledigungsanspruchs. Geht der Erledigungsanspruch verloren, ist das Verfahren mit **Beschluss einzustellen** ([BVwG 28.03.2025, W287 2301192-1](#); [31.03.2025, W137 2289435-1](#)).

### Rechtsprechung der LVwG

Aus der Rechtsprechung der LVwG:

- Unter [www.signaturpruefung.gv.at](http://www.signaturpruefung.gv.at) steht ein durch die Rundfunk und Telekom Regulierungs-GmbH (**RTR-GmbH**) betriebenes **zentrales Prüfservice für amtssignierte elektronische Dokumente** zur Verfügung. Unter **Verifizierung** iSd § 20 E-GovG ist die Bestätigung zu verstehen, dass die als Ausdruck vorliegende Erledigung einer Behörde von dieser stammt. Ein zu prüfender **Bescheid** muss für die Verifizierung zur Gänze vorliegen, wobei ein Abbild (Scan, Kopie) ausreicht. Somit kann nur ein digital vorliegender amtssignierter Bescheid unmittelbar online verifiziert werden. Ausdrücke (somit in Papierform vorliegende Schriftstücke) von amtssignierten elektronischen Dokumenten können nicht direkt online verifiziert werden, sie können jedoch zur Prüfung übermittelt werden ([LVwG Innsbruck 14.05.2025, LVwG-2024/27/1150-1](#)).
- Da aus der **Liegenschaftsadresse** auf die Identität und Wohnadresse des Grundstückseigentümers geschlossen werden kann, ist die Bekanntgabe der Liegenschaftsadresse ein personenbezogenes Datum. Die Betroffenen haben ein **Geheimhaltungsinteresse** an ihren von einem Abbruchantrag betroffenen Grundstücksadressen. Dem antragstellenden Gemeinderatsabgeordneten und Landtagsabgeordneten kommen jedoch aufgrund seiner Stellung umfassende Kontrollbefugnisse und Kontrollpflichten zu, weshalb die **Interessenabwägung** zu seinen Gunsten ausfällt. Die **Baupolizei (MA 37)** hat die Adressen der Liegenschaften bekanntzugeben, für die Ansuchen auf Abbruch von Bauwerken wegen wirtschaftlicher Abbruchreife eingebracht worden sind ([LVwG Wien 13.01.2025, VGW-101/042/17553/2024](#)).

### Rechtsprechung der DSB

DSB 13.01.2022, 2021-0.450.072

#### **Berufsemail, Löschung, Datenübertragung, Informationspflicht, Einschränkung**

- Ein ehemaliger Mitarbeiter eines Transportunternehmens nutzte während seiner Anstellung eine rein zu **beruflichen Zwecken eingerichtete E-Mail-Adresse**. Nach seinem Ausscheiden gingen auf diese E-Mail-Adresse weiterhin E-Mails ein, darunter Rechnungen und geschäftliche Korrespondenz. Das Unternehmen nahm nur Einsicht in die beruflichen E-Mails und leitete diese weiter. Einen Monat nach der Deaktivierung des E-Mail-Accounts wurde dieser vollständig gelöscht. Der ehemalige Mitarbeiter verlangte die Übermittlung sämtlicher auf dem E-Mail-Account gespeicherten personenbezogenen Daten, einschließlich privater und beruflicher Korrespondenz sowie deren Löschung oder Einschränkung der Verarbeitung. Das Transportunternehmen kam diesem Ersuchen teilweise nach, indem es eine datenschutzrechtliche Auskunft erteilte und die privaten E-Mails löschte. Daraufhin erhob der ehemalige Mitarbeiter (erfolglos) Datenschutzbeschwerde an die DSB.

Die DSB hat erwogen: Der Anwendungsbereich des **Grundrechts auf Datenschutz** ist eröffnet, weil es sich um personenbezogene Daten des ehemaligen Mitarbeiters handelt, an deren Geheimhaltung dieser ein schutzwürdiges Interesse hat. Das Geheimhaltungsrecht gilt jedoch nicht absolut. Eine Verarbeitung personenbezogener Daten ist zulässig, wenn **überwiegende berechtigte Interessen** eines anderen vorliegen.

Das Transportunternehmen verarbeitet die Daten auf Grundlage berechtigter Interessen gemäß Art 6 Abs 1 lit f DSGVO. Da die E-Mail-Adresse aufgrund einer **dienstlichen Anweisung** ausschließlich für **berufliche Zwecke** genutzt werden durfte, konnte das Transportunternehmen davon ausgehen, dass neu eingehende E-Mails geschäftlich sind. Selbst bei Unkenntnis des ehemaligen Mitarbeiters über die dienstliche Anweisung besteht ein berechtigtes Interesse des Transportunternehmens, den **ungestörten Geschäftsablauf** sicherzustellen – etwa durch die Einsicht in bzw die Weiterleitung von Rechnungsdaten und beruflichen E-Mails. Den berechtigten Interessen des Transportunternehmens war daher ein höherer Stellenwert einzuräumen als den berechtigten Interessen des ehemaligen Mitarbeiters. Der Eingriff in das Recht auf Geheimhaltung war daher gerechtfertigt.

Der Anspruch auf **Datenübertragbarkeit** bezieht sich nur auf Daten, die dem Verantwortlichen von der betroffenen Person bereitgestellt wurden. Chat-Verläufe und empfangene E-Mails, die neben Äußerungen des

Betroffenen auch solche anderer Personen enthält, fallen daher nicht unter den Anspruch des Art 20 DSGVO. Darüber hinaus dürfen bei der Ausübung des Rechts auf Datenübertragbarkeit die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden. Da der ehemalige Mitarbeiter nun für ein **Konkurrenzunternehmen** arbeitet und sich in dem E-Mail-Account berufliche E-Mails mit diversen Geschäftskontakten und Rechnungsdaten befinden, würde die Datenübertragung die **Rechte und Freiheiten des Transportunternehmens** und **seiner Geschäftskunden** beeinträchtigen. Auch private E-Mails könnten Informationen über Dritte enthalten und deren Interessen beeinträchtigen.

Das Transportunternehmen erteilte dem ehemaligen Mitarbeiter bereits vor Erhebung der Datenschutzbeschwerde eine datenschutzrechtliche Auskunft, womit sämtliche **Metainformationen**, die nach Art 13 und 14 DSGVO zur Verfügung zu stellen sind, bereits im Rahmen der Erfüllung des Auskunftsrechts nach Art 15 Abs 1 DSGVO übermittelt wurden. Die Informationspflicht entfällt gemäß Art 13 Abs 4 bzw Art 14 Abs 5 lit a DSGVO, wenn der Betroffene über die entsprechenden Informationen verfügt. Eine Informationspflicht über Datenübermittlungen in Drittländer besteht nur, wenn eine solche tatsächlich beabsichtigt wird.

Das **Recht auf Löschung** besteht nicht, wenn gesetzliche Aufbewahrungspflichten entgegenstehen. Darüber hinaus ist die Speicherung der beruflichen E-Mails zur **Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen** erforderlich, weil zwischen dem Transportunternehmen und dem neuen Arbeitgeber des ehemaligen Mitarbeiters bereits Rechtsstreitigkeiten anhängig sind. Zudem steht eine weitere Klagsführung des Transportunternehmens gegen den ehemaligen Mitarbeiter unmittelbar vor der gerichtlichen Einbringung.

Das **Recht auf Einschränkung** der Datenverarbeitung setzt eine objektiv rechtswidrige Verarbeitung voraus. Die Verarbeitung der Daten durch das Transportunternehmen war jedoch rechtmäßig, sodass kein Anspruch auf Einschränkung der Datenverarbeitung besteht.

to the point

# Datenschutzmonitor. 22/2025 vom 04.06.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Leitlinien veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 27.05.2025, 39056/22, *Selishcheva/Russland* (politische Meinung, Rückwirkungsverbot)

- **Rechtsprechung des VwGH**

VwGH 09.05.2025, Ra 2022/16/0118 (Beschweadressat, Gültigkeit)

- **Rechtsprechung des BVwG**

BVwG 31.03.2025, W287 2246105-1 (Verantwortlicher, Betriebsrat, Betriebsratsfonds, Wahlvorstand, Fürsorgepflicht, Internal Investigations)

BVwG 28.03.2025, W292 2301229-1 (automatisierte Entscheidung, Bonitätsscore, Zahlungserfahrungsdaten, Speicherfrist)

BVwG 07.04.2025, W256 2245984-1 (Apotheke, berechtigtes wirtschaftliches Interesse, gelindere Mittel)

BVwG 31.03.2025, W137 2256492-1 (Verantwortlicher, Auftragsverarbeiter)

BVwG 31.03.2025, W137 2254660-1 (Nachbarschaft, berechtigtes Interesse, allgemein verfügbare Daten)

BVwG 27.03.2025, W274 2290131-1; 28.03.2025, W274 2294608-1 (Exzess, Rechtsmissbrauch)

BVwG 31.03.2025, W258 2134678-1 (Verhandlungsprotokoll, Datenweitergabe innerhalb der Organisationsstruktur)

BVwG 31.03.2025, W258 2245052-1 (OGH, Personalakt, Geheimhaltung)

BVwG 27.03.2025, W254 2297150-1 (E-Mail, Personenbezug, Auskunft)

BVwG 02.04.2025, W291 2307872-1 (Datenschutzbeschwerde, Feststellungsbegehren)

BVwG 21.03.2025, W292 2307654-1 (Kohärenzverfahren, Säumnisbeschwerde)

BVwG 17.03.2025, W292 2281684-1 (Säumnisbeschwerde, Klaglosstellung)

- **EU-Rechtsakte**

Omnibus IV-Paket (DSGVO, Digitalisierung)

## To the Point:

### Rechtsprechung des EGMR

EGMR 27.05.2025, 39056/22, Selishcheva/Russland

#### **Politische Meinung, Rückwirkungsverbot**

- In Russland wurde ein Gesetz beschlossen, das Personen, die an Aktivitäten von als extremistisch eingestuften Vereinigungen beteiligt waren, von der Kandidatur bei allen Wahlen ausschließt. Mehreren Kandidaten wurde deshalb die Registrierung bei Kommunalwahlen verwehrt. Die Datenerhebung beruhte auf allgemeinen polizeilichen Befugnissen. Ein klarer Rechtsrahmen für die Überwachung politischer Aktivitäten fehlte. Die betroffenen Personen hatten weder die Möglichkeit zu erfahren, welche Daten über sie gesammelt wurden, noch auf welcher Grundlage dies geschah. Zudem fehlten Regelungen zur Speicherdauer, zur Löschung der Daten, etc. Da keine Kriterien für die Datenerhebung definiert wurden, war die Datenerhebung intransparent und konnte willkürlich erfolgen. Auch konnte die Datenerhebung nicht wirksam angefochten werden. Die Kandidaten erhoben erfolgreiche Beschwerden an den EGMR.

Der EGMR hat erwogen: Bereits die bloße Speicherung von Informationen über das Privatleben einer Person – einschließlich Daten zu **politischen Meinungen** und der **Teilnahme an friedlichen Protesten** – ist ein Eingriff in das Recht auf Achtung des Privatlebens (Art 8 Abs 1 EMRK).

Daten über politische Meinungen und Aktivitäten sind **besondere Kategorien personenbezogener Daten**. Dies wiegt besonders schwer, weil die beobachteten Aktivitäten bei der legitimen Ausübung der Rechte auf Meinungs- und Versammlungsfreiheit nach Art 10 und 11 EMRK erfolgt sind. Zudem gab es keine Hinweise auf gewalttätiges Verhalten, das eine intensive Überwachung hätte rechtfertigen können. Eine **breit angelegte Datenerhebung** kann abschreckend wirken und Menschen davon abhalten, ihre Rechte auf Meinungs- und Versammlungsfreiheit wahrzunehmen. Da der Eingriff weder gesetzlich vorgesehen war noch ein legitimes Ziel verfolgte oder in einer demokratischen Gesellschaft notwendig war, ist Art 8 EMRK verletzt worden.

Die **Verweigerung der Wahlzulassung** wegen angeblicher Beteiligung an extremistischen Organisationen verletzt zudem die Rechte auf Meinungs- und Versammlungsfreiheit gemäß Art 10 und 11 EMRK. Sanktioniert wurden Aktivitäten, die vor dem Verbot der Organisationen und vor Inkrafttreten der einschlägigen Gesetzesänderung stattfanden. Die Betroffenen konnten nicht vorhersehen, dass ihre damaligen legalen Aktivitäten später zu einem Wahlverbot führen

würden. Darüber hinaus ist die gesetzliche Regelung unbestimmt, weil der Begriff "Beteiligung" an extremistischen Organisationen **zu weit gefasst** ist. Der Begriff wird in Russland so ausgelegt, dass nahezu jede Form der Unterstützung oder Sympathiebekundung ausreicht, um eine Wahlteilnahme zu verhindern. Dies hat eine abschreckende Wirkung auf die politische Betätigung und gefährdet den politischen Pluralismus.

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Für die **Gültigkeit** eines Bescheids ist die Nennung eines Adressaten erforderlich. Dieses Erfordernis ist erfüllt, wenn bei schriftlichen Ausfertigungen aus **Spruch, Begründung** und **Zustellverfügung** eindeutig erkennbar ist, gegenüber welchem individuellem Rechtsträger die Behörde einen Bescheid erlassen wollte. Ist der **Bescheidadressat** unklar, liegt **kein Bescheid** vor. Weist das Adressfeld nur den Platzhalter "Empfänger\_Anschrift" auf, genügt es nicht, dass von der zuständigen Sachbearbeiterin Vor- und Familienname sowie E-Mail-Adresse für den Zustellvorgang und das Setzen der Zustellverfügung im EDV-System verwendet werden ([VwGH 09.05.2025, Ra 2022/16/0118](#)).

### Rechtsprechung des BVwG

BVwG 31.03.2025, W287 2246105-1

#### **Verantwortlicher, Betriebsrat, Betriebsratsfonds, Wahlvorstand, Fürsorgepflicht, Internal Investigations**

- Die stellvertretende Vorsitzende eines Angestelltenbetriebsrats stand unter Verdacht, Skontobeträge, die aus von ihr abgewickelten Apothekenbestellungen für Mitarbeiter resultierten, auf ihrem privaten Konto einbehalten zu haben. Aufgrund dessen kamen der Vorsitzende des Zentralbetriebsrats sowie ein Mitglied der Geschäftsleitung in die Büroräumlichkeiten des Angestelltenbetriebsrats und nahmen Unterlagen betreffend die getätigten Apothekenbestellungen an sich. Weitere Dokumente wurden vom Betriebsratsfonds und vom Wahlvorstand an die Geschäftsleitung übermittelt. Der Angestelltenbetriebsrat übermittelte keine Unterlagen.

Die stellvertretende Vorsitzende brachte bei der DSB eine Datenschutzbeschwerde gegen den Angestelltenbetriebsrat ein, weil sie sich durch die Weitergabe der Unterlagen an den Arbeitgeber in ihrem Recht auf Geheimhaltung verletzt sah. Die DSB wies die Datenschutzbeschwerde wegen fehlender Passivlegitimation ab. Denn die Datenschutzbeschwerde wäre richtigerweise gegen den Betriebsratsfonds als Verantwortlichen zu

erheben gewesen. Auch eine entsprechende Datenschutzbeschwerde gegen den Betriebsratsfonds wäre jedoch abzuweisen gewesen, weil sowohl dem Arbeitgeber als auch dem Betriebsratsfonds gemäß § 1 Abs 2 DSG ein das Geheimhaltungsinteresse der stellvertretenden Vorsitzenden überwiegendes berechtigtes Interesse an der Aufklärung des Sachverhalts zukam. Dagegen erhob die stellvertretende Vorsitzende eine erfolglose Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Gemäß Art 4 Z 7 DSGVO ist "**Verantwortlicher**" derjenige, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der **Betriebsrat** sowie der **Betriebsratsfonds** sind jeweils eigenständige Verantwortliche. Dasselbe gilt aufgrund der dem Betriebsrat vergleichbaren Stellung als weisungsfreies Kollegialorgan auch für den **Wahlvorstand**.

Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Einwilligung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung zur Wahrung **überwiegender berechtigter Interessen** eines anderen zulässig (§ 1 Abs 2 DSG). Die **Verhütung und Aufklärung von Betrug oder sonstigem Fehlverhalten** sind berechnete Interessen. Hinsichtlich der mitgenommenen Unterlagen überwogen die Interessen des Arbeitgebers, die gegenüber der stellvertretenden Vorsitzenden erhobenen **Vorwürfe aufzuklären** sowie in einem mit der stellvertretenden Vorsitzenden geführten **zivilgerichtlichen Verfahren** Beweise vorlegen zu können.

Den Arbeitgeber trifft eine allgemeine **Fürsorgepflicht** gegenüber seinen Arbeitnehmern. Diese Fürsorgepflicht ist eine echte **Rechtspflicht** und keine bloß ethisch gebotene freiwillige Rücksichtnahme. Der Arbeitgeber ist verpflichtet, seine Arbeitnehmer gegen Verfehlungen anderer Arbeitnehmer zu schützen. Aus dieser Schutzpflicht folgt eine Notwendigkeit der Durchführung interner Untersuchungen ("**Internal Investigations**") im Unternehmen.

BVwG 28.03.2025, W292 2301229-1

### **Automatisierte Entscheidung, Bonitäts-score, Zahlungserfahrungsdaten, Speicherfrist**

- Eine Kreditauskunftei verarbeitete bonitätsrelevante Daten eines Kreditwerbers, ua Informationen über die Erledigung eines **außergerichtlichen Ausgleichs** samt Forderungsverzicht sowie den "**Scorewert 0: Keine Berechnung möglich**". Der Scorewert wurde nicht berechnet, weil mit der von der Kreditauskunftei verwendeten Berechnungsmethode aus den Informationen über den außergerichtlichen Ausgleich kein

Scorewert abgeleitet werden konnte. Diese Informationen gab die Kreditauskunftei an ein Kreditinstitut weiter, das die Anfrage des Kreditwerbers nach einem Konsumkredit mit der Begründung ablehnte, dass die Kreditauskunftei keinen Scorewert berechnen könne, wofür technische Probleme bei der Kreditauskunftei ausschlaggebend seien.

Der Kreditwerber erhob Datenschutzbeschwerde an die DSB gegen die Kreditauskunftei, weil diese sich weigerte, die entsprechenden Daten des Kreditwerbers zu löschen. Die DSB gab dieser Datenschutzbeschwerde statt, wogegen die Kreditauskunftei eine teilweise erfolgreiche Bescheidbeschwerde an das BVwG erhob.

Das BVwG hat erwogen: Für die Ausübung des **Gewerbes der Kreditauskunfteien** gemäß § 152 GewO kann die Verarbeitung (bonitätsrelevanter) personenbezogener Daten ohne Einwilligung nur auf den Erlaubnistatbestand des **berechtigten Interesses** nach Art 6 Abs 1 lit f DSGVO gestützt werden. Informationen zu einem **Schuldenregulierungsverfahren**, die bereits öffentlich in einer staatlichen Insolvenzdatenbank einsehbar waren, sind ab dem Zeitpunkt, ab dem das jeweilige nationale Insolvenzrecht die öffentliche Publikation der betreffenden Informationen nicht mehr als erforderlich erachtet, von privaten Kreditauskunfteien ebenfalls nicht weiter zu verarbeiten.

Hinsichtlich Informationen, die zu keinem Zeitpunkt in einer staatlich geführten Insolvenzdatenbank öffentlich zugänglich waren, ist hingegen in einer **einzelfallbezogenen Interessensabwägung** zu beurteilen, wie lange eine Speicherung in der **privaten Bonitätsdatenbank** einer Kreditauskunftei zulässig ist.

Bei der Aufnahme von **Verbraucherkrediten** ist der Kreditgeber zur eingehenden Prüfung der Kreditwürdigkeit des Verbrauchers verpflichtet, erforderlichenfalls auch anhand von **Auskünften** aus öffentlichen und privaten Datenbanken. Gemäß der [KapitaladäquanzVO \(EU\) 575/2013](#) sind Unternehmen der kreditgebenden Wirtschaft verpflichtet, die Bonität potenzieller Kreditnehmer auch anhand historischer **Zahlungserfahrungsdaten** über einen **Beobachtungszeitraum von fünf Jahren** einzuschätzen.

Die **Kreditwürdigkeitsprüfung** schützt nicht nur den Verbraucher, sondern das **reikreditlose Funktionieren des gesamten Kreditystems**. Die Verarbeitung bonitätsrelevanter Daten aus öffentlichen und privaten Datenbanken ist sohin zur Wahrung der wirtschaftlichen Interessen der Kreditauskunftei sowie der kreditgebenden Wirtschaft zulässig. Da die Kreditauskunftei nur solchen Unternehmen Zugang zum außergerichtlichen Ausgleich gewährte, die der kreditgebenden Wirtschaft angehörten, durften die entsprechenden Informationen von der



Kreditauskunftei für fünf Jahre aufbewahrt werden. Der Bescheid der DSB war daher dahingehend abzuändern, dass die Datenschutzbeschwerde des Kreditwerbers hinsichtlich der Zahlungserfahrungsdaten abgewiesen wird.

Ein "**Bonitätsscore**", der maßgeblich für die Verweigerung eines Vertragsabschlusses mit einem Kreditinstitut ist, ist eine automatisierte Entscheidung, die gegenüber dem Kreditwerber "*rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt*" (Art 22 Abs 1 DSGVO). Daran ändert es auch nichts, wenn kein Scorewert berechnet werden konnte, weil die Kreditauskunftei die Information, "*0 - Berechnung nicht möglich*" an das Kreditinstitut weitergegeben hat. Der Umstand, dass die **Letztentscheidung** über die Gewährung des Verbraucherkredits innerhalb der Entscheidungsstruktur des Kreditinstituts – und damit nicht innerhalb der Kreditauskunftei – liegt, steht der rechtlichen Qualifikation der Information als eine automatisierte Entscheidung nicht entgegen. Aus dem Ablehnungsschreiben des Kreditinstituts folgt nämlich klar, dass der übermittelte "Scorewert" für die ablehnende Entscheidung des Kreditinstituts **maßgeblich** war.

Die **Ausnahmetatbestände** des Art 22 Abs 2 DSGVO gelangen nicht zur Anwendung, denn § 152 GewO ist keine Rechtsvorschrift iSd Art 22 Abs 2 lit b DSGVO. Die Verarbeitung der Information "XXXX - Scorewert 0: Keine Berechnung möglich" war somit rechtswidrig. Diese Information ist daher zu löschen. **Anm: Die Information über das Nichtberechnen eines Scores ist somit eine "Entscheidung".**

BVwG 07.04.2025, W256 2245984-1

### **Apotheke, berechtigtes wirtschaftliches Interesse, gelindere Mittel**

- Eine Ärztin für Allgemeinmedizin betrieb eine Ordination in einem Gebäude, in dem sich ein weiterer Allgemeinmediziner sowie eine Apotheke befanden. Die Vermieterin vermietete Räumlichkeiten an alle genannten Beteiligten. Nach der Pensionierung des weiteren Allgemeinmediziners kam es zu einem Gespräch zwischen Vertretern der Apotheke und der Vermieterin, in dem diese davon überzeugt werden sollte, die freiwerdende Ordination an eine Kassenärztin für Allgemeinmedizin zu vermieten und nicht an eine Wahlärztin für Psychiatrie. Die Vertreter der Apotheke gaben die (auf Tausender gerundete) Anzahl der von der Ärztin ausgestellten und bei der Apotheke eingelösten Rezepte bekannt und argumentierten, dass eine weitere Kassenärztin für die Umsätze der Apotheke besser wäre.

Die Ärztin erachtete sich in ihrem Recht auf Geheimhaltung verletzt und brachte eine

Datenschutzbeschwerde ein. Die DSB stellte eine Verletzung des Rechts auf Geheimhaltung fest. Die Apotheke erhob Bescheidbeschwerde an das BVwG, das ihr stattgab.

Das BVwG hat erwogen: Die **Apotheke** hat ein **berechtigtes wirtschaftliches Interesse** daran, der Vermieterin im Zusammenhang mit der Nachbesetzung der Ordination die Anzahl der bei ihr eingelösten Rezepte zu nennen. Die wirtschaftliche Existenz der Apotheke hängt maßgeblich von der Patientenfrequenz der im Haus tätigen Ärzte ab. Die Weitergabe der auf Tausender gerundeten Rezeptzahlen an die Vermieterin lässt **keine konkreten Rückschlüsse** auf die wirtschaftliche Leistungsfähigkeit der Ärztin, auf Details zu Behandlungsdaten, zur Art oder Dauer der Behandlungen oder zur genauen Patientenzahl zu. Geschlossen werden kann nur auf die (ungefähre) Höhe der von der Ärztin ausgestellten und bei der Apotheke eingelösten Rezepte sowie auf die (ungefähre) Anzahl der entsprechenden Patienten.

Die Datenweitergabe erfolgte im geschäftlichen Kontext und ist in solchen Situationen üblich und verhältnismäßig. Das Interesse der Ärztin an der Geheimhaltung der Rezeptzahlen ist vergleichsweise als gering anzusehen. Die von der DSB geforderte abstrakte Darstellung ohne Zahlen hätte die wirtschaftliche Abhängigkeit der Apotheke nicht in gleicher Weise verdeutlicht und wäre kein **gelinderes**, zum Ziel führendes **Mittel** gewesen.

BVwG 31.03.2025, W137 2256492-1

### **Verantwortlicher, Auftragsverarbeiter**

- Eine Schulungseinrichtung leitete die private E-Mail-Adresse eines Seminarteilnehmers ohne seine Einwilligung an Dritte weiter. Der Seminarteilnehmer fühlte sich durch die Übermittlung in seinem Recht auf Geheimhaltung verletzt und brachte Datenschutzbeschwerde bei der DSB ein. Die Schulungseinrichtung argumentierte, sie sei als Auftragsverarbeiterin tätig geworden. Die Verarbeitung sei gemäß Art 6 Abs 1 lit b DSGVO zur Vertragserfüllung sowie auf Grundlage berechtigter Interessen erfolgt. Die E-Mail-Adresse sei ausschließlich zur Übermittlung der Zugangsdaten zum Kurs verarbeitet worden. Die DSB wies die Datenschutzbeschwerde mangels Verantwortlicheneigenschaft der Schulungseinrichtung ab. Der Seminarteilnehmer erhob daraufhin (erfolgreich) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Eine natürliche oder juristische Person, die **allein** oder **gemeinsam** mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, gilt gemäß Art 4 Z 7 DSGVO als **Verantwortlicher**. Der Verantwortliche ist Adressat von **Pflichten** aus der

DSGVO, von **Ansprüchen** der betroffenen Personen und **Ansprechstelle** für Maßnahmen der Aufsichtsbehörde.

Mit dem **Zweck** der Datenverarbeitung wird definiert, **warum** eine Datenverarbeitung stattfindet. Die **Mittel** der Verarbeitung betreffen die **Art und Weise**, wie das Ziel erreicht wird. Davon ist auch die Entscheidung umfasst, an wen Daten übermittelt oder wann sie gelöscht werden. Wesentlich für die Abgrenzung zwischen Auftragsverarbeiter und Verantwortlichem ist der **tatsächliche Einfluss** auf die Entscheidung über Zweck und Mittel. Dabei ist der Begriff des Verantwortlichen **weit zu verstehen**.

Der **Verantwortliche entscheidet** immer über den **Zweck** der Verarbeitung. Bei der Festlegung der **Mittel** hat ein **Auftragsverarbeiter** einen gewissen **Handlungsspielraum**. Mittel, die in engem Zusammenhang mit Zweck und Umfang einer Verarbeitung stehen, zB die Festlegung der Kategorien von **Betroffenen**, der **Datenarten**, der **Speicherdauer** und der Kategorien von **Empfängern**, werden vom **Verantwortlichen** bestimmt.

Ausschlaggebend ist, wer **tatsächlich** über die Daten **entscheidet**. **Auftragsverarbeiter** können zum **Verantwortlichen werden**, wenn sie, ohne legitimiert zu sein, über Zwecke und Mittel einer Verarbeitung selbst entscheiden. Da die Schulungseinrichtung die Verarbeitung im Rahmen der vorgegebenen Zwecke und Mittel vornahm, ist sie als Auftragsverarbeiterin zu qualifizieren.

BVwG 31.03.2025, W137 2254660-1

### **Nachbarschaft, berechtigtes Interesse, allgemein verfügbare Daten**

- Ein Grundstücksbewohner und sein Nachbar befanden sich aufgrund des Baus einer Einfriedungsmauer an deren Grundstücksgrenze in einem **Nachbarschaftskonflikt**. Der Grundstücksbewohner fertigte Bild- und Videoaufnahmen ua von der Liegenschaft, Teilen des Wohnhauses sowie einer Kamerakonstruktion des Nachbarn an. Diese Aufnahmen übermittelte er iZm einer früheren Datenschutzbeschwerde als Beweismittel an die DSB sowie in "cc" an die Bezirkshauptmannschaft (**BH**). Zudem sendete er Aufnahmen der benachbarten Liegenschaft an ein Bauunternehmen, welches der Nachbar zur Errichtung der Einfriedungsmauer beauftragt hatte. Aus den E-Mails ging ua der Name des Nachbarn hervor. Der Grundstücksbewohner wollte mit den Aufnahmen Beweise zu baulichen Auswirkungen der Einfriedungsmauer auf sein Grundstück sichern. Dadurch erachtete sich der Nachbar in seinem Recht auf Geheimhaltung verletzt.

Die DSB gab der entsprechenden Datenschutzbeschwerde des Nachbarn teilweise statt. Der Grundstücksbewohner habe

bereits vor der Datenübermittlung Auskunft darüber erhalten, dass die BH hierfür nicht die zuständige Behörde sei. Weiters liege auch kein berechtigtes Interesse vor, die Aufnahmen an das Bauunternehmen zu senden. Die Bescheidbeschwerde des Grundstücksbewohners blieb erfolglos.

Das BVwG hat erwogen: Der Grundstücksbewohner übermittelte seine (frühere) Datenschutzbeschwerde auch an die BH, obwohl er wusste, dass diese nicht zuständig ist. Somit scheidet die Rechtmäßigkeit der Datenübermittlung an die BH sowohl an der Wahrnehmung eines **berechtigten Interesses** als auch an der **Erforderlichkeit** der Übermittlung.

Die Bestimmung des § 1 Abs 1 S 2 DSG schließt die Verletzung eines schutzwürdigen Geheimhaltungsinteresses der Betroffenen bei "**allgemein verfügbaren Daten**" ausdrücklich aus. Obwohl die personenbezogenen Daten des Nachbarn bereits teilweise öffentlich zugänglich waren, bleibt **das Datenschutzregime** jedoch **anwendbar**. Dies gilt auch für personenbezogene Daten, die öffentlich nicht zugänglich, aber einer Person – wie dem Bauunternehmen – möglicherweise bekannt waren.

Gemäß Art 6 Abs 1 lit f DSGVO ist die Verarbeitung personenbezogener Daten in "**Gleichordnungsverhältnissen**" unter Privaten, wenn sie zur Wahrung **berechtigter Interessen** erforderlich ist, zulässig. Grundsätzlich ist der Zweck der Beweissicherung iZm allfälligen Gefahren durch die Einfriedungsmauer gegeben. Zum Zeitpunkt der Übermittlung an das Bauunternehmen lagen die betreffenden Aufnahmen jedoch bereits den zuständigen (Bau-)Behörden vor. Weiters konnte der Grundstücksbewohner nicht darlegen, warum die Aufnahmen, die das Wohnhaus des Nachbarn zeigen, für die Beweissicherung erforderlich sind.

BVwG 27.03.2025, W274 2290131-1; 28.03.2025, W274 2294608-1

### **Exzess, Rechtsmissbrauch**

- Der Insasse einer Justizanstalt erhob zwei Datenschutzbeschwerden bei der DSB und behauptete, durch mehrere Verantwortliche in seinem Recht auf Geheimhaltung verletzt worden zu sein. Die Verantwortlichen hätten etwa Einschreiben vom Insassen nicht vertragsgemäß behandelt und nicht zugestellt. Zudem sollen unbefugte Dritte Inhalte und Daten des Insassen unrechtmäßig geöffnet und entnommen haben. In der zweiten Datenschutzbeschwerde behauptete er, dass andere Verantwortliche wiederum seine Gesundheitsdaten unrechtmäßig verarbeitet und manipuliert sowie persönliche Daten an Dritte weitergegeben hätten.

Die DSB lehnte die Behandlung beider Datenschutzbeschwerden gemäß Art 57 Abs 4

DSGVO ab. Die DSB begründete dies damit, dass der Insasse iZm seiner Verurteilung und Inhaftierung bereits 44 Datenschutzbeschwerden erhoben habe und zudem unterschiedlichste Verfahren bei Kammern, Gerichten, Behörden, Staatsanwaltschaften, etc angestrengt habe. In den bereits beendeten Verfahren wurde von den Gerichten stets festgehalten, dass die vom Insassen behaupteten Verstöße nicht nachvollzogen werden könnten. Bei den Datenschutzbeschwerden würde es sich um wiederholende Eingaben handeln, die einen erheblichen Aufwand für die DSB mit sich brächten. Zudem würde der Insasse mit haltlosen Behauptungen dem datenschutzrechtlichen Verfahren **fremde Zwecke** verfolgen. Vor diesem Hintergrund sei die Datenschutzbeschwerde **rechtsmissbräuchlich**. Die Bescheidbeschwerden des Insassen an das BVwG blieben erfolglos.

Das BVwG hat erwogen: Bei **offenkundig unbegründeten** oder **exzessiven** Anfragen darf die DSB eine Gebühr verlangen oder sich weigern, tätig zu werden (Art 57 Abs 4 DSGVO). Die Aufsichtsbehörde trägt die **Beweislast** für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage. Der EuGH legt Art 57 Abs 4 DSGVO dahingehend aus, dass Anfragen nicht allein aufgrund ihrer Zahl als exzessiv eingestuft werden können. Die Aufsichtsbehörde muss das Vorliegen einer **Missbrauchsabsicht** der anfragenden Person nachweisen. Eine Missbrauchsabsicht liegt vor, wenn Beschwerden eingereicht werden, ohne dass dies objektiv erforderlich ist, um die Rechte aus der DSGVO zu schützen.

Die **Zahl der Datenschutzbeschwerden** allein reicht nicht aus, um eine Missbrauchsabsicht festzustellen. Die DSB muss alle relevanten Umstände jedes Einzelfalls berücksichtigen. Eine übermäßige Inanspruchnahme der Behörde durch zahlreiche Datenschutzbeschwerden kann ein **Indiz für exzessive Anfragen** sein, wenn die Datenschutzbeschwerden nicht objektiv durch Erwägungen gerechtfertigt sind, die sich auf den Schutz der Rechte beziehen.

Der Insasse behauptete zahlreiche Rechtsverletzungen, die zwar individuelle Elemente enthielten, jedoch legte er nicht offen, woraus er den unrechtmäßigen Umgang, die Fälschungen oder Manipulationen ableitete. In einer **Gesamtwürdigung aller Umstände** ist die Annahme einer **Missbrauchsabsicht** begründet. Der Insasse gab nicht konkret an, welche Datenschutzverletzungen er welchen Verantwortlichen vorwirft. Die behaupteten Datenschutzverstöße sind als bloße Mutmaßungen zu qualifizieren. Die DSB durfte die Behandlung der Datenschutzbeschwerden daher wegen **Exzessivität** iSd Art 57 Abs 4 DSGVO ablehnen.

BVwG 31.03.2025, W258 2134678-1

### **Verhandlungsprotokoll, Datenweitergabe innerhalb der Organisationsstruktur**

- Eine Patientin führte gegen eine Krankenanstalt wegen datenschutzrechtlichen Verstößen mehrere Verfahren vor der DSB und dem BVwG, weil Mitarbeiter der Krankenanstalt unbefugt auf ihre Gesundheitsdaten zugegriffen haben sollen. Die Krankenanstalt leitete die Korrespondenzen und Verfahrensinhalte zur weiteren Bearbeitung an den Verwaltungsdirektor weiter, welcher diese wiederum an seine Sekretärin und den Datenschutzbeauftragten weiterleitete. Zudem leitete der Verwaltungsdirektor das **Verhandlungsprotokoll** einer öffentlichen Verhandlung an die dort befragten Zeugen weiter, damit sie ihre Zeugenaussagen prüfen konnten.

Die Patientin erachtete sich in ihrem Recht auf Geheimhaltung verletzt und brachte eine Datenschutzbeschwerde bei der DSB ein. Darin brachte sie vor, dass der Verwaltungsdirektor ausschließlich für die Wirtschaftsführung zuständig sei und keine datenschutzrechtlichen Verwaltungs- oder Gerichtsverfahren bearbeiten oder führen dürfe. Sie beantragte die Feststellung einer Rechtsverletzung und weitere Maßnahmen, wie die Untersagung der Datenverwendung und Sanktionen. Nachdem die DSB die Datenschutzbeschwerde abwies, richtete die Patientin eine erfolglose Bescheidbeschwerde an das BVwG. In weiterer Folge brachte die Patientin eine Revision an den VwGH ein. Der VwGH hob das Erkenntnis des BVwG auf, weil die Patientin Tatsachenfragen aufgeworfen hatte, die einer Erörterung in einer mündlichen Verhandlung bedürft hätten. Daran anschließend fand eine mündliche Verhandlung vor dem BVwG statt und der Bescheidbeschwerde der Patientin im **zweiten Rechtsgang** wurde teilweise Folge gegeben.

Das BVwG hat erwogen: Nach Feststellung des VwGH ist die **Rechtslage zum Zeitpunkt** der jeweiligen Vorgänge maßgeblich. Es ist daher die Rechtslage vor Inkrafttreten der DSGVO anzuwenden. Für die verfahrensgenständlichen Vorgänge galt somit das DSG 2000.

Die Krankenanstalt ist als **juristische Person** auf natürliche Personen zur Wahrnehmung ihrer Aufgaben angewiesen. Sie bestimmt, wen sie für die Erfüllung ihrer Aufgaben bezieht, sofern keine gesetzlichen oder organisationsrechtlichen Einschränkungen bestehen. Die Aufgaben und Kompetenzen des **Verwaltungsdirektors** waren ua im Tiroler Krankenanstaltengesetz (**Tir KAG**), sowie in der **Anstaltsordnung** des Krankenhauses geregelt. Der Verwaltungsdirektor war gemäß § 16 Tir KAG für die wirtschaftlichen, administrativen, technischen

und personellen Angelegenheiten der Krankenanstalt verantwortlich. Als Teil der Anstaltsleistung war der Verwaltungsdirektor damit betraut, Beschwerden zu überprüfen, Maßnahmen zur Abstellung von Unzukömmlichkeiten einzuleiten und für die Einhaltung gesetzlicher Bestimmungen zu sorgen.

Die Bearbeitung datenschutzrechtlicher Verwaltungs- und Gerichtsverfahren fiel somit in den **Aufgabenbereich** des Verwaltungsdirektors. Die Einbindung der **Sekretärin** zur administrativen Unterstützung und des **Datenschutzbeauftragten** zur fachlichen Beratung war zulässig und erforderlich. Auch die Befassung der in den Verfahren involvierten **Ärzte** war unbedenklich, weil es für eine ordnungsgemäße Verfahrensführung notwendig ist, die betroffenen Ärzte über die gegen sie erhobenen Vorwürfe zu informieren und **anzuhören**.

Durch die Weiterleitung des **vollständigen Protokolls** an die Zeugen wurde jedoch eine Rechtsverletzung verwirklicht, weil dies über das erforderliche Maß hinausging und gegen den **Grundsatz der Datenminimierung** iSd § 6 Abs 1 Z 3 DSGVO verstieß. Die Weitergabe hätte sich auf die jeweils relevanten Teile beschränken müssen, ohne die Aussage aller Zeugen und das Vorbringen der Patientin zu enthalten.

#### Aus der weiteren Rechtsprechung des BVwG:

- Die Führung von **Personalakten** der **Richter des OGH** ist der **Justizverwaltung** zuzuordnen, die von der **Präsidentin des OGH** erledigt wird. Personalakten unterliegen grundsätzlich der **Auskunftspflicht** nach dem AuskunftspflichtG. In den Personalakten sind etwaige absolvierte Schulungen der Richter auch enthalten. Die Richter des OGH haben jedoch ein datenschutzrechtliches **Geheimhaltungsinteresse** an Informationen über ihre Ausbildung. Die Geheimhaltung der Inhalte von Personalakten hat in der Rechtsordnung einen **besonders hohen Stellenwert**. Das Interesse des Auskunftswerbers, Informationen über die Ausbildung der OGH-Richter zu erhalten, um diese in einem EGMR-Verfahren vorlegen zu können, überwiegt nicht ([BVwG 31.03.2025, W258 2245052-1](#)).
- Eine E-Mail-Adresse ist ein **personenbezogenes Datum**. Für die Ausübung des Auskunftsrechts müssen **keine Voraussetzungen** erfüllt sein. Eine Ausnahme von der Verpflichtung zur Auskunftserteilung betreffend Informationen, über die der Betroffene verfügt, sieht Art 15 DSGVO nicht vor ([BVwG 27.03.2025, W254 2297150-1](#)).
- In einer **Datenschutzbeschwerde** ist die Feststellung einer konkreten Rechtsverletzung zu begehren. Enthält eine Datenschutzbeschwerde kein **Feststellungsbegehren**,

ist sie von der DSB zurückzuweisen. Die dagegen gerichtete Bescheidbeschwerde ist vom BVwG abzuweisen ([BVwG 02.04.2025, W291 2307872-1](#)).

- Die DSB hat über Datenschutzbeschwerden grundsätzlich innerhalb von **sechs Monaten** zu entscheiden. Die Zeit während eines **Kohärenzverfahrens** wird in diese **Entscheidungsfrist** jedoch nicht eingerechnet. Bei einer "**grenzüberschreitenden Verarbeitung**" ist eine **Säumnisbeschwerde** daher vor Abschluss des Kohärenzverfahrens mangels Säumnis der DSB zurückzuweisen. Daran ändert es auch nichts, wenn das Kohärenzverfahren noch gar nicht eingeleitet wurde, weil der DSB zur Einleitung des Kohärenzverfahrens **kein Ermessen** zukommt. Das Kohärenzverfahren wird daher schon bei Vorliegen der gesetzlichen Voraussetzungen und somit beim Einbringen der Datenschutzbeschwerde automatisch in Gang gesetzt ([BVwG 21.03.2025, W292 2307654-1](#)).
- In einem **Säumnisbeschwerdeverfahren** kann das BVwG der DSB auftragen, den **versäumten Bescheid** unter Zugrundelegung der vom BVwG festgelegten Rechtsanschauung innerhalb von acht Wochen **nachzuholen**. Weicht die DSB im daraufhin erlassenen Bescheid von den Vorgaben des BVwG ab, hat das BVwG in der Sache zu entscheiden. Entspricht im **Laufe eines solchen Verfahrens** der Verantwortliche dem Auskunftsersuchen iSd § 24 Abs 6 DSGVO, kann das Verfahren daher nicht mit Beschluss in Folge Klaglosstellung eingestellt werden, sondern die Datenschutzbeschwerde ist abzuweisen ([BVwG 17.03.2025, W292 2281684-1](#)).

#### EU-Rechtsakte

##### Omnibus IV Simplification Package

##### **DSGVO, Digitalisierung**

- Die Europäische Kommission möchte mit dem sog **Omnibus-Paket** die Bürokratie für Unternehmen abbauen. Am **21.05.2025** wurde das Omnibus IV Paket veröffentlicht. In diesem Paket enthalten sind ua (i) "*Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures*", [COM\(2025\) 501 final](#); (ii) "*Proposal for a Directive of the European Parliament and of the Council amending Directives 2014/65/EU and (EU) 2022/2557 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further*

simplifying measures", [COM\(2025\) 502 final](#); (iii) "Proposal for a Directive of the European Parliament and of the Council amending Directives 2000/14/EC, 2011/65/EU, 2013/53/EU, 2014/29/EU, 2014/30/EU, 2014/31/EU, 2014/32/EU, 2014/33/EU, 2014/34/EU, 2014/35/EU, 2014/53/EU, 2014/68/EU and 2014/90/EU of the European Parliament and of the Council as regards digitalisation and common specifications", [COM\(2025\) 503 final](#); und (iv) "Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) No 765/2008, (EU) 2016/424, (EU) 2016/425, (EU) 2016/426, (EU) 2023/1230, (EU) 2023/1542 and (EU) 2024/1781 as regards digitalisation and common specifications", [COM\(2025\) 504 final](#).

Mit den **ersten beiden Gesetzesentwürfen** führt die Kommission den neuen Begriff der "**small mid-cap enterprises**" in die dort genannten Rechtsakte ein, der auch größere Unternehmen als der bisherige Begriff der KMUs erfassen soll. Ebenso wie KMUs soll diese neue Unternehmenskategorie von den Bürokratieabbaumaßnahmen des Omnibus IV profitieren. Der Bürokratieabbau betrifft neben der **DSGVO** ua auch die **MIFID** und die **CER**-Richtlinien, mit welchen die Märkte für Finanzinstrumente reguliert und die Resilienz kritischer Einrichtungen gestärkt wird. Mit den **weiteren zwei Gesetzesentwürfen** sollen eine Reihe von näher bezeichneten Richtlinien und Verordnungen durch die Einführung elektronischer Formate modernisiert und der **Digitalisierung** angepasst werden.

In die **DSGVO** sollen neue Legaldefinitionen bzw Verweise auf Legaldefinitionen zu KMUs und "**small mid-cap enterprises**" eingefügt werden. Zudem soll die Pflicht ein **Verarbeitungsverzeichnis** zu führen, auch für Unternehmen und Organisationen mit weniger als 750 Mitarbeitern entfallen, sofern mit der Verarbeitungstätigkeit voraussichtlich kein hohes Risiko iSd Art 35 DSGVO verwirklicht wird.

to the point

# Datenschutzmonitor. 23/2025 vom 11.06.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Leitlinien veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 03.06.2025, 9389/19, *Uygun/Türkei* (Recht auf Korrespondenz, Haft)

- **Rechtsprechung des EuGH**

EuGH 05.06.2025, C-541/24, *Naltov* (Akteneinsicht, Unzuständigkeit)

EuGH SA 05.06.2025, C-769/22, *Kommission/Ungarn* (Strafregisterdaten)

### NACHTRAG

EuGH SA 15.05.2025, C-209/23, *RRC Sports* (FIFA, FFAR, berechnete Interessen)

- **Rechtsprechung des VwGH**

VwGH 27.03.2025, Ro 2022/04/0023 (Mitarbeiter, Rollenverteilung, Übergangsbestimmung, Beschwerdegegner)

VwGH 30.04.2025, Ro 2021/04/0005 (Übergangsbestimmung, Lösungsersuchen, Informationspflicht)

VwGH 30.04.2025, Ro 2021/04/0024 (Videoüberwachung, Geldbuße, Kumulationsprinzip)

VwGH 15.04.2025, Ra 2021/04/0094 (Anwaltsgeheimnis, Auskunft)

VwGH 15.04.2025, Ro 2021/04/0012 (ASFINAG, Mautprellerei)

VwGH 06.05.2025, Ra 2024/07/0121 (Forderungskauf, keine Winkelschreiberei)

VwGH 24.04.2025, Ra 2023/15/0105 (Arbeitnehmerveranlagung, Werbungskosten)

- **Rechtsprechung des OGH**

OGH 30.04.2025, 5Ob35/25w (Smart Meter, Stromabschaltung)

OLG Linz 13.05.2025, 4R64/25x (Beweismittel, Rechtsstaat)

OLG Linz 14.05.2025, 3R58/25g (Erleichterungsgrundsatz, Identifizierung)

- **Rechtsprechung des BVwG**

BVwG 27.01.2025, W605 2248297-1 (Grundbuch, informationeller Mehrwert, konkrete Empfänger, Dateninhalt, Akteneinsicht)

BVwG 03.04.2025, W176 2259543-1 (Adressverlag, Kreditauskunftei, Bonitätsbewertung)

BVwG 21.05.2024, W605 2232133-1 (justizielle Tätigkeit, Gerichtsvollzieher)

BVwG 21.05.2024, W605 2287853-1 (objektive Präklusivfrist)

BVwG 04.03.2024, W605 2274353-1 (BVwG, Anonymisierung, Kostenersatz)

BVwG 20.02.2024, W605 2286285-1 (Einbringung, BVwG)

BVwG 23.05.2024, W298 2261880-1 (COVID, Impfreister, Patientenindex)

BVwG 14.04.2025, W137 2297606-1 (Säumnis, Schadenersatz, Privatbeteiligung)

BVwG 21.05.2024, W605 2286028-1 (Ermittlungspflicht)

BVwG 21.05.2024, W605 2278491-1 (Kohärenzverfahren, Aussetzung)

BVwG 09.07.2024, W258 2272449-1 (Beschwerdegegner)

- **Rechtsprechung der DSB**

DSB 07.10.2024, 2024-0.671.673 (Data Breach, Mitwirkung, Doppelbestrafung)

- **Leitlinien EDSA**

Guidelines 02/2024 on Article 48 GDPR<sup>2</sup>

## To the Point:

### Rechtsprechung des EGMR

- Die Weigerung einer Gefängnisbehörde, die Briefe eines Häftlings zu versenden, ist ein Eingriff in das **Recht auf Korrespondenz** gemäß Art 8 EMRK. Grundsätzlich kann es zulässig sein, die Briefe eines Häftlings, der wegen Mitgliedschaft in einer Terrororganisation verurteilt wurde, zurückzuhalten. Wird jedoch nur ein Absatz des Briefs für bedenklich erachtet, kann damit die Zurückhaltung des gesamten Briefs des Häftlings an seine Verlobte nicht gerechtfertigt werden ([EGMR 03.06.2025, 9389/19, Uygun/Türkei](#)).

### Rechtsprechung des EuGH

- Nach dem bulgarischen Recht haben Anwälte unabhängig von der Parteistellung **Zugang zu gerichtlichen Akten**. Ein Anwalt begehrte Einsicht in einen Akt, in dem sein Mandant keine Parteistellung hatte. Die Anwälte der Verfahrensparteien hatten keine Einwände gegen die Gewährung der Akteneinsicht. Das Gericht hatte jedoch Zweifel, ob die bulgarische Regelung mit dem **Datenschutzrecht** vereinbar ist und stellte dem EuGH entsprechende Fragen. Der EuGH wies das **Vorabentscheidungsersuchen** wegen **Unzuständigkeit** zurück, weil die gestellten Fragen nicht die Lösung des vor dem Gericht anhängigen Rechtsstreits, sondern den **Antrag auf Akteneinsicht** betrafen. Über den Antrag auf Akteneinsicht wird in einem Verwaltungsverfahren entschieden, ein Vorabentscheidungsersuchen an den EuGH ist erst zulässig, wenn über ein Rechtsmittel gegen die Verwaltungsentscheidung auf Akteneinsicht abzusprechen ist ([EuGH 05.06.2025, C-541/24, Naltov](#)).
- Die Europäische Kommission leitete gegen **Ungarn** ein **Vertragsverletzungsverfahren** wegen nationalen Rechtsvorschriften gegen "pädophile Straftäter" und zum "Schutz von Kindern" vor LGBTI-Inhalten ein. Die Generalanwältin schlägt dem EuGH vor, sechs Verstöße Ungarns gegen EU-Primär- und Sekundärrecht festzustellen. Zum Verstoß gegen die DSGVO hat die Generalanwältin erwogen: Der **Schutz Minderjähriger** ist ein **öffentliches Interesse von höchster Bedeutung**. **Strafregisterdaten** sind jedoch **höchstensensible Daten** und könnten zu Stigmatisierung führen. Das ungarische Gesetz ist nicht ausreichend klar und präzise hinsichtlich der Kategorien von Personen, die auf das Strafregister zugreifen dürfen, und enthält keine hinreichenden Garantien zum Schutz der Betroffenen ([EuGH SA 05.06.2025, C-769/22, Kommission/Ungarn](#)).

## NACHTRAG

- Dem FIFA-Spielervermittlerreglement (**FFAR**) unterworfenen Vermittler haben Detailinformationen zu Kundenverträgen, Vergütungen und ihrer Mitwirkung auf eine von der **FIFA** betriebene Plattform hochzuladen. Diese Datenverarbeitung könnte (zumindest teilweise) auf die **Wahrung berechtigter Interessen** gestützt werden, wenn über diese berechtigten Interessen **informiert** wurde. Die von der FIFA geltend gemachten berechtigten Interessen, (i) Begrenzung von Interessenkonflikten, (ii) Verhinderung missbräuchlicher Praktiken, (iii) Überwachung und Durchsetzung des FFAR sind berechnete Interessen. Ob die Transparenz ein berechtigtes Interesse ist, hängt vom Zweck der Transparenz ab. Das nationale Gericht hat zu prüfen, ob der gesamte Umfang der erhobenen Daten für die Wahrung der berechtigten Interessen erforderlich ist und ob die Interessen der Betroffenen überwiegen, insb ob die Betroffenen einer unzumutbaren Belastung ausgesetzt werden ([EuGH SA 15.05.2025, C-209/23, RRC Sports](#)).

### Rechtsprechung des VwGH

VwGH 27.03.2025, Ro 2022/04/0023

#### **Mitarbeiter, Rollenverteilung, Übergangsbestimmung, Beschwerdegegner**

- Ein Betroffener erhob am 07.10.2019 Datenschutzbeschwerde gegen eine Stadtgemeinde. Er brachte vor, dass seine im Zentralen Melderegister (ZMR) gespeicherten Daten im Jahr 2016 mindestens dreimal von Bediensteten der Stadtgemeinde aus persönlichem Interesse und in eigener Verantwortung abgefragt wurden. Die DSB wies die Datenschutzbeschwerde mit der Begründung ab, dass die Bediensteten als "Auftraggeber" im Sinne des DSGVO 2000 anzusehen sind. Der Betroffene erhob Beschwerde an das BVwG, das diese abwies. Der VwGH wies die daraufhin erhobene Revision ebenfalls ab.

Der VwGH hat erwogen: Die maßgebliche Rechtslage ergibt sich aufgrund der **Übergangsbestimmung** des § 69 Abs 5 DSGVO aus dem (aktuellen) DSGVO und der DSGVO. Der Begriff des Verantwortlichen für eine Datenverarbeitung entspricht inhaltlich der Vorgängerbestimmung aus dem DSGVO 2000 ("Auftraggeber").

Aus dem MeldeG ergibt sich keine Verantwortlicheneigenschaft der Stadtgemeinde. Die Bediensteten verwendeten zwar die von der Stadtgemeinde eingerichtete technische Abfragemöglichkeit, das bedeutet aber nur, dass die Mittel der Stadtgemeinde genutzt wurden. Die Entscheidung über die Nutzung dieses Mittels und des Zwecks der ZMR-Abfrage wurde jedoch von den Bediensteten getroffen, weshalb diese als Verantwortliche

anzusehen sind. Da die Stadtgemeinde in keiner Weise in diese Entscheidung eingebunden war, ist sie auch nicht "Gemeinsam Verantwortliche" iSd Art 26 DSGVO.

Zu beachten ist, dass die Stadtgemeinde die ZMR-Daten nicht selbst gespeichert hat. Hätten die Bediensteten auf Daten zugegriffen, die die Stadtgemeinde speichert, hätte dies eine Verantwortlicheigenschaft der Stadtgemeinde begründen können, weil die Speicherung eine Verarbeitungstätigkeit ist.

Die Datenschutzbeschwerde war ausdrücklich und unmissverständlich gegen die Stadtgemeinde gerichtet. Ein Austausch der Person des Verantwortlichen im verwaltungsgewöhnlichen Verfahren kommt nicht in Betracht. Die Revision war daher als unbegründet abzuweisen.

VwGH 30.04.2025, Ro 2021/04/0005

### **Übergangsbestimmung, Lösungsersuchen, Informationspflicht**

- Ein Betroffener brachte im April 2018 bei der DSB eine Datenschutzbeschwerde ein, weil eine Kreditauskunftei seinem Ersuchen auf Datenlöschung nicht nachkam. Die DSB gab der Datenschutzbeschwerde statt, weil der Betroffene anlässlich der Eintragung seiner Daten bei der Kreditauskunftei nicht nachweislich informiert wurde. Die DSGVO finde Anwendung, weil die Löschung der Daten bis zum Verfahrensabschluss erfolgen könne. Die Kreditauskunftei erhob dagegen erfolgreiche Bescheidbeschwerde an das BVwG, das den Bescheid der DSB dahingehend abänderte, dass die Datenschutzbeschwerde des Betroffenen abgewiesen wird. Die unterlassene **Vorabinformation** an den Betroffenen führe zu keiner Datenschutzverletzung, die eine Lösungsverpflichtung nach sich ziehe. Gegen das Erkenntnis des BVwG erhob die DSB (erfolglos) Amtsrevision an den VwGH.

Der VwGH hat erwogen: Zu beurteilen ist ein Sachverhalt aus dem Jahr 2017. Nach der Rechtsprechung des VwGH bezieht sich der Beschwerdegegenstand hinsichtlich des Auskunftsrechts auf die durch ein bestimmtes Auskunftsersuchen begründete Auskunftspflicht und deren Nichterfüllung oder unvollständige Erfüllung. Nichts anderes kann für ein **Lösungsersuchen** gelten. Demnach ist die Frage, ob die Kreditauskunftei gegen ihre **Informationspflicht** verstoßen hat, am Maßstab der zum damaligen Zeitpunkt geltenden Rechtslage zu beurteilen. Somit findet die DSGVO keine Anwendung.

VwGH 30.04.2025, Ro 2021/04/0024

### **Videüberwachung, Geldbuße, Kumulationsprinzip**

- Ein Lokalbetreiber, in dessen Lokal **illegale Glücksspielgeräte** betrieben wurden, installierte eine Videoüberwachungsanlage, mit der ua ein angrenzender Gehsteig und ein öffentlicher Parkplatz erfasst wurden. Die Daten nutzte der Lokalbetreiber zur Identifizierung und Kategorisierung von Personen ("Finanzpolizei" und "Spieler"). Die Videoüberwachung war nicht gekennzeichnet. Die Aufnahmen wurden mindestens 18 Tage lang gespeichert. Die DSB verhängte wegen der Videoüberwachung, der Verarbeitung der Bilddaten und der Speicherdauer eine Geldstrafe iHv EUR 3.000 zuzüglich EUR 300 Verfahrenskostenbeitrag. Das BVwG bestätigte das Straferkenntnis der DSB. Aufgrund der ordentlichen Revision des Betreibers setzte der VwGH die Geldstrafe auf EUR 1.500 und den Verfahrenskostenbeitrag auf EUR 150 herab.

Der VwGH hat erwogen: Der Spruch eines Straferkenntnisses muss so gefasst sein, dass die **Subsumtion** der als erwiesen angenommenen Tat unter die verletzte Verwaltungsvorschrift eindeutig und vollständig erfolgt, also aus der Tathandlung auf das Vorliegen der bestimmten Übertretung geschlossen werden kann. Die Beschreibung von Gehsteig und Parkplatz war ausreichend präzise, weil ausgeführt wurde, dass sich diese unmittelbar neben dem Objekt befanden und es darauf ankam, dass sich die Videoüberwachungsanlage auf öffentlichen Raum erstreckt. Zwar sind im Spruch sämtliche **Tatbestandselemente** zu umschreiben, es schadet aber nicht, wenn die im Spruch angeführte "unverhältnismäßig lange Speicherdauer" in der Begründung durch die ziffernmäßige Angabe von 18 Tagen präzisiert wird.

Geldbußen nach der DSGVO sind Verwaltungsstrafen. Das VStG findet auf die Verhängung von Geldbußen gemäß Art 83 DSGVO insoweit Anwendung, als die DSGVO nicht speziellere Regelungen vorsieht. Die verhängte **Gesamtstrafe** verstößt nicht gegen das **Kumulationsprinzip** des § 22 VStG. Nach den Gesetzesmaterialien zum DSG ist bei der Verhängung von Geldbußen zwar grundsätzlich das VStG anzuwenden, im Fall der spezielleren Regelung des Art 83 Abs 3 DSGVO geht diese jedoch aufgrund des **Anwendungsvorrangs** des Unionsrechts dem in § 22 VStG normierten Kumulationsprinzip vor.

Die **Gesamtverfahrensdauer** von **fünf Jahren** war **unangemessen lang** iSd Art 6 Abs 1 EMRK, weil diese nicht der Sphäre des Lokalbetreibers zuzurechnen oder einer ungewöhnlichen Komplexität und Schwierigkeit der Rechtssache geschuldet war. Dieser



Umstand ist gemäß § 19 VStG iVm § 34 Abs 2 StGB als **strafmildernd** zu bewerten, sodass die verhängte Geldstrafe herabzusetzen war.

VwGH 15.04.2025, Ra 2021/04/0094

### **Anwaltsgeheimnis, Auskunft**

- Ein Betroffener beehrte von einem Rechtsanwalt Auskunft über seine personenbezogenen Daten, welche dieser in seiner Funktion als Rechtsvertreter einer Gemeinde verarbeitete, mit der sich der Betroffene im Rechtsstreit befand. Unter Berufung auf seine berufliche Verschwiegenheitspflicht erteilte der Rechtsanwalt keine Auskunft. Weiters verwies er darauf, dass die Daten und Schriftstücke dem Betroffenen bekannt sind. Der Betroffene brachte Datenschutzbeschwerde bei der DSB ein. Diese gab dem Betroffenen teilweise recht, weil der Rechtsanwalt zumindest eine Auskunft über die Stammdaten hätte erteilen müssen. Beide Verfahrensparteien erhoben Bescheidbeschwerde an das BVwG. Das BVwG wies beide Bescheidbeschwerden ab.

Der Rechtsanwalt richtete eine außerordentliche Revision an den VwGH, weil der Normenkonflikt zwischen den Regelungen der RAO einerseits und der DSGVO sowie des DSG andererseits höchstgerichtlich noch nicht geklärt sei. Weiters gäbe es von den Standesvertretungen der österreichischen Rechtsanwälte keine Vorgaben. Diese Rechtsunsicherheit träfe alle österreichischen Rechtsanwälte, weil möglicherweise Gegner eines Mandanten Auskunft über personenbezogene Daten verlangen könnten. Eine konkrete Begründung, warum die Stammdaten nicht beauskunftet wurden, brachte der Anwalt nicht vor. Der VwGH wies die außerordentliche Revision zurück.

Der VwGH hat erwogen: Unter Berufung auf ihre Verschwiegenheitspflicht können Rechtsanwälte die Auskunft an Betroffene nach der DSGVO und dem DSG einschränken, soweit dies zum Schutz der Partei, der Rechte und Freiheiten anderer Personen oder zur Durchsetzung zivilrechtlicher Ansprüche erforderlich ist. Die Verschwiegenheitspflicht von Rechtsanwälten gemäß § 9 Abs 4 RAO kann nur **punktuell** und unter **klar definierten** Voraussetzungen die Betroffenenrechte nach der DSGVO einschränken. Eine Einschränkung muss dabei für alle Daten **gesondert begründet** werden und kann nicht mit einem pauschalen Verweis auf Verschwiegenheitsverpflichtungen erfolgen. Im vorliegenden Fall habe der Rechtsanwalt nicht dargelegt, inwiefern die Auskunftserteilung über die Stammdaten tatsächlich seine Verschwiegenheitspflicht verletzen würde.

### Aus der weiteren Rechtsprechung des VwGH:

- Nach § 19a BStMG darf die **ASFINAG** zur Feststellung der ordnungsgemäßen Entrichtung der Maut und zur **Verfolgung von Mautprellerei automatische Überwachung** einsetzen. Die DSB brachte in ihrer Amtsrevision vor, dass für die Aufklärung des **Verdachts auf Mautprellerei** keine Datenspeicherung zulässig war. In der Zwischenzeit wurde § 19a BStMG dahingehend klarstellend novelliert, dass die ASFINAG auch beim Verdacht auf Mautprellerei die erhobenen Daten (insbesondere Bilddaten) verarbeiten darf. Da die revisionsgegenständliche Regelung außer Kraft getreten ist und nur einen kleinen potenziellen Personenkreis betraf, ist die Revision nicht zulässig ([VwGH 15.04.2025, Ro 2021/04/0012](#)).
- Eine Gesellschaft, die auf die **Abwicklung des Forderungskaufs** aus Fluggastrechten, Verstößen gegen die **DSGVO** und Online-Glücksspiel spezialisiert ist, greift, sofern sie die erworbenen Forderungen bloß **im eigenen Namen** durchsetzt, noch nicht in die den Rechtsanwälten vorbehaltenen Befugnisse ein ([VwGH 06.05.2025, Ra 2024/07/0121](#)).
- Die **Aufwendungen für eine Datenschutzbeschwerde** sind, sofern die Rechtsdurchsetzung vorrangig den Bereich **der persönlichen Lebensführung** betrifft, **keine Werbungskosten**. Sie können daher in einer **Arbeitnehmerveranlagung** nicht als Werbungskosten geltend gemacht werden ([VwGH 24.04.2025, Ra 2023/15/0105](#)).

### **Rechtsprechung der Justiz**

#### Aus der Rechtsprechung der Justiz:

- Lehnt der Netzbenutzer den Austausch eines "eichfälligen" Zählers gegen ein intelligentes Messgerät ("**Smart Meter**") ab, darf der Netzbetreiber keine **Stromabschaltung** androhen. Dem Netzbetreiber steht es aber offen, gerichtliche Hilfe bei der Durchsetzung seines Interesses auf Tausch des Stromzählers in Anspruch zu nehmen ([OGH 30.04.2025, 5Ob35/25w](#)).
- Ein Antrag auf Erlass einer **einstweiligen Verfügung** zur **Sicherung von Daten** als Beweismittel greift in Grundrechte ein und ist unverhältnismäßig, wenn mit einem auf **Herausgabe der Daten** gerichteten **Sicherungsantrag** dasselbe Ziel erreicht werden kann. Bestehen keine hinreichenden Anhaltspunkte dafür, dass eine Partei Beweismittel vernichten oder unterdrücken wird, kann dieser Partei die potenzielle **Beweismittelvernichtung** nicht unterstellt werden. Denn ein **Rechtsstaat** hat grundsätzlich von der Normtreue der

Normunterworfenen auszugehen ([OLG Linz 13.05.2025, 4R64/25x](#)).

- Einen Auskunftsanspruch hat nur die Betroffene, deren personenbezogene Daten verarbeitet wurden. Es genügt ein formloses Ersuchen, das schriftlich, elektronisch und auch mündlich gestellt werden kann. Der Verantwortliche hat die Ausübung der Betroffenenrechte zu erleichtern ("**Erleichterungsgrundsatz**"). Die Kopie eines gültigen Nachweises über die **Änderung des Namens** darf zur **Identifizierung** des Betroffenen nicht verlangt werden ([OLG Linz 14.05.2025, 3R58/25q](#)).

### **Rechtsprechung des BVwG**

[BVwG 27.01.2025, W605 2248297-1](#)

#### **Grundbuch, informationeller Mehrwert, konkrete Empfänger, Dateninhalt, Akteneinsicht**

- Ein Unternehmen betreibt eine kostenpflichtige Web-Applikation, in der öffentlich zugängliche Informationen aus dem **Grundbuch** eingespeist werden. Ein Betroffener, der ein Auskunftersuchen an das Unternehmen stellte, erachtete die erteilte Auskunft mangels konkreter Empfänger und mangels Informationen über geeignete Garantien bei Drittlandsübermittlungen für unvollständig. Er erhob Datenschutzbeschwerde bei der DSB wegen Verletzung in seinen Rechten auf Auskunft, Information, Geheimhaltung und später auch wegen Verletzung im Recht auf Einschränkung der Datenverarbeitung. Die DSB wies die Datenschutzbeschwerde hinsichtlich der behaupteten Verletzungen in den Rechten auf Auskunft, Geheimhaltung und Einschränkung der Verarbeitung ab, wobei sie in Hinblick auf das Auskunftsrecht, über die Frage, ob konkrete Empfänger zu beauskunften sind, explizit nicht absprach. Hinsichtlich der behaupteten Verletzung im Recht auf Information gab die DSB der Datenschutzbeschwerde statt und trug dem Unternehmen auf, dem Betroffenen eine entsprechende Information zu erteilen. Das BVwG gab der Bescheidbeschwerde des Betroffenen teilweise statt.

Das BVwG hat erwogen: Die Bestimmungen des Art 15 Abs 1 und des Art 15 Abs 1 lit c DSGVO sind zusammen zu lesen, sodass ein Recht auf Auskunft über die konkret an die Empfänger übermittelten Daten besteht. Da die DSB die Fragen zu den **konkreten Empfängern** und zum **Inhalt der** an die Empfänger **übermittelten Daten** im fortgesetzten Verfahren mit Bescheid erledigt hat, sind diese jedoch nicht vom gegenständlichen Verfahren umfasst.

Bei **Übermittlungen in Drittländer** unter Verwendung **geeigneter Garantien** nach Art 46 DSGVO hat der Verantwortliche die betroffene Person zu unterrichten. Da die

DSB mit der Frage der konkreten Empfänger bis zur Vorabentscheidung durch den EuGH zugewartet hat, durfte sie nicht davon ausgehen, dass keine Übermittlung personenbezogener Daten an ein Drittland erfolgt wäre. Dem Betroffenen ist daher zu Unrecht eine Unterrichtung über die geeigneten Garantien gemäß Art 46 DSGVO verweigert worden.

Eine mangelnde Schutzwürdigkeit iSd § 1 Abs 1 DSG ist nur bei bloßer Reproduktion von "allgemein zugänglichen Daten" ohne Generierung neuer Information anzunehmen. Da die abgefragten **Grundbuchdaten** neu kombiniert und dargestellt werden und somit ein **informationeller Mehrwert** generiert wird, ist von einer neuen Datenverwendung auszugehen, deren Zulässigkeit nach dem DSG und der DSGVO zu prüfen ist. Da die DSB eine Verletzung im **Recht auf Information** gemäß Art 14 Abs 1 lit d DSGVO feststellte, liegt auch eine **Verletzung des Transparenzgebots** iSd Art 5 Abs 1 lit a DSGVO vor. Selbst bei Vorliegen eines **berechtigten Interesses** gemäß Art 6 Abs 1 lit f DSGVO ergibt sich aus der Verletzung dieses Grundsatzes eine Verletzung des Betroffenen im Recht auf Geheimhaltung gemäß § 1 DSG iVm Art 5 Abs 1 lit a DSGVO.

Da die Verarbeitung auch gegen den Grundsatz von Treu und Glauben gemäß Art 5 Abs 1 lit a DSGVO verstieß, stand dem Betroffenen ein Lösungsanspruch zu und die Verarbeitung hätte gemäß Art 18 Abs 1 DSGVO **eingeschränkt** werden müssen.

Auch wenn unzweifelhaft **Betriebs- und Geschäftsgeheimnisse** eine Ausnahme von der **Akteneinsicht** nach § 17 Abs 3 AVG begründen können, bedarf es bei der Verweigerung der Akteneinsicht einer genauen und nachvollziehbaren Begründung, weil die Verweigerung der Akteneinsicht die rechtlichen Möglichkeiten der Partei wesentlich einschränkt. Der pauschale Verweis auf Betriebs- und Geschäftsgeheimnisse reicht nicht aus. Da dem Betroffenen im Rahmen des verwaltungsgerichtlichen Verfahrens Akteneinsicht eingeräumt wurde, wurde ein infolge der Verweigerung der Akteneinsicht vorliegender Verfahrensmangel geheilt.

[BVwG 03.04.2025, W176 2259543-1](#)

#### **Adressverlag, Kreditauskunftei, Bonitätsbewertung**

- Ein Betroffener erhob Datenschutzbeschwerde gegen die Übermittlung seiner Daten durch einen Adressverlag. Der Adressverlag übermittelte den Namen, das Geburtsdatum und die Adresse des Betroffenen an eine Kreditauskunftei, die diese Daten für Bonitätsbewertungen nutzte. Der Betroffene hatte dieser Zweckänderung nie zugestimmt. Aufgrund der Datenschutzbeschwerde des Betroffenen stellte die DSB

fest, dass der Adressverlag gegen den Grundsatz der Zweckbindung verstoßen hat. Ein ebenfalls begehrtes Verarbeitungsverbot ordnete die DSB nicht an, weil Art 58 DSGVO einem Betroffenen darauf kein subjektives Recht einräumt. Gegen diese Entscheidung erhoben der Betroffene und der Adressverlag jeweils erfolglose Bescheidbeschwerden an das BVwG.

Das BVwG hat erwogen: Der Vertrag zwischen dem **Adressverlag** und der **Kreditauskunftei** ermächtigte die Kreditauskunftei zur Datenverarbeitung zu "sonstigen Zwecken". Der Adressverlag hätte daher von einer Verarbeitung zur **Bonitätsbewertung** ausgehen müssen. Personenbezogene Daten, welche ursprünglich zu Marketingzwecken erhoben wurden, dürfen an eine Kreditauskunftei nicht übermittelt werden, außer es kann davon ausgegangen werden, dass sie nur für Marketingzwecke verwendet werden. Eine Datenverarbeitung zu Marketingzwecken ist mit der **Weiterverarbeitung** für eine Bonitätsbewertung unvereinbar.

Entspricht eine Datenverarbeitung nicht den Grundsätzen nach Art 5 DSGVO, kann die DSB nach Art 57 und 58 DSGVO tätig werden. Dabei hat die DSB für ein **angemessenes Schutzniveau** für den Betroffenen zu sorgen. Es ist aber Sache der DSB, das geeignete Mittel zu wählen, um Abhilfe zu schaffen. Das Verbot einer Verarbeitung ist eine **belastende Maßnahme**, weshalb die DSB vor dem Verbot weniger eingriffsintensive Maßnahmen prüfen muss. Die DSB ist auch **nicht verpflichtet**, eine Maßnahme zu erlassen, wenn diese nicht geeignet, erforderlich oder verhältnismäßig ist, um der festgestellten Unzulänglichkeit abzuwehren. Betroffene haben kein **subjektives Recht** auf das Anordnen eines Verarbeitungsverbots. **Anm: Im oben zitierten Urteil des OLG Linz (13.05.2025, 4R64/25x) geht das Zivilgericht davon aus, dass in einem Rechtsstaat von der Normtreue der Normunterworfenen auszugehen ist. Das BVwG nimmt offenbar die gegenteilige Position ein. Denn die Verwendung von Marketingdaten für Bonitätsbewertungen ist gesetzlich ausdrücklich untersagt (§ 151 GewO). Dennoch hätte der Adressverlag der Kreditauskunftei die rechtswidrige Verwendung zu unterstellen gehabt.**

Aus der weiteren Rechtsprechung des BVwG:

- Die DSB ist für die Aufsicht über die von den Gerichten in Ausübung ihrer **justiziellen Tätigkeit** ausgeübten Datenverarbeitungen nicht zuständig. Die **Gerichtsvollzieher** sind Exekutivorgane, die bei einer Vollstreckung nach der EO als "richterliche Hilfsorgane" auftreten und "**abgeleitete richterliche Akte**" setzen. Ihre Tätigkeit ist daher

der Gerichtsbarkeit zuzuordnen ([BVwG 21.05.2024, W605 2232133-1](#)).

- Unabhängig vom Zeitpunkt der Kenntnisnahme ist eine Datenschutzbeschwerde längstens innerhalb von drei Jahren, nachdem das Ereignis stattgefunden hat, einzubringen. Dh, selbst wenn die Datenschutzbeschwerde ab Kenntnisnahme innerhalb von einem Jahr eingebracht wird (**subjektive Präklusivfrist**), ist das Recht auf Einbringen einer Datenschutzbeschwerde **erloschen**, wenn die **absolute** bzw **objektive Präklusivfrist** von drei Jahren bereits abgelaufen ist ([BVwG 21.05.2024, W605 2287853-1](#)).
- Die Erkenntnisse des BVwG sind in anonymisierter Form im RIS zu veröffentlichen. Die **Anonymisierung** ist Gegenstand der Rechtsprechung, weshalb für Datenschutzbeschwerden nicht die DSB, sondern das **BVwG zuständig** ist. Unterlässt das BVwG die Anonymisierung, erfolgt eine Verletzung im Recht auf Geheimhaltung, die durch nachträgliche Anonymisierung nicht rückwirkend beseitigt werden kann. Dem Beschwerdeführer sind die **Kosten** der Eingabegebühr sowie der pauschalierte Schriftsatzaufwand zu **ersetzen** ([BVwG 04.03.2024, W605 2274353-1](#)).
- Die **E-Mail** ist **keine zulässige Form der elektronischen Einbringung** beim BVwG (§ 1 Abs 1 letzter Satz BVwG-EVV). Ein mit E-Mail eingebrachter Schriftsatz entfaltet keine Rechtswirkungen, weshalb kein Verbesserungsauftrag zu erteilen ist. Ein per E-Mail eingebrachter Schriftsatz gilt als **nicht eingebracht** und ist daher zurückzuweisen ([BVwG 20.02.2024, W605 2286285-1](#)).
- Gemäß **§ 24d Abs 2 Z 5 GTelG** dürfen im **zentralen Impfregeister** gespeicherte Daten für das **Krisenmanagement** verarbeitet werden. Das Krisenmanagement umfasst das **Ausbruchmanagement** und die **Pharmakovigilanz**. Zum Zeitpunkt der Abfrage des Impfregeisters gab es keine Rechtsgrundlage, die das Versenden eines **Impferinnerungsschreibens** zur dritten Corona-Schutzimpfung gerechtfertigt hätte. Ebenso wenig war der Zugriff auf den **Patientenindex** zur Adressermittlung berechtigt ([BVwG 23.05.2024, W298 2261880-1](#)).
- Deckt der Spruch des Bescheids der DSB den Beschwerdeinhalt vollinhaltlich ab, liegt **keine Säumnis** hinsichtlich eines Teilinhalts der Datenschutzbeschwerde vor. Ein Anspruch auf die Feststellung von separaten Rechtsverletzungen betreffend Teilhandlungen besteht nicht. Die **Säumnisbeschwerde** ist daher abzuweisen. Ein Anspruch über **Schadenersatz** oder einen Anschluss als **(strafrechtlicher) Privatbeteiligter** ist im datenschutzrechtlichen Verwaltungsverfahren nicht vorgesehen ([BVwG 14.04.2025, W137 2297606-1](#)).

- Der rechtlich relevante Sachverhalt ist von der DSB **von Amts wegen** vollständig zu ermitteln. Die DSB darf sich über erhebliche Behauptungen von Parteien nicht ohne **Ermittlungen** hinwegsetzen ([BVwG 21.05.2024, W605 2286028-1](#)).
- Steht die **federführende Aufsichtsbehörde** noch nicht fest, regelt § 24 Abs 10 Z 2 DSG lediglich eine Hemmung des Fristenlaufs, enthält aber keine Grundlage für eine **Verfahrensaussetzung**. Gegenstand des Beschwerdeverfahrens vor dem BVwG ist nur die **Rechtmäßigkeit der beschneidmässigen Aussetzung** durch die DSB ([BVwG 21.05.2024, W605 2278491-1](#)).
- Die DSB überschreitet die "Sache" des Verfahrens, wenn sie eine Datenschutzbeschwerde **einseitig abändert**. Die Änderung einer eindeutig bestimmten Partei ist nicht zulässig. Erlässt die DSB ihren Bescheid gegen einen **Beschwerdegegner**, der von der Datenschutzbeschwerde nicht umfasst war, ist dieser Bescheid ersatzlos zu beheben ([BVwG 09.07.2024, W258 2272449-1](#)).

### Rechtsprechung der DSB

Aus der Rechtsprechung der DSB:

#### **Data Breach, Mitwirkung, Doppelbestrafung**

- Bringt ein Verantwortlicher eine Sicherheitsverletzungs-Meldung ("**Data Breach**"-Meldung) iSd Art 33 DSGVO bei der DSB ein, hat er an einem daraufhin eingeleiteten **Sicherheitsverletzungs-Verfahren** mitzuwirken. Bei Verweigerung der Mitwirkung wird über den Verantwortlichen eine **Geldbuße** verhängt. Das Sicherheitsverletzungs-Verfahren kann unabhängig von der Verhängung der Geldbuße fortgesetzt werden. Wirkt der Verantwortliche nach erneuter Aufforderung zur Rechtfertigung erneut nicht mit, wird für die mangelnde Mitwirkung im **Zeitraum** nach dem ersten Straferkenntnis eine **weitere Geldbuße** verhängt ([DSB 07.10.2024, 2024-0.671.673](#)). **Anm: Die Verletzung der Mitwirkungspflicht ist ein Dauerdelikt durch Unterlassung.** Zwar sind die Geldbußen für zwei unterschiedliche Zeiträume verhängt worden. Das Dauerdelikt ist jedoch – anders als das fortgesetzte Delikt (auch tatbestandliche Handlungseinheit genannt) – eine einzige Tat. Die Vereinbarkeit der zweiten Geldbuße mit dem **Verbot der Doppelbestrafung** erscheint daher fraglich.

### Leitlinien des EDSA

- Nach Durchführen einer öffentlichen Konsultation veröffentlichte der **EDSA** am **05.06.2025** die finalen "[Guidelines 02/2024 on Article 48 GDPR<sup>2</sup>](#)". Gemäß

Art 48 DSGVO dürfen Urteile bzw Entscheidungen von Gerichten und Verwaltungsbehörden eines Drittlands nur dann anerkannt werden, wenn sie auf eine internationale Übereinkunft gestützt sind. Die Leitlinien enthalten Empfehlungen an Verantwortliche und Auftragsverarbeiter, wie mit Anfragen von Gerichten und Verwaltungsbehörden aus Drittstaaten umzugehen ist. **Anm: Die erste Version dieser Leitlinien wurde vor der öffentlichen Konsultation veröffentlicht. Eine Zusammenfassung der ersten Version finden Sie im [Datenschutzmonitor vom 18.12.2024](#).**

to the point

# Datenschutzmonitor. 24/2025 vom 18.06.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr Email-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 12.06.2025, 33037/22, *TH/Tschechien* (Geschlechtseintrag, Personenstand, körperliche Unversehrtheit)

- **Rechtsprechung des VwGH**

VwGH 30.04.2025, Ra 2021/04/0118 (Meldedaten, Bürgerbeteiligung, Übergangsbestimmung)

VwGH 29.04.2025, Ra 2024/11/0150; 29.04.2025, Ra 2024/11/0151 (KFZ, Zulassungsevidenz, rechtliches Interesse)

- **Rechtsprechung der Justiz**

LG Innsbruck 19.06.2024, 350Jv184/25a (Dienste der Informationsgesellschaft, Herkunftsländprinzip, Zuständigkeit)

OGH 13.05.2025, 10b27/25i; 14.05.2025, 50b23/25f; 21.05.2025, 70b34/25p; 22.05.2025, 40b11/25h; 22.05.2025, 40b61/25m (Smart Meter, einstweilige Verfügung, Sicherheitsleistung)

OLG Wien 27.03.2025, 33R49/25f (Prozessführung, Rechtsmissbrauch, Geschäftsgeheimnis)

- **Rechtsprechung des BVwG**

BVwG 09.07.2024, W258 2261773-1 (ne bis in idem)

BVwG 09.04.2025, W287 2272807-1; 22.04.2025, W287 2271841-1 (Betroffenheit, Mitwirkungspflicht)

BVwG 29.04.2025, W254 2252989-2 (Akteneinsicht, Vollmacht, Telefax)

BVwG 24.04.2025, W298 2308675-1 (Unterichtungspflicht, Feststellung)

BVwG 07.04.2025, W252 2297618-1; 23.04.2025, W605 2281980-1 (Zurückziehung der Bescheidbeschwerde)

- **Rechtsprechung des BFG**

BFG 14.05.2025, RV/7100831/2020 (Online-Glücksspiel, Glücksspielabgabe, Teilnahme vom Inland)

- **Rechtsprechung der LVwG**

LVwG NÖ 07.05.2025, LVwG-AV-1103/001-2024 (KFZ, Zulassungsevidenz, Pressefreiheit, Art 6 Abs 1 lit e DSGVO)

- **Rechtsprechung der DSB**

DSB 18.04.2025, 2025-0.303.076 (Schengener Informationssystem, Löschung)

DSB 03.06.2025, 2025-0.177.424 (Mitwirkungspflicht, Geldbuße, Vorsatz)

- **EU-Rechtsakte**

Delegierte VOs zu Kryptowerte-Dienstleistungen

Empfehlung des Rates zum Cybersicherheitskrisenmanagement (Cyber Blueprint)

- **Nationale Rechtsakte**

Oö ITEG (künstliche Intelligenz, automatisierte Entscheidung)

- **Vorschau EuGH-Rechtsprechung**

## To the Point:

### Rechtsprechung des EGMR

EGMR 12.06.2025, 33037/22, TH/Tschechien

#### **Geschlechtseintrag, Personenstand, körperliche Unversehrtheit**

- Nach tschechischem Recht ist eine rechtliche Anerkennung des Geschlechts nur nach einer geschlechtsangleichenden Operation samt Sterilisation zulässig. Eine **nicht-binäre Person**, die bei ihrer Geburt im Personenstandsregister als "männlich" registriert wurde, beantragte mehrfach die Änderung des Geschlechtseintrags in ihrem Personalausweis auf "weiblich". Sie unterzog sich hormonellen und ästhetischen Behandlungen, wollte jedoch aus gesundheitlichen Gründen keine irreversible **geschlechtsangleichende Operation** einschließlich Sterilisation. Die zuständige Behörde lehnte ihre Anträge ab. Die tschechischen Gerichte wiesen ihre anschließende Klage unter Verweis auf die geltende Rechtslage sowie das Interesse an verlässlichen **Personenstandsdaten** im Rahmen eines **binären Geschlechtersystems** ab. Eine Verfassungsbeschwerde blieb erfolglos, sodass die nicht-binäre Person den EGMR anrief.

Der EGMR hat erwogen: Das Recht auf Privatleben nach Art 8 EMRK umfasst die **Geschlechtsidentität** als Bestandteil der persönlichen Identität. Dieses Recht gilt für alle Menschen, auch für solche, die keine geschlechtsangleichenden Maßnahmen durchführen lassen.

Staaten müssen rasche, transparente und zugängliche Verfahren zur Änderung des eingetragenen Geschlechts für **Transpersonen** bereitstellen. Aufgrund der besonderen Bedeutung von Geschlechtsidentität und persönlicher Autonomie ist der staatliche **Ermessensspielraum** bei der Umsetzung dieser positiven Verpflichtungen **besonders eng**. Die Sicherung der Zuverlässigkeit und Konsistenz von **Personenstandsdaten** sowie das Interesse an der **Rechtssicherheit** sind legitime Gemeinwohlinteressen, die strenge Verfahren rechtfertigen können. Eine gesetzliche Regelung, die die Anerkennung der Geschlechtsidentität von Transpersonen von einer Operation mit Sterilisation abhängig macht, ist jedoch eine Bedingung, die die Ausübung des Rechts auf Achtung des Privatlebens an den Verzicht auf die **körperliche Unversehrtheit** knüpft. Die betroffene Person steht vor dem **unauflösbaren Dilemma**, entweder die körperliche Unversehrtheit aufzugeben oder auf die Anerkennung der eigenen Geschlechtsidentität zu verzichten. Die innerstaatlichen Behörden haben das erforderliche ausgewogene Verhältnis zwischen Allgemeininteresse und den Rechten des Einzelnen nicht gewahrt, sodass eine Verletzung des Art 8 EMRK vorliegt.

Anm: Im vergangenen Jahr hat auch das tschechische Verfassungsgericht entschieden, dass eine Änderung des Geschlechtseintrags künftig ohne Sterilisation und chirurgische geschlechtsangleichende Maßnahmen möglich sein muss. Eine Gesetzesreform zum Verfahren der Geschlechtsanerkennung scheint zwar im Gange zu sein, ein entsprechendes Gesetz wurde aber noch nicht verabschiedet.

### Rechtsprechung des VwGH

VwGH 30.04.2025, Ra 2021/04/0118

#### **Meldedaten, Bürgerbeteiligung, Übergangsbestimmung**

- Die Stadt Wels führte im Jahr 2016 eine Bürgerumfrage durch. Hierfür wurden Meldedaten aus dem zentralen Melderegister (**ZMR**) abgefragt, um den teilnahmeberechtigten Personen ein Informationsschreiben samt persönlichem Zugangscode postalisch zuzusenden. Dagegen erhob ein Betroffener Datenschutzbeschwerde. Er brachte vor, dass die Verwendung seiner Meldedaten einer gesetzlichen Zweckbindung unterliege. Die Datenverwendung zum Zweck der Bürgerumfrage sei keine "gesetzlich übertragene Aufgabe" iSd § 8 Abs 3 Z 1 DSGVO 2000 und somit unzulässig gewesen. Die DSB gab der Datenschutzbeschwerde statt. Der Magistrat der Stadt Wels erhob daraufhin Bescheidbeschwerde an das BVwG, das diese abwies. Gegen das Erkenntnis des BVwG erhob der Magistrat (erfolgreich) Revision an den VwGH.

Der VwGH hat erwogen: Zu beurteilen ist ein Sachverhalt aus dem Jahr 2016, weshalb die **alte Rechtslage** des DSGVO 2000 anzuwenden ist. Gemäß § 7 Abs 1 DSGVO 2000 durften personenbezogene Daten nur verarbeitet werden, soweit Zweck und Inhalt der Datenverarbeitung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Verantwortlichen gedeckt waren und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzt werden.

Das postalisch versendete Informationsschreiben fand seine gesetzliche Grundlage in § 70 des Statuts der Stadt Wels 1992, wonach die Stadt ihre Einwohner über bestimmte Vorhaben zu informieren hat. Die Verwendung der **Meldedaten** iZm dem Informationsschreiben war erforderlich und das gelindeste zur Verfügung stehende Mittel. Eine Datenverarbeitung kann nämlich auch dann erforderlich sein, wenn damit die im öffentlichen Interesse stehenden Aufgaben des Verantwortlichen **effizient(er)** erfüllt werden können. Durch die Versendung des Informationsschreibens samt persönlichem Zugangscode wurde eine einfache Teilnahme an der **Bürgerumfrage** ermöglicht und dadurch eine möglichst hohe

**Partizipation** der Bevölkerung erreicht. Die Datenverarbeitung war daher rechtmäßig.

Aus der weiteren Rechtsprechung des VwGH:

- Gemäß **§ 47 Abs 2a KFG** ist Privatpersonen, die ein rechtliches Interesse glaubhaft machen, aus der **Zulassungsevidenz** eine Auskunft über **Name und Anschrift** der KFZ-Zulassungsbesitzer zu erteilen. Diese Auskunft ist nicht nur natürlichen Personen, sondern auch **juristischen Personen** zu erteilen. Das **rechtliche Interesse** kann ein **subjektiv öffentliches Recht** sein oder aus dem **Privatrecht** erfließen. Das Bestehen des rechtlichen Interesses ist jedoch zu belegen. Auf bloße Behauptungen kann das rechtliche Interesse nicht gestützt werden. Zudem muss ein Zusammenhang mit einem bestimmten Kraftfahrzeug und dessen Verwendung bestehen (VwGH [29.04.2025, Ra 2024/11/0150](#); [29.04.2025, Ra 2024/11/0151](#)).

### **Rechtsprechung der Justiz**

LG Innsbruck 19.06.2024, 350Jv184/25a

#### **Dienste der Informationsgesellschaft, Herkunftslandprinzip, Zuständigkeit**

- Drei Polizeibeamte beantragten beim LG Innsbruck die Betreiberin einer Internetplattform mit Sitz in Irland zu verpflichten, ihnen die Identität (Name, Geburtsdatum, Post- und E-Mail-Adresse) der Person bekanntzugeben, die auf der Plattform ein Video hochgeladen hatte. Auf dem Video konnten die Polizeibeamten während einer Amtshandlung deutlich erkannt werden. Sie argumentierten, das Video sei ohne ihre Zustimmung aufgenommen und veröffentlicht worden, es verletze ihre Persönlichkeitsrechte, insb den Bildnisschutz nach § 78 UrhG, sowie ihre Datenschutzrechte. Die Plattformbetreiberin lehnte ein zuvor an sie gerichtetes Auskunftersuchen ab. Das LG Innsbruck wies den Antrag wegen internationaler Unzuständigkeit zurück.

Das LG Innsbruck hat erwogen: Gemäß Art 7 Abs 2 EuGVVO kann eine Person, die einen Wohnsitz im Hoheitsgebiet eines Mitgliedstaats hat, vor dem Gericht des Ortes eines anderen Mitgliedstaats, an dem das schädigende Ereignis eingetreten ist oder einzutreten droht, geklagt werden. Dies aber nur, wenn eine unerlaubte Handlung oder Ansprüche aus einer solchen Handlung den Gegenstand des Verfahrens bilden. Ein Auskunftsanspruch gegen einen Dienstanbieter nach § 13 Abs 3 ECG (vormals quasi wortgleich § 18 Abs 4 ECG) ist kein Anspruch aus unerlaubter Handlung. Dies gilt auch, wenn der Auskunftswerber behauptet, kreditschädigenden Äußerungen ausgesetzt worden zu sein. Die internationale Zuständigkeit österreichischer Gerichte ist daher nicht gegeben.

Nach dem **Herkunftslandprinzip** (§ 20 ECG, Art 3 RL 2000/31/EG) ist auf die Betreiberin irisches Recht anzuwenden.

Gemäß § 22 Abs 1 ECG kann ein Gericht oder eine Verwaltungsbehörde im Rahmen seiner bzw ihrer gesetzlichen Befugnisse abweichend vom Herkunftslandprinzip Maßnahmen ergreifen, die den freien Verkehr der **Dienste der Informationsgesellschaft** aus einem anderen Mitgliedsstaat einschränken. Solche Maßnahmen müssen jedoch zum Schutz eines der in § 22 Abs 2 ECG genannten Rechtsgüter – wie etwa den Schutz der Menschenwürde – erforderlich sein. Die behauptete schädigende Handlung (das Hochladen des Videos) wurde von einem Dritten begangen.

Das **irische Recht** kennt keine mit § 18 Abs 4 ECG vergleichbare Auskunftspflicht. Das Video zeigt die Polizeibeamten zwar erkennbar, jedoch ausschließlich bei einer korrekt durchgeführten Amtshandlung. Eine Verletzung der Menschenwürde oder ein besonders intensiver Eingriff in die Persönlichkeitssphäre (wie etwa durch Erfüllung eines Tatbestands von § 1330 ABGB, § 152 StGB oder § 78 UrhG) liegt nicht vor. Die Voraussetzungen für eine Ausnahme vom Herkunftslandprinzip sind deshalb nicht erfüllt.

Dienstanbieter sind grundsätzlich nicht für von Dritten hochgeladene Inhalte **verantwortlich**, solange sie keine tatsächliche Kenntnis von einer Rechtsverletzung haben bzw nach Kenntniserlangung unverzüglich tätig werden. Im vorliegenden Fall lag keine offensichtliche Rechtsverletzung vor, die eine **Auskunftspflicht** begründen könnte.

Aus der weiteren Rechtsprechung der Justiz:

- Lehnt der Netzbenutzer den Austausch eines "eichfälligen" Zählers gegen ein intelligentes Messgerät ("**Smart Meter**") ab, darf der Netzbetreiber keine **Stromabschaltung** androhen. Dem Netzbetreiber steht es aber offen, gerichtliche Hilfe bei der Durchsetzung seines Interesses auf Tausch des Stromzählers in Anspruch zu nehmen. Die vom Rekursgericht erlassene **einstweilige Verfügung** zugunsten des Netzbenutzers wird bestätigt. Sie wird jedoch ungültig, wenn der Netzbenutzer beim Erstgericht keine **Sicherheitsleistung** iHv EUR 10.000 erlegt (OGH [13.05.2025, 10b27/25i](#); [14.05.2025, 50b23/25f](#); [21.05.2025, 70b34/25p](#); [22.05.2025, 40b11/25h](#); [22.05.2025, 40b61/25m](#)).
- Ein **Auskunftersuchen** darf darauf abzielen, **Beweismaterial** für eine spätere **Prozessführung** zu beschaffen. Der Einwand des **Rechtsmissbrauchs** schlägt daher nicht durch. Eine nähere Prüfung des **Motivs** des Auskunftswerbers ist nicht erforderlich. Daten aus einer gemeinsamen Geschäftsbeziehung können **kein Geschäftsgeheimnis**

des Verantwortlichen sein ([OLG Wien 27.03.2025, 33R49/25f](#)).

### **Rechtsprechung des BVwG**

Aus der Rechtsprechung des BVwG:

- Entscheidet die DSB über eine Datenschutzbeschwerde zweimal, ist der spätere Bescheid ersatzlos zu beheben (**ne bis in idem**), weil der DSB für die neuerliche Entscheidung keine Kompetenz zukommt ([BVwG 09.07.2024, W258 2261773-1](#)).
- Eine Verletzung des Rechts auf Geheimhaltung kann nur dann vorliegen, wenn **tatsächlich Daten des Betroffenen verarbeitet wurden**. Den Betroffenen trifft eine **Mitwirkungspflicht**, den **Nachweis** der Verarbeitung zu erbringen. Es besteht eine **erhöhte Mitwirkungspflicht**, wenn es um Umstände geht, die in der persönlichen Sphäre der Parteien liegen (BVwG [09.04.2025, W287 2272807-1](#); [22.04.2025, W287 2271841-1](#)).
- Wird ein **Antrag auf Akteneinsicht** durch einen Bevollmächtigten gestellt, ist die Vollmacht schriftlich vorzulegen. Maßgeblich für die Schriftlichkeit ist, dass die **Vollmachtsurkunde** eigenhändig unterschrieben oder qualifiziert signiert ist. Eine per **Telefax** eingebrachte Vollmachtsurkunde genügt nicht ([BVwG 29.04.2025, W254 2252989-2](#)).
- Erhebt ein Betroffener eine Datenschutzbeschwerde an die DSB, hat die DSB den Betroffenen innerhalb von drei Monaten über den Stand oder das Ergebnis des Verfahrens zu unterrichten. Über Säumnisbeschwerden wegen Verletzung der **Unterrichtungspflicht** entscheidet das BVwG. Die Säumnisbeschwerde ist jedoch zurückzuweisen, wenn der Betroffene über den Stand des Verfahrens und das Ergebnis der Ermittlung tatsächlich informiert worden ist. Eine **Feststellung** der Verletzung der Unterrichtungspflicht **in der Vergangenheit** kommt zudem nicht in Betracht ([BVwG 24.04.2025, W298 2308675-1](#)).
- Die **Zurückziehung einer Bescheidbeschwerde** führt zum Verlust des Erledigungsanspruchs. Geht der Erledigungsanspruch verloren, ist das Verfahren **einzustellen** (BVwG [07.04.2025, W252 2297618-1](#); [23.04.2025, W605 2281980-1](#)). **Anm: Das Erkenntnis des Senats W605 weicht von der ständigen Rechtsprechung des BVwG ab, weil – statt mit Beschluss – mit Erkenntnis entschieden wurde.**

### **Rechtsprechung des BFG**

Aus der Rechtsprechung des BFG:

- Gemäß § 57 Abs 2 GSpG ist eine **Glücksspielabgabe** für **Online-Glücksspiel** zu

entrichten, an dem die Teilnahme vom Inland aus erfolgt. Das Tatbestandsmerkmal "**Teilnahme vom Inland**" kann aus eigener Wahrnehmung des Glücksspielanbieters ohne entsprechende Ermittlungen nicht erhoben werden. Die Teilnahme vom Inland ist daher anhand von Indizien wie "**inländische Registrierungsadresse**", "**inländische IP-Adresse**" oder "**Wohnsitzadresse**" zu beurteilen. Die Kumulation der – gleichwertigen – Indizien der Registrierungsadresse und der IP-Adresse wird nicht gefordert. Mit dem Indiz der IP-Adresse kann dem Indiz der Registrierungsadresse auch nicht entgegengetreten werden. Daher besteht kein Erfordernis, die IP-Adresse zu ermitteln ([BFG 14.05.2025, RV/7100831/2020](#)).

### **Rechtsprechung der LVwG**

[LVwG NÖ 07.05.2025, LVwG-AV-1103/001-2024](#)

#### **KFZ, Zulassungsevidenz, Pressefreiheit, Art 6 Abs 1 lit e DSGVO**

- Ein Journalist beehrte Auskunft von der LPD NÖ über den **Zulassungsbesitzer** eines KFZ. Er begründete sein Auskunftsinteresse mit Recherchen zu möglichen Verstößen gegen das **Unvereinbarkeits- und Transparenzgesetz** sowie das **Parteiengesetz** iZm der Nutzung von Dienstfahrzeugen durch Politiker. Die LPD NÖ lehnte die Auskunftsanträge ab. Privatpersonen können zwar nach § 47 Abs 2a KFG Auskunft zu einem Kennzeichen verlangen, müssen jedoch ein rechtliches Interesse an der Auskunft nachweisen. Bei der Auskunft zu journalistischen Zwecken handelt es sich um kein im KFG genanntes rechtliches Interesse. Nach Ansicht des Journalisten müsse die Bestimmung des KFG iSd Art 20 Abs 4 B-VG verfassungskonform ausgelegt werden. Darüber hinaus müsse auch das AuskunftspflichtG beachtet werden. Gegen das Erkenntnis erhob der Journalist erfolglose Bescheidbeschwerde an das LVwG.

Das LVwG hat erwogen: Die Kraftfahrbehörde darf personenbezogene Daten gemäß § 47 Abs 2a KFG aus der **Zulassungsevidenz** bei Glaubhaftmachung eines **rechtlichen Interesses** an eine Privatperson herausgeben. Das rechtliche Interesse muss im **konkreten Einzelfall** begründet werden. Ein allgemeines Berufen auf ein journalistisches oder öffentliches Interesse reicht nicht aus. Bei der Zulassungsevidenz handelt es sich anders als beim Grundbuch um **kein** öffentliches Register. Die Auskunft kann nicht auf das **Auskunftspflichtgesetz** gestützt werden, weil dieses nur **subsidiär** zur Anwendung kommt. Wenn in einem Gesetz schon eine Auskunftspflicht geregelt ist, sind diese Regelungen bei der Auskunft zu beachten. Da die Bestimmung des § 47 KFG die



Auskunft abschließend regelt, ist das AuskunftspflichtG nicht anzuwenden.

Eine Bestimmung ist, wenn sie als Rechtsgrundlage iSd **Art 6 Abs 1 lit e iVm Abs 3 lit b DSGVO** herangezogen wird, **unionsrechtskonform** auszulegen. Eine Behörde hat **vor Herausgabe** personenbezogener Daten die Rechte der Betroffenen und die Grundsätze für die Verarbeitung iSd Art 5 Abs 1 DSGVO sicherzustellen. Eine allgemein auf die **Pressefreiheit** gestützte Herausgabe von staatlich verwalteten Daten, die lediglich den Zulassungsbesitzer betreffen, würde die Rechte des betroffenen Zulassungsbesitzers nicht in ausreichendem Maße schützen.

### Rechtsprechung der DSB

DSB 18.04.2025, 2025-0.303.076

#### **Schengener Informationssystem, Löschung**

- Ein Asylwerber beehrte vom **Bundesamt für Fremdenwesen und Asyl** die Löschung eines Eintrags im **Schengener Informationssystem (SIS)**, weil er bereits das Land verlassen habe und nun in Portugal wohne. Die portugiesischen Behörden hätten ihm einen Aufenthaltstitel und eine Arbeitserlaubnis in Aussicht gestellt, sofern er nicht mehr im SIS aufscheint. Das Bundesamt lehnte die Löschung ab. Die Löschung dürfe nur erfolgen, wenn die für die Eintragsentscheidung zuständige Behörde die Entscheidung, aufgrund derer der Eintrag gemacht wurde, zurücknimmt, für nichtig erklärt oder wenn ein Fremder den **Schengenraum** nachweislich verlassen hat. Aufgrund der Ablehnung fühlte sich der Asylwerber in seinem **Recht auf Löschung** verletzt und brachte erfolglose Datenschutzbeschwerde bei der DSB ein.

Die DSB hat erwogen: In Art 14 Abs 1 **SIS Rückkehr VO** sind die Möglichkeiten der Löschung von Einträgen angeführt. Die Voraussetzungen für die Löschung sind entweder die Rücknahme der Entscheidung der zuständigen Behörde oder ein Nachweis des Verlassens des **Schengenraums**. Wenn einem Asylwerber durch einen anderen Mitgliedstaat eine Aufenthaltsbewilligung oder ein Visum für einen längeren Aufenthalt gewährt wird, hat dieser den eintragenden Staat zu informieren. Der Zweck der Eintragung (Speicherung) im SIS gemäß Art 3 Abs 1 SIS-VO liegt darin, eine Überprüfung zu ermöglichen, ob der **Rückkehrverpflichtung** nachgekommen wurde und um die Vollstreckung der Rückkehrentscheidung zu unterstützen.

Die Datenverarbeitung im SIS ist rechtmäßig und es besteht **kein Lösgrund** iSd Art 6 und Art 8 bis Art 12 sowie Art 14 Abs 1

erster Satz SIS Rückkehr VO, weswegen keine Verletzung im Recht auf Löschung vorliegt.

### Aus der weiteren Rechtsprechung der DSB:

- Verantwortliche und Auftragsverarbeiter haben auf Anfrage mit der DSB zusammenzuarbeiten (**Mitwirkungspflicht**). Diese Mitwirkungspflicht ist **strafbewehrt**. Kommt der Verantwortliche seiner Mitwirkungspflicht nicht nach, verwirklicht er den **objektiven Tatbestand**. Der Verantwortliche verweigerte systematisch die Mitwirkung an Verfahren der DSB. Gegen ihn wurden deshalb bereits mehrere Geldbußen verhängt. Der Mitwirkungsverstoß erfolgte somit **vorsätzlich**. Die einschlägigen Verstöße waren zudem **erschwerend** zu berücksichtigen, weshalb die konkret verhängte Strafe iHv **EUR 16.000** tat- und schuldangemessen ist ([DSB 03.06.2025, 2025-0.177.424](#)).

### EU-Rechtsakte

- Am **10.06.2025** wurden folgende **drei** delegierte Verordnungen zur Ergänzung der "*VO (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über **Märkte für Kryptowerte** [...]*" (**MiCAR**) kundgemacht: Die (i) "*Delegierte Verordnung (EU) 2025/1140 der Kommission vom 27. Februar 2025 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch **technische Regulierungsstandards** zur Festlegung der über sämtliche **Kryptowerte-Dienstleistungen, Tätigkeiten, Aufträge und Geschäfte zu führenden Aufzeichnungen***", [ABI L 2025/1140](#); (ii) "*Delegierte Verordnung (EU) 2025/1141 der Kommission vom 27. Februar 2025 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch **technische Regulierungsstandards** zur Präzisierung der Anforderungen an Strategien und Verfahren zu **Interessenkonflikten für Emittenten vermögenswertereferenzierter Token***", [ABI L 2025/1141](#); und (iii) "*Delegierte Verordnung (EU) 2025/1142 der Kommission vom 27. Februar 2025 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch **technische Regulierungsstandards** zur Präzisierung der Anforderungen an Strategien und Verfahren zu **Interessenkonflikten für Anbieter von Kryptowerte-Dienstleistungen** und der Einzelheiten und Methoden für den Inhalt der Offenlegung von Interessenkonflikten*", [ABI L 2025/1142](#). In diesen drei delegierten Verordnungen werden zur Ergänzung der **MiCAR** technische Regulierungsstandards zu **Aufzeichnungspflichten** und **Interessenkonflikten** festgelegt. Die

Aufzeichnungspflichten umfassen sowohl Aufzeichnungsmodalitäten als auch Aufbewahrungspflichten.

- Am **06.06.2025** ist der "[Cyber Blueprint](#)", eine Empfehlung des **Rates**, angenommen worden. Ziel dieser Blaupause ist die Schaffung eines unionsweiten Rahmens für das **Cybersicherheitskrisenmanagement bei großangelegten Cybersicherheitsvorfällen**. Beschrieben werden Kooperationsmechanismen zwischen den verschiedenen involvierten Akteuren.

### **Nationale Rechtsakte**

- Am **12.06.2025** wurde das "*Oberösterreichische Informationstechnologien-Einsatz-Gesetz*" (**Oö ITEG**), [LGBl 2025/46](#), kundgemacht. Ziel ist die Förderung des Landtags, des Landesrechnungshofs, des LVwG sowie der Behörden und Dienststellen des Landes Oberösterreich, der oö Gemeinden und Gemeindeverbände sowie der sonstigen oö Körperschaften des öffentlichen Rechts bei der **digitalen Transformation**, dem Einsatz von **künstlicher Intelligenz** sowie bei **automatisierten Entscheidungen**. Insb soll die Beteiligung an **KI-Reallaboren** gefördert werden. Zudem dürfen Entscheidungen, die die genannten Einrichtungen als Träger von Privatrechten treffen, auf automatisierte Entscheidungen gestützt werden.

to the point

# Datenschutzmonitor. 25/2025 vom 25.06.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH 19.06.2025, C-509/23, *Laimz* (Geldwäsche, Glücksspiel, Datenschutzstrategien, Informationsaustausch, Identitätsfeststellung)

EuGH 19.06.2025, C-200/24, *Kommission/Polen (Publicité pour les pharmacies)* (reglementierte Berufe, Apotheken, Online-Werbung)

- **Rechtsprechung der Justiz**

OGH 22.05.2025, 4Ob28/25h; 26.05.2025, 8Ob11/25p; 27.05.2025, 9Ob22/25p; 27.05.2025, 9Ob26/25a; 27.05.2025, 9Ob7/25g; 27.05.2025, 9Ob9/25a (Smart Meter, einstweilige Verfügung, Sicherheitsleistung)

- **Rechtsprechung des BVwG**

BVwG 24.04.2025, W298 2310614-1 (Zuständigkeit, justizielle Tätigkeit, Notar, Gerichtskommissär)

BVwG 11.06.2025, W211 2308914-1 (Videoüberwachung, Transparenz, Geldbuße)

BVwG 06.05.2025, W254 2309877-1 (Kohärenzverfahren, Fristenhemmung)

BVwG 16.04.2025, W298 2310614-1 (Verfahrenshilfe)

- **EU-Rechtsakte**

Verfahrensverordnung zur DSGVO

EK Pressemitteilung 18.06.2025, IP/25/1551 (AliExpress, DSA)

## To the Point:

### Rechtsprechung des EuGH

Aus der Rechtsprechung des EuGH:

- Verpflichtete der **EU-Geldwäscherichtlinie**, wie **Glücksspielanbieter**, haben, wenn sie einer Gruppe angehören, **gruppenweite Datenschutzstrategien** sowie Strategien und Verfahren für den **Informationsaustausch** einzurichten. Ziel ist ua, eine wiederholte **Feststellung der Identität von Kunden** zu vermeiden. Die Mitgliedstaaten sind verpflichtet, innerhalb einer Gruppe einen Informationsaustausch zuzulassen ([EuGH 19.06.2025, C-509/23, Laimz](#)).
- Den Angehörigen **reglementierter Berufe**, wie des Berufs der **Apotheker**, darf nicht jede **Online-Werbung** verboten werden. Die **berufsrechtlichen Regeln** dürfen zwar Inhalt und Form der kommerziellen Kommunikation eingrenzen, sie dürfen Online-Werbung jedoch nicht verbieten ([EuGH 19.06.2025, C-200/24, Kommission/Polen \(Publicité pour les pharmacies\)](#)).

### Rechtsprechung der Justiz

Aus der Rechtsprechung der Justiz:

- Lehnt der Netzbenutzer den Austausch eines **"eichfälligen"** Zählers gegen ein intelligentes Messgerät ("**Smart Meter**") ab, darf der Netzbetreiber keine **Stromabschaltung** androhen. Dem Netzbetreiber steht es aber offen, gerichtliche Hilfe bei der Durchsetzung seines Interesses auf Tausch des Stromzählers in Anspruch zu nehmen. Die vom Rekursgericht erlassene **einstweilige Verfügung** zugunsten des Netzbenutzers wird bestätigt. Sie wird jedoch ungültig, wenn der Netzbenutzer beim Erstgericht keine **Sicherheitsleistung** iHv EUR 10.000 erlegt ([OGH 22.05.2025, 4Ob28/25h](#); [26.05.2025, 8Ob11/25p](#); [27.05.2025, 9Ob22/25p](#); [27.05.2025, 9Ob26/25a](#); [27.05.2025, 9Ob7/25g](#); [27.05.2025, 9Ob9/25a](#)).

### Rechtsprechung des BVwG

[BVwG 24.04.2025, W298 2310614-1](#)

#### **Zuständigkeit, justizielle Tätigkeit, Notar, Gerichtskommissär**

- Ein potenzieller Erbe verlangte Akteneinsicht von dem mit der Verlassenschaftsabwicklung betrauten Notar. Nachdem dieser die Akteneinsicht verweigerte, brachte der Erbe Datenschutzbeschwerde wegen Nichterteilen der Auskunft bei der DSB ein. Als Erbe stünde ihm auch ohne Erbantrittserklärung ein Recht auf Akteneinsicht zu, weshalb er gemäß Art 15 DSGVO Einsicht zu den entsprechenden Verfahrensdaten verlange. Die DSB wies die Datenschutzbeschwerde ab.

Ein Auskunftersuchen müsse ein Mindestmaß an Inhalt aufweisen, um die Geltendmachung eines Betroffenenrechts zu erkennen. Der Erbe habe dem Notar gegenüber aber ausschließlich die Akteneinsicht begehrt und keine Auskunft nach Art 15 DSGVO verlangt.

Dagegen erhob der Erbe Bescheidbeschwerde an das BVwG. Mit einem Begehren auf Akteneinsicht sei zwangsläufig auch ein Auskunftersuchen verbunden. Das BVwG wies die Bescheidbeschwerde ab und änderte den Spruch des Bescheids der DSB dahingehend ab, dass die Datenschutzbeschwerde zurückgewiesen wird.

Das BVwG hat erwogen: Die DSB ist für Beschwerden über die Verweigerung der Erfüllung von Betroffenenrechten im Rahmen der Ausübung von **justizieller Tätigkeit** eines Gerichts oder gerichtlichen Organs **unzuständig**. Die justizielle Tätigkeit ist ein unionsrechtlicher Begriff, der im österreichischen Rechtsverständnis teilweise die Akte der Gerichtsbarkeit und auch der Justizverwaltung umfasst. Im Verlassenschaftsverfahren wird der Notar **ex lege** gemäß § 1 Abs 2 NO iVm § 1 Abs 1 und § 2 Abs 1 GKG als **Gerichtskommissär** tätig. Funktional betrachtet handelt es sich bei dem Notar in dieser Rolle um ein gerichtliches bzw hoheitliches Organ. Datenverarbeitungen in diesem Zusammenhang fallen unter den Begriff der "justiziellen Tätigkeit" gemäß Art 55 Abs 3 DSGVO. Somit ist die DSB für die datenschutzrechtliche Kontrolle der Tätigkeiten des Notars als Gerichtskommissär **unzuständig**. Eine datenschutzrechtliche Kontrolle dieser Tätigkeit durch die DSB ist ein **unzulässiger Eingriff** in die richterliche Unabhängigkeit, weil sie geeignet ist, gerichtliche Entscheidungen zumindest mittelbar zu beeinflussen.

Die Kontrolle von Datenschutzverletzungen im Rahmen justizieller Tätigkeit ist gemäß § 85 Abs 1 und 2 GOG **ausschließlich** den **ordentlichen Gerichten** vorbehalten. Für die Entscheidung über eine Beschwerde ist das im Instanzenzug übergeordnete Gericht zuständig. Da es sich bei Verlassenschaftsverfahren gemäß § 104a JN um Außerstreitsachen handelt, ist in diesem Fall das **örtlich zuständige Landesgericht** zuständig.

[BVwG 11.06.2025, W211 2308914-1](#)

#### **Videüberwachung, Transparenz, Geldbuße**

- Ein Unternehmen beauftragte eine Auftragsverarbeiterin mit der Errichtung eines videobasierten Personenzählsystems, um Besuchermengen zu ermitteln. Hierfür wurden 27 Videokameras im öffentlichen Raum einer Stadt montiert, wobei keine Kennzeichnung erfolgte. In Folge wurde die Personenzählung zu einer Frequenzmessung umgebaut. Die Kameras nahmen in Echtzeit auf

und generierten digitales Bildmaterial, das an ein Computersystem eines externen Technologieunternehmens weitergeleitet und dort durch spezielle Software in Echtzeit analysiert und in Textdaten umgewandelt wurde. Die Bilddaten wurden dabei nach maximal 50 Millisekunden im Arbeitsspeicher gelöscht, eine Speicherung des Bildmaterials erfolgte nicht. Die Livebilder konnten von der Auftragsverarbeiterin und dem Technologieunternehmen betrachtet werden, der Zugriff war jedoch beschränkt, weil zunächst ein Port freigeschalten werden musste. Zudem wurden solche Zugriffe protokolliert. Die durch die Besucherstromanalyse bzw. Frequenzanalyse gewonnenen Daten sollten der Planung, Organisation und Durchführung von Events und Marketingmaßnahmen dienen. Die DSB verhängte eine Geldbuße iHv EUR 19.200. Daraufhin erhob das Unternehmen eine erfolglose Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die Videoüberwachung durch das Unternehmen ist eine Verarbeitung personenbezogener Daten. **Marketinginteressen** können grundsätzlich ein berechtigtes Interesse iSd Art 6 DSGVO sein, jedoch war die Aufzeichnung durch 27 Kameras über 24 Stunden am Tag unverhältnismäßig und überschritt den erforderlichen Umfang. Dem Unternehmen standen weniger eingriffsintensive Alternativen zur Verfügung, wie zB analoge Zählsysteme. Zudem wurden die **Kameras nicht gekennzeichnet**. Damit handelt es sich jedenfalls um eine **exzessive** und unverhältnismäßige **Datenverarbeitung**. Das Geheimhaltungsinteresse der Betroffenen überwiegt das Marketinginteresse des Unternehmens.

iSd **Transparenzgrundsatzes** muss gemäß Art 13 und 14 DSGVO für Betroffene erkennbar sein, dass personenbezogene Daten verarbeitet werden, welche Daten verarbeitet werden, für welche Zwecke sie verarbeitet werden und durch wen sie verarbeitet werden. Diese Informationen müssen gemäß Art 12 DSGVO präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache erteilt werden. Bei Videokameras kann etwa in einem ersten Schritt durch eine **Beschilderung** auf die Datenverarbeitung hingewiesen werden. Während die wichtigsten Informationen in einem **Warnhinweis** dargestellt werden sollten, können notwendige weitere Informationen in einem **zweiten Schritt** mit anderen Mitteln zur Verfügung gestellt werden. Das Unternehmen hat es unterlassen, auf die durchgeführte Datenverarbeitung hinzuweisen. Damit hat es den Betroffenen **erschwert**, ihre Rechte iSd Art 15 DSGVO auszuüben.

Für die **Strafbarkeit einer juristischen Person** genügt ein Verschulden in Form von Vorsatz oder Fahrlässigkeit. Das Unternehmen beschäftigte sich nur oberflächlich mit

datenschutzrechtlichen Fragen und handelte dabei **leicht fahrlässig**.

Die **Geldstrafe** ist nach Art 83 DSGVO **zu bemessen**, sie muss wirksam, verhältnismäßig und abschreckend sein. Das Unternehmen ist ein Unternehmen der kleinsten Kategorie, der Schweregrad des Verstoßes ist leicht, aber es liegt ein **gravierender Eingriff** in die Grundrechte auf Datenschutz und Privatsphäre einer großen Zahl von Betroffenen über einen langen Zeitraum vor.

**Strafmildernd** zu berücksichtigen ist, dass keine früheren Verstöße des Unternehmens gegen die DSGVO vorlagen und das Unternehmen im Verfahren kooperativ mitgewirkt hat. Die Geldstrafe ist von EUR 19.200 auf EUR 7.000 zu reduzieren. **Anm: Das Erkenntnis des BVwG im vorangegangenen amtswegigen Prüfverfahren kann im [Datenschutzmonitor vom 21.05.2025](#) nachgelesen werden.**

#### Aus der weiteren Rechtsprechung des BVwG:

- Gemäß § 73 Abs 1 AVG sind Behörden verpflichtet, über Parteienanträge ohne unnötigen Aufschub, spätestens aber sechs Monate nach deren Einlangen, zu entscheiden. Laut § 24 Abs 10 Z 2 DSG ist die Zeit während eines **Kohärenzverfahrens** gemäß Art 56, 60 und 63 DSGVO in die Entscheidungsfrist des § 73 AVG nicht einzurechnen. Die **Frist** ist während der federführenden Zuständigkeit der ausländischen Aufsichtsbehörde **gehemmt**. Das Verfahren über eine Datenschutzbeschwerde iZm **grenzüberschreitender Datenverarbeitung** besteht aus **drei Phasen**: Zuerst bestimmen die beteiligten Aufsichtsbehörden ihre jeweilige Rolle nach Art 56 DSGVO. Danach führt die federführende Aufsichtsbehörde das **Kohärenzverfahren** nach Art 60 DSGVO durch und fasst einen **verbindlichen Beschluss**. Im letzten Schritt erlässt die Aufsichtsbehörde, bei der die Datenschutzbeschwerde eingebracht wurde, den Bescheid hinsichtlich abweisender oder ablehnender Spruchpunkte ([BVwG 06.05.2025, W254 2309877-1](#)).
- Erscheint die Rechtsverfolgung oder Rechtsverteidigung aussichtslos, ist **keine Verfahrenshilfe** zu bewilligen. Da die DSB für die datenschutzrechtliche Kontrolle von **justizieller Tätigkeit**, die in der gerichtskommissarischen Betrauung eines öffentlichen Notars liegt, unzuständig ist, erscheint die Rechtsverfolgung **aussichtslos** und ist die Verfahrenshilfe nicht zu bewilligen ([BVwG 16.04.2025, W298 2310614-1](#)).

## **EU-Rechtsakte**

- Am **16.06.2025** erzielten der Rat und das Europäische Parlament eine vorläufige Einigung über den Entwurf der neuen **Verfahrensverordnung zur DSGVO**, [COM\(2023\) 348 final](#). Mit dieser Verordnung soll die Zulässigkeit **grenzüberschreitender Datenschutzbeschwerden** harmonisiert werden. Vereinbart wurden ua Fristen und Mechanismen im **Kohärenzverfahren** ([Pressemitteilung des Rates](#); [Pressemitteilung des EP](#)).
- Am **18.06.2025** veröffentlichte die **Europäische Kommission (EK)** eine Pressemitteilung, in der sie mitteilte, von **AliExpress** angebotene Verpflichtungen zur Einhaltung des Gesetzes über digitale Dienste (**DSA**) zu akzeptieren, und gleichzeitig Verstöße von AliExpress hinsichtlich der Verbreitung illegaler Produkte festgestellt zu haben. Durch die von AliExpress angebotenen und verbindlich gemachten Verpflichtungen hofft die Kommission, ua die Transparenz der Plattform betreffend **Werbe- und Empfehlungssystem** zu erhöhen ([EK Pressemitteilung 18.06.2025, IP/25/1551](#)).

to the point

# Datenschutzmonitor. 26/2025 vom 02.07.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH 26.06.2025, C-555/23, *Makeleio* (Audiovisuelle Medien, Grundsatz der Rechtssicherheit bei der Verhängung von Strafen)

EuGH SA 19.06.2025, C-738/22 P, *Google/Kommission* (kartellrechtliche Geldbuße, Android, Google Suche und Chrome)

- **Rechtsprechung des VfGH**

VfGH 16.06.2025, G55/2025 (Gesetzesprüfungsverfahren, Beweisverwertung, StPO)

- **Rechtsprechung des BVwG**

BVwG 14.04.2025, W137 2257572-1 (Kreditinstitut, Datenlöschung, Sorgfaltspflicht, öffentliches Interesse)

BVwG 09.04.2025, W287 2271595-1 (Direktmarketingunternehmen, Löschungersuchen, Sperrdatei)

BVwG 22.04.2025, W256 2248647-1 (Gesundheitsdaten, Krankenanstalt, Übermittlungsform)

BVwG 07.04.2025, W108 2283036-1 (Exzess, Missbrauchsabsicht)

BVwG 17.04.2025, W605 2257579-1 (Bilddatenverarbeitung, Öffnungsklausel, gelindere Mittel)

BVwG 23.04.2025, W291 2299266-1 (Cookie-Banner, Leistungsauftrag)

BVwG 02.12.2024, W254 2299670-1 (Datenschutzbeschwerde, Mindestinhalt, Verbesserungsauftrag)

- **Rechtsprechung der DSB**

DSB 04.07.2024, 2024-0.199.724 (Rechnungshof, politische Meinung, Parteiengesetz, Zuständigkeit, Parlamentarisches Datenschutzkomitee)

DSB 12.06.2024, 2023-0.836.312 (justizielle Tätigkeit, Zuständigkeit, Beschwerdegegner, Übermaßverbot)

- **EU-Rechtsakte**

Durchführungsbeschlüsse (EU) 2025/1225 und (EU) 2025/1226 zum UK-Angemessenheitsbeschluss

Draft implementing regulation for fair use for inter EU communication

## To the Point:

### Rechtsprechung des EuGH

Aus der Rechtsprechung des EuGH:

- Anbieter von **Online-Fernsehdiensten** sind Mediendiensteanbieter iSd Richtlinie über **audiovisuelle Mediendienste** ([RL 2010/13/EU](#)). Kurze Videos, die auf der Website einer Zeitung angeboten werden, sind Sendungen iS dieser RL, wenn die Bereitstellung der Videos **eigenständig** erfolgt. Nach der Richtlinie über audiovisuelle Mediendienste sind die Mitgliedstaaten verpflichtet, die **Menschenwürde** zu schützen, sodass keine Inhalte ausgestrahlt werden dürfen, die die Menschenwürde beeinträchtigen. Die **unionsrechtskonforme Auslegung** verlangt eine **weite Auslegung** innerstaatlicher Rechtsvorschriften, um die volle Wirksamkeit des Unionsrechts zu gewährleisten. Die unionsrechtskonforme Auslegung ist jedoch durch die besondere Ausprägung des allgemeinen **Grundsatzes der Rechtssicherheit** iZm **Straftaten** und **Strafen begrenzt**. Dies gilt auch für Sanktionen **ohne strafrechtlichen Charakter** ([EuGH 26.06.2025, C-555/23, Makeleio](#)).
- Die Generalanwältin schlägt dem EuGH in ihren Schlussanträgen vor, das Urteil des EuG zu bestätigen, mit dem das EuG eine Geldbuße iHv **EUR 4,125 Mrd** gegen **Google** verhängt hat. Google wird der Missbrauch einer marktbeherrschenden Stellung iZm dem **Betriebssystem Android** sowie den Anwendungen **Google Search**, **Google Chrome** und **Google Play Store** vorgeworfen ([EuGH SA 19.06.2025, C-738/22 P, Google/Kommission](#)).

### Rechtsprechung des VfGH

Aus der Rechtsprechung des VfGH:

- Im **Gesetzesprüfungsverfahren** darf der Umfang der in Prüfung gezogenen Norm nicht **zu eng gewählt** werden. Die Anfechtung nur der §§ 134 Z 3 und 135 Abs 3 StPO (Überwachung von Nachrichten) ist zu eng gewählt, weil sich der Gesetzesprüfungsantrag in der Sache nicht gegen die Überwachung von Nachrichten durch österreichische Behörden, sondern gegen die **Verwertung der Ermittlungsergebnisse ausländischer Behörden**, die der StPO nicht unterliegen, richtet. Der Antragsteller hätte auch jene Bestimmungen anfechten müssen, die die **Beweisverwertung** im strafgerichtlichen Verfahren regeln, nämlich insb § 140 Abs 1 StPO und allenfalls § 55d Abs 7 iVm § 55a Abs 1 Z 13 EU-JZG. Da der Antragsteller nur die §§ 134 Z 3 und 135 Abs 3 StPO angefochten hat, ist der Antrag zurückzuweisen ([VfGH 16.06.2025, G55/2025](#)).

### Rechtsprechung des BVwG

BVwG 14.04.2025, W137 2257572-1

#### **Kreditinstitut, Datenlöschung, Sorgfaltspflicht, öffentliches Interesse**

- Ein Kunde eröffnete bei einem Kreditinstitut ein Konto und stellte einen Monat später einen Antrag auf Ausstellung einer Kreditkarte. Zum Nachweis ausreichender Bonität ersuchte das Kreditinstitut um Übermittlung der Gehaltszettel der vorangegangenen drei Monate und der Kontoumsätze des alten Gehaltskontos. Der Kunde übermittelte die angeforderten Unterlagen nicht und zog seinen Antrag auf Ausstellung einer Kreditkarte zurück. Zusätzlich stellte er ein Ersuchen um Löschung der im Zuge der Antragstellung übermittelten Daten. Das Kreditinstitut verweigerte die Löschung mit Verweis auf anwendbare Sorgfaltspflichten gemäß dem Finanzmarkt-Geldwäschegesetz (**FM-GwG**) zur Verhinderung von Geldwäsche und Terrorismusfinanzierung. Der Kunde erhob daraufhin Datenschutzbeschwerde bei der DSB, welche der Datenschutzbeschwerde stattgab. Da es gegenständlich aufgrund der Antragszurückziehung zu keiner Begründung einer zusätzlichen dauerhaften Geschäftsbeziehung gekommen sei, seien die Sorgfaltspflichten nicht anwendbar. Die Daten seien daher zu löschen. Dagegen erhob das Kreditinstitut (erfolgreich) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die Verarbeitung personenbezogener Daten zu **Zwecken der Verhinderung von Geldwäsche und Terrorismusfinanzierung** ist als Angelegenheit im **öffentlichen Interesse** gemäß der DSGVO anzusehen. Verpflichtete müssen ausreichend Informationen zur Identität ihrer Kunden und deren wirtschaftlich Berechtigten, zum Zweck und zur Art der angestrebten Geschäftsbeziehung und zur Herkunft der eingesetzten Mittel eingeholt haben, diese Informationen regelmäßig aktualisieren und die Geschäftsbeziehung kontinuierlich überwachen. Wenn der Kunde einen Anlass gibt, dann sind seine Unterlagen zu aktualisieren. Dies trifft bereits zu, wenn die verpflichtete Bank auf irgendeine andere Art und Weise Kenntnis von einer Änderung erlangt. Dies war durch den gestellten und wieder zurückgezogenen Kreditkartenantrag der Fall.

Die **Geschäftsbeziehung** mit dem Kunden ist die Summe aller bestehenden auf Dauer angelegten Vertragsbeziehungen zwischen dem Kreditinstitut und dem Kunden (zB Konto, Depot, Kredit, Safe). Somit ist betreffend Sorgfaltspflichten ausschlaggebend, bis zu welchem Zeitpunkt eine durchgängige Geschäftsbeziehung (ohne Unterbrechung) mit dem Kunden bestand, und zwar unabhängig von den einzelnen Produkten. Die im Zusammenhang mit dem Kreditkartenantrag



verarbeiteten Daten fallen daher bereits unter die Sorgfaltspflichten des Kreditinstituts. Erst nach Beendigung der letzten dauerhaften Geschäftsbeziehung (hier: Konto) beginnt die **Löschfrist** zu laufen. Die Datenspeicherung war daher rechtmäßig.

BVwG 09.04.2025, W287 2271595-1

### **Direktmarketingunternehmen, Löschungsersuchen, Sperrdatei**

- Eine Betroffene forderte bei einem **Direktmarketingunternehmen** die **Löschung** ihrer Daten und erhielt eine Bestätigung über die vollständige Löschung. Drei Jahre später stellte die Betroffene ein Auskunftersuchen und erfuhr, dass ihre Daten nach der Löschung wieder erhoben und verarbeitet wurden. Sie beantragte daraufhin erneut die Löschung und widersprach der Verarbeitung ihrer Daten. Die DSB gab der Datenschutzbeschwerde statt und stellte fest, dass das Direktmarketingunternehmen die Betroffene in ihrem Recht auf Geheimhaltung verletzt habe, weil es ihre Daten trotz des erhobenen Widerspruchs erneut für Direktmarketingzwecke verwendet und damit unrechtmäßig verarbeitet habe. Das Direktmarketingunternehmen erhob (erfolglose) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die Verarbeitung zu Zwecken der Direktwerbung kann ein berechtigtes Interesse sein, erfordert jedoch eine **Interessenabwägung**. Widerspricht die Betroffene der Verarbeitung zu Werbezwecken, dürfen die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet werden. Zudem hat die Betroffene ein Recht auf Löschung, wenn sie Widerspruch erhoben hat.

Gemäß **§ 151 Abs 8 GewO** muss die Löschung in Form einer Sperrung der Verwendung dieser Daten für Marketingaussendungen erfolgen, wenn die Betroffene nicht auf die **physische Löschung** ihrer Daten besteht. § 151 Abs 8 GewO dient dazu, Situationen zu verhindern, in denen Betroffene ihr Löschungsrecht wahrnehmen und dann dennoch von einer erneuten Datenverarbeitung betroffen sind.

Das an das Direktmarketingunternehmen gerichtete Löscher- und Widerspruchersuchen war nicht eindeutig als Löscherersuchen aller verarbeiteten Daten zu interpretieren, sondern bezog sich vielmehr darauf, die Daten nicht mehr für Werbezwecke zu verarbeiten. Das Direktmarketingunternehmen hätte daher den **wahren Willen** der Betroffenen eruieren müssen, sie auf die **Folgen der Löschung** unter gleichzeitiger Darlegung der Möglichkeit der Überführung der zur Identifizierung erforderlichen (Stamm-)Daten in eine **Sperrdatei** hinweisen und in Erfahrung bringen müssen, ob sie dennoch auf eine gänzliche Löschung ihrer

Daten besteht. Nur wenn die Betroffene weiterhin die Löschung aller Daten verlangt hätte, wäre diese vorzunehmen gewesen.

Das Direktmarketingunternehmen unterließ diese **Aufklärung iSd § 151 Abs 8 GewO**. Es hätte daher die Verarbeitung der Daten nur sperren dürfen. Die **Verletzung von Informationspflichten** hat zwar grundsätzlich **keine Auswirkung auf die Rechtmäßigkeit** der Verarbeitung. Die Betroffene konnte jedoch mangels Belehrung und Begründung ihres wahren Willens die Nachteile einer vollständigen Löschung im Vergleich zu einer Überführung in eine Sperrdatei nicht abschätzen, sodass ihre Willensbildung beeinträchtigt war.

Die Betroffene durfte darauf **vertrauen**, dass ihre Daten nicht erneut für Direktmarketingzwecke verarbeitet werden. Diese **Erwartungshaltung** muss im Rahmen der Interessenabwägung im Zuge der neuerlichen Datenerhebung zugunsten der Betroffenen berücksichtigt werden. Die neuerliche Erhebung und Verarbeitung verstieß daher gegen Art 5 Abs 1 lit a iVm Art 6 Abs 1 lit f DSGVO und war somit rechtswidrig.

BVwG 22.04.2025, W256 2248647-1

### **Gesundheitsdaten, Krankenhaus, Übermittlungsform**

- Eine Patientin absolvierte nach einer Hüftoperation ein Anschlussheilverfahren in einem Rehabilitationszentrum, das von der Versicherungsanstalt öffentlich Bediensteter, Eisenbahnen und Bergbau (**BVAEB**) betrieben wird. Zum Zeitpunkt des Aufenthalts war die Patientin 77 Jahre alt. Aufgrund zweier früherer Gehirnoperationen war sie kognitiv signifikant eingeschränkt, was dem ärztlichen Team des Rehabilitationszentrums bekannt war. Bei Antritt des Anschlussheilverfahrens brachte die Patientin keine medizinischen Befunde mit und verwies auf ihren Ehemann als Vertreter sowie auf ihre Hausärztin. Ihr Ehemann übergab dem ärztlichen Team in der Folge radiologische Bilder, wobei zu einem MRT-Bild des Schädels der Befund fehlte. Da das ärztliche Team den fehlenden Befundteil für die Beurteilung des Gesundheitszustands als wichtig erachtete, forderte es den neurologischen Befund bei dem radiologischen Institut an und erhielt ihn per Fax zugestellt.

Nach dem Anschlussheilverfahren verlangte die Patientin vom Rehabilitationszentrum die Übermittlung ihrer Befunde per E-Mail und erteilte dafür ihre Zustimmung. Das Rehabilitationszentrum lehnte dies jedoch wegen mangelnder Sicherheit des Übertragungswegs ab und sendete die Befunde postalisch zu. Die Patientin erhob daraufhin eine Datenschutzbeschwerde bei der DSB, weil sie sich durch die Abfrage bezüglich des fehlenden Befundteils und durch die Nichtzustellung

der Befunde per E-Mail in ihrem Recht auf Datenschutz als verletzt erachtete. Die Bescheidbeschwerde der Patientin gegen den abweisenden Bescheid der DSB an das BVwG blieb erfolglos.

Das BVwG hat erwogen: Die DSGVO schützt personenbezogene Daten und gewährt Betroffenen bestimmte Rechte, darunter auch das Recht auf Auskunft. Die DSGVO enthält jedoch **kein eigenständiges Recht** auf Erhalt personenbezogener Daten in einer **bestimmten Form**. Die Übermittlung der Befunde per Post verletzt somit kein Recht der Patientin.

Bei dem eingeholten neurologischen Befund handelt es sich um **gesundheitsbezogene Daten**, die grundsätzlich einem Verarbeitungsverbot gemäß Art 9 Abs 1 DSGVO unterliegen. **Art 9 Abs 2 lit h DSGVO** erlaubt jedoch die Verarbeitung von Gesundheitsdaten ohne Einwilligung, wenn sie für Zwecke der Gesundheitsvorsorge, medizinischen Diagnostik, Versorgung oder Behandlung erforderlich ist. Bei der Verarbeitung von sensiblen Daten muss eine gesetzliche Anordnung bzw Erlaubnis vorliegen, die Verarbeitung muss erforderlich sein und die Anforderungen des Art 9 Abs 3 DSGVO müssen erfüllt sein, wonach die Verarbeitung durch Fachpersonal, das einer Verschwiegenheitspflicht unterliegt, erfolgen muss.

Mit Blick auf die klaren Regelungen der § 17 und § 20 NÖ Krankenanstaltengesetz erfüllt das tätig gewordene **ärztliche Team** zweifellos die Voraussetzungen des Art 9 Abs 3 DSGVO. Das Rehabilitationszentrum ist als **Sonderkrankenanstalt** gemäß §§ 16b ff, § 21 NÖ Krankenanstaltengesetz verpflichtet, eine ordnungsgemäße **Behandlung und Dokumentation** sicherzustellen. Die Behandlungspflicht umfasst die Berücksichtigung aller relevanten medizinischen Faktoren, um damit eine umfassende und bestmögliche Betreuung der Patienten gewährleisten zu können.

Für eine **optimale Nachbehandlung** nach einer Hüftoperation war die Einholung des neurologischen Befundes **erforderlich**, weil das zentrale Nervensystem für die Steuerung des Bewegungsapparats zuständig ist. Die abstrakte Möglichkeit einer für die Behandlung nachteiligen Störung rechtfertigt die medizinische Abklärung durch Einholung des Befundes. Die Erforderlichkeit der Abklärung hängt nicht davon ab, ob tatsächlich eine Störung vorliegt, sondern schon der Ausschluss einer solchen Störung ist für die Behandlung entscheidend. Die Einholung des neurologischen Befundes war im Interesse der Patientin und erforderlich.

#### Aus der weiteren Rechtsprechung des BVwG:

- Datenschutzbeschwerden sind nicht allein aufgrund ihrer Zahl während eines

bestimmten Zeitraums als **exzessiv** iSv Art 57 Abs 4 DSGVO einzustufen. Auch kann sich die DSB nicht auf die **erhebliche Inanspruchnahme ihrer Ressourcen und Beeinträchtigung** ihrer anderen Aufgaben stützen, um eine inhaltliche Auseinandersetzung zu verweigern. Für das Vorliegen eines Exzesses muss **Missbrauchsabsicht** vorliegen, welche nur dann gegeben ist, wenn das **unlautere Motiv der Rechtsausübung das lautere Motiv eindeutig überwiegt**. Der **Schädigungszweck** muss so **augenscheinlich** im Vordergrund stehen, dass andere Ziele der Rechtsausübung völlig in den Hintergrund treten. Der DSB gelang der **Nachweis der Missbrauchsabsicht** nicht ([BVwG 07.04.2025, W108 2283036-1](#)).

- Die **§§ 12 und 13 DSGVO** sind mangels **Öffnungsklausel** der DSGVO nicht anwendbar. Eine **Bilddatenverarbeitung** durch Videokameras ist daher allein anhand von Art 6 DSGVO zu beurteilen. Eine Videoüberwachung ist rechtswidrig, wenn ein berechtigtes Interesse am Schutz des Eigentums zwar besteht, dem Verantwortlichen aber **gelingendere Mittel** zur Verfügung stehen ([BVwG 17.04.2025, W605 2257579-1](#)).
- Trägt die DSB einem Websitebetreiber auf, seinen **Cookie-Banner** derart abzuändern, dass auf der ersten Ebene des Cookie-Banners neben der Option "Akzeptieren" eine optisch gleichwertige Option vorhanden ist, um den Cookie-Banner ohne Abgabe einer Einwilligung zu schließen, kann diesem Leistungsauftrag **während des laufenden Verfahrens** vor dem BVwG entsprochen werden. Dadurch entfällt die Grundlage für den **Leistungsauftrag**, weshalb dieser vom BVwG zu beheben ist ([BVwG 23.04.2025, W291 2299266-1](#)).
- Ist der Beschwerdegegner unklar oder ist der **Datenschutzbeschwerde** nicht zu entnehmen, welcher Sachverhalt ihr zugrunde gelegt wird, ist der geforderte **Mindestinhalt** der Datenschutzbeschwerde gemäß § 24 Abs 2 Z 2 und Z 3 DSGVO nicht erfüllt. Entspricht der Beschwerdeführer einem aus diesen Gründen gestellten **Verbesserungsauftrag** nicht, ist die Datenschutzbeschwerde zurückzuweisen. Die Zurückweisung der Datenschutzbeschwerde steht der neuerlichen mangelfreien Beschwerdeerhebung nicht entgegen ([BVwG 02.12.2024, W254 2299670-1](#)).

#### **Rechtsprechung der DSB**

DSB 04.07.2024, 2024-0.199.724

#### **Rechnungshof, politische Meinung, Parteiengesetz, Zuständigkeit, Parlamentarisches Datenschutzkomitee**

- Ein Spender einer österreichischen Partei erhob Datenschutzbeschwerde bei der DSB,

weil der **Rechnungshof Österreich ("RH")** seinen Namen und die Höhe seiner Parteispende auf Grundlage des Parteiengesetzes auf dessen Website veröffentlicht hatte. Er sah sich dadurch in seinem Recht auf Geheimhaltung verletzt, weil aus der Spende Rückschlüsse auf seine politische Meinung gezogen werden können. Nach Aussetzung des Verfahrens bis zur Entscheidung des EuGH (zu [C-33/22, Österreichische Datenschutzbehörde](#)) und anschließender Fortsetzung des Verfahrens wies die DSB die Datenschutzbeschwerde ab.

Die DSB hat erwogen: Für die Einhaltung des Datenschutzes im Bereich der Gesetzgebung, wozu der RH zählt, hat der Gesetzgeber mit dem **Parlamentarischen Datenschutzkomitee** eine eigene Aufsichtsbehörde geschaffen. Da dieses Komitee erst mit dem 01.01.2025 eingerichtet wird, ist zum Zeitpunkt dieser Entscheidung noch die DSB zuständig.

Der RH handelt als Verantwortlicher im Sinne der DSGVO. Die Veröffentlichung personenbezogener Daten (Name, Spendentätigkeit, Postleitzahl) ist eine Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art 9 Abs 1 DSGVO, weil aus diesen Daten die **politische Meinung** hervorgehen kann. Eine Verarbeitung ist nur aufgrund der Ausnahmebestimmungen des Art 9 Abs 2 DSGVO zulässig. Art 9 Abs 2 lit g DSGVO erlaubt eine Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses, sofern diese verhältnismäßig ist und angemessene und spezifische Maßnahmen zum Schutz der Betroffenen vorsieht. Die **Transparenz der Parteienfinanzierung** ist ein **erhebliches öffentliches Interesse**.

Das **Parteiengesetz** sieht eine stufenweise Veröffentlichungspflicht vor: Ab EUR 150 ist der Name an den Rechnungshof zu melden, ab EUR 500 zusätzlich die Postleitzahl, ab EUR 2.500 (im Wahlkampfzeitraum) auch die Anschrift. Die Veröffentlichung erfolgt jeweils abgestuft nach Höhe und Zeitpunkt der Spende. Der Gesetzgeber hat im **Gesetzgebungsverfahren** eine **Datenschutz-Folgenabschätzung** durchgeführt und Maßnahmen zur Wahrung der Grundrechte der Betroffenen vorgesehen, wie insb die Beschränkung der veröffentlichten Daten auf Name und Postleitzahl (statt vollständiger Adresse) sowie die Anordnung einer Löschfrist für die Namen der Spender. Die Veröffentlichungen sind geeignet und erforderlich, um Transparenz über die Finanzierung politischer Parteien herzustellen, mögliche Interessenkonflikte offenzulegen und die Einhaltung von Compliance-Regeln zu ermöglichen. Das öffentliche Interesse an Transparenz überwiegt das Interesse des Spenders am Datenschutz.

DSB 12.06.2024, 2023-0.836.312

### **Justizielle Tätigkeit, Zuständigkeit, Beschwerdegegner, Übermaßverbot**

- Eine Rechtsanwältin sagte bei Gericht eine Hauptverhandlung krankheitsbedingt ab. Später stellte sich heraus, dass die Rechtsanwältin hatte eine Terminkollision hatte. Um diesen Umstand aufzuklären, nahm die zuständige Richterin eines Landesgerichts (**LG**) Einsicht in das zentrale Register "Verfahrensautomation Justiz" (**VJ-Register**) und kontaktierte die für das andere Verfahren zuständige Richterin. Als sich der Verdacht eines vorgetäuschten Krankenstands bestätigte, brachte sie eine Sachverhaltsdarstellung bei der zuständigen Rechtsanwaltskammer (**RAK**) ein. Die Rechtsanwältin fühlte sich durch die Einsicht in das VJ-Register durch die Richterin in ihrem Recht auf Geheimhaltung verletzt und brachte eine Datenschutzbeschwerde bei der DSB gegen die Richterin ein. Die DSB benannte als Zweitbeschwerdegegnerin das **LG**. Sie wies die Datenschutzbeschwerde gegen die Richterin ab und gegen das **LG** zurück.

Die DSB hat erwogen: **Parteienerklärungen**, worunter auch die **Bezeichnung des Beschwerdegegners** fallen, sind der **Einzelfallauslegung** zugänglich, weil § 24 DSG keine strengen Formerfordernisse vorsieht. Die DSB kann daher auch die Bezeichnung des Beschwerdegegners umdeuten bzw ein Verfahren gegen zwei Beschwerdegegner führen, obwohl nur ein Beschwerdegegner in der Datenschutzbeschwerde genannt ist, sofern dies interpretativ möglich ist.

Die Einsichtnahme in das VJ-Register erfolgte im Rahmen eines anhängigen Strafverfahrens. Die **DSB** ist gemäß § 31 Abs 1 DSG **nicht** für die **Aufsicht** über die von **Gerichten** im Rahmen ihrer **justiziellen Tätigkeit** vorgenommenen Verarbeitungen **zuständig**. Eine Tätigkeit eines Gerichts im Rahmen der justiziellen Tätigkeit liegt dann vor, wenn ein Richter in Ausübung des richterlichen Amtes handelt oder ein Richter oder ein Staatsanwalt sonst in Besorgung der übertragenen Amtsgeschäfte weisungsfrei gestellt ist.

Maßgeblich für die **Abgrenzung der justiziellen Tätigkeit** ist, ob eine datenschutzrechtliche **Kontrolle** die **Unabhängigkeit** der Richterinnen und Richter oder ihrer **Entscheidungen beeinträchtigen** könnte. Die Erhebung der Daten aus dem VJ-Register und das Gespräch mit einer Richterkollegin, um die Notwendigkeit der Abberaumung einer Hauptverhandlung zu prüfen und anschließend standesrechtliche Maßnahmen einzuleiten, stehen in **direktem Zusammenhang** mit einem **Strafverfahren**. Eine **Kontrolle** der Datenerhebung durch die DSB hätte einen **unmittelbaren Einfluss** auf die

**Unabhängigkeit** der richterlichen Entscheidung und fällt daher nicht in die Zuständigkeit der DSB.

Eine **eigenständige Verantwortung** der Richterin lag **nicht vor**, weil die Erhebungen in ihrer **Rolle als richterliches Organ** in Ausübung der justiziellen Tätigkeit erfolgten.

Auch könnte die Datenschutzbeschwerde aufgrund des **Übermaßverbots nicht erfolgreich** sein, weil die Kontrolle der Ermittlungsschritte einen **Eingriff** in die **sachliche Zuständigkeit** des Gerichts bewirken würde.

### EU-Rechtsakte

- Am **23.06.2025** wurde der [Entwurf einer Durchführungsverordnung](#) der Kommission zur [EU-Netzneutralitäts-Verordnung 2015/2120](#) veröffentlicht. Festgelegt werden sollen Bedingungen für eine **faire Nutzung** von **Auslandstelefonie** und SMS-Nachrichten innerhalb der EU.
- Am **26.06.2025** wurden der (i) "*Durchführungsbeschluss (EU) 2025/1225 der Kommission vom 24. Juni 2025 zur Änderung des Durchführungsbeschlusses (EU) 2021/1773 gemäß der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zur **Angemessenheit des Schutzes personenbezogener Daten** durch das Vereinigte Königreich*", [ABI L 2025/1225](#); sowie (ii) "*Durchführungsbeschluss (EU) 2025/1226 der Kommission vom 24. Juni 2025 zur Änderung des Durchführungsbeschlusses (EU) 2021/1772 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur **Angemessenheit des Schutzes personenbezogener Daten** durch das Vereinigte Königreich*", [ABI L 2025/1226](#), veröffentlicht. Mit diesen Durchführungsbeschlüssen werden die **Geltungsdauer** der für das Vereinigte Königreich geltenden **Angemessenheitsbeschlüsse** vom 27.06.2025 bis zum **27.12.2025** verlängert, sofern sie nicht erneut verlängert werden.

to the point

# Datenschutzmonitor. 27/2025 vom 09.07.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 01.07.2025, 6033/19, *AR/Vereinigtes Königreich* (Strafregisterauszug, Vorhersehbarkeit, Unschuldsvermutung)

- **Rechtsprechung des EuGH**

EuGH SA 03.06.2025, C-291/24, *Steiermärkische Bank und Sparkasse* (Geldwäsche, Haftung, juristische Person, Verjährung)

EuGH 03.07.2025, C-529/23 P, *Parlament/TC* (Parteienghör, Akteneinsicht, Datenspeicherung im Konfliktfall, Personalakte)

- **Rechtsprechung des VfGH**

VfGH 24.06.2025, E4624/2024 (ORF-Beitrags Service GmbH, Beitragsdaten, Massenverfahren)

- **Rechtsprechung des OGH**

OLG Graz 16.05.2025, 5R25/25y (Berichterstattung, Persönlichkeitsrecht, Bildnisschutz)

OGH 28.05.2025, 3Ob30/25w; 03.06.2025, 2Ob31/25k (Smart Meter, einstweilige Verfügung, Sicherheitsleistung)

- **Rechtsprechung des BVwG**

BVwG 02.05.2025, W137 2301309-1 (Universität, Videoaufnahme, Verordnung)

BVwG 28.04.2025, W211 2289521-1 (Rechtsanwalt, Exekution, justizielle Tätigkeit)

BVwG 30.04.2025, W171 2298465-1 (Krankentransport, Spendenbrief, Gesundheitsdaten, Zweckänderung)

BVwG 28.04.2025, W211 2283135-1 (Exzess, Missbrauchsabsicht, Ressourcen)

BVwG 29.04.2025, W101 2308679-1 (Kohärenzverfahren, Fristhemmung)

BVwG 23.05.2025, W605 2307742-1 (Untätigkeitsklage, Kohärenzverfahren, Nichtweiterleiten der Datenschutzbeschwerde)

BVwG 24.04.2025, W298 2309933-1 (res iudicata, Präklusion)

BVwG 23.04.2024, W605 2283487-1 (Berichtigung, Geschlechtsidentität, "Sanierung")

BVwG 02.05.2025, W256 2275267-1 (Zurückweisung der Bescheidbeschwerde)

BVwG 06.05.2025, W256 2307865-1 (Auskunftserteilung im laufenden Verfahren)

- **EU-Rechtsakte**

Delegierte Verordnung (EU) 2025/532 (zur Ergänzung der DORA)

Berichtigung der Verordnung (EU) 2024/2847 (Cyberresilienz-Verordnung)

Delegierte Verordnung über den Zugang zu Daten gemäß dem Gesetz über digitale Dienste (DSA-Datenzugangsportale)

- **Nationale Rechtsakte**

Änderung des Universitätsgesetzes 2002 sowie des Bildungsdokumentationsgesetzes 2020

DSB 30.06.2025, Leitfaden zum Informationsfreiheitsgesetz

## To the Point:

### Rechtsprechung des EGMR

EGMR 01.07.2025, 6033/19, AR/Vereinigtes Königreich

#### **Strafregisterauszug, Vorhersehbarkeit, Unschuldsumutung**

- Ein Brite, der damals als Taxifahrer tätig war, wurde wegen Vergewaltigung einer 17-jährigen Passagierin angeklagt. Nach einem Strafverfahren erfolgte ein Freispruch. In den folgenden Jahren beantragte er für Bewerbungen zwei erweiterte Führungszeugnisse (**Enhanced Criminal Record Certificates; "ECRC"**). Die ECRC enthielten Informationen über die damalige Anklage, den Prozessverlauf und den Freispruch.

Der Brite legte Einspruch gegen die Offenlegung dieser Daten im erweiterten Führungszeugnis ein. Die Behörde hielt an der Offenlegung fest. Die daraufhin erhobene Beschwerde wurde abgewiesen. Der zuständige Beamte begründete die Maßnahme mit dem Risiko, der Brite könne seine Stellung missbrauchen, um ähnliche Straftaten zu begehen. Der Brite beantragte die gerichtliche Überprüfung der Entscheidung und berief sich auf Art 6 Abs 2 und Art 8 EMRK. Das Gericht erachtete Art 8 EMRK für einschlägig, bewertete die Offenlegung jedoch als verhältnismäßig und geeignet zum Schutz junger und gefährdeter Personen. Eine Verletzung der **Unschuldsumutung** wurde nicht festgestellt (Art 6 Abs 2 EMRK). Nach erfolglosem Ausschöpfen des Rechtswegs erhob der Brite (erfolgreiche) Beschwerde an den EGMR.

Der EGMR hat erwogen: Die Offenlegung der Daten über die Anklage beruhte auf einem **unklaren rechtlichen Rahmen**. Das maßgebliche nationale Gesetz sah vor, dass leitende Polizeibeamte Informationen offenlegen durften, wenn sie diese für "relevant" hielten. Es fehlten jedoch klare Kriterien zur Ausübung dieses Ermessens. Der Brite konnte nicht **vorhersehen**, dass die Umstände seiner Anklage im Rahmen eines ECRC offengelegt würden. Zum fraglichen Zeitpunkt bestand weder eine gesetzliche noch eine hinreichend präzise behördliche Anleitung, wie dieses Ermessen auszuüben war.

Dies ermöglichte eine **willkürliche** und für Betroffene nicht vorhersehbare Offenlegung. Es fehlte insbesondere eine Anleitung zur Bewertung der Relevanz strittiger Vorwürfe, zur Form der Offenlegung sowie zu deren Auswirkungen auf potenzielle Entscheidungsinstanzen wie Arbeitgeber oder Genehmigungsbehörden.

**Bestrittene Vorwürfe** sind nur dann für einen potenziellen Arbeitgeber relevant, wenn sie zutreffen. Sind sie unbegründet, haben sie keinerlei Einfluss auf die Eignung eines

Bewerbers für die Stelle. Angesichts des Freispruchs des Briten bestanden erhebliche Zweifel an der Vergewaltigungsanzeige. Der Brite erhielt jedoch keine Gelegenheit zur **Stellungnahme** vor der Datenoffenlegung. Da keine ausreichenden Schutzvorkehrungen bestanden, entsprach die Offenlegung nicht den Anforderungen des Gesetzes.

Die **Feststellung der Rechtsverletzung** bietet einen hinreichenden Ausgleich für den erlittenen **immateriellen Schaden**, sodass kein Schadenersatz zugesprochen wird.

### Rechtsprechung des EuGH

EuGH SA 03.06.2025, C-291/24, Steiermärkische Bank und Sparkasse

#### **Geldwäsche, Haftung, juristische Person, Verjährung**

- Eine Bank wurde von der **Finanzmarktaufsichtsbehörde (FMA)** mit einer Sanktion belegt, weil sie in den Jahren 2017 bis 2019 Sorgfaltspflichten nach dem **Finanzmarkt-Geldwäschegesetz (FM-GwG)** verletzt habe. Die Bank sowie zwei natürliche Personen in leitender Funktion erhoben Beschwerde an das BVwG. Dieses legte dem EuGH die Frage vor, ob die österreichischen Regelungen, die die Haftung einer juristischen Person zwingend an die **Feststellung der schuldhaften Pflichtverletzung einer identifizierten natürlichen Person** in Führungsposition knüpfen, mit den Vorgaben der **EU-Geldwäscherichtlinie** (Richtlinie (EU) 2015/849 idgF) vereinbar sind. Das BVwG fragte auch, ob das Urteil des [EuGH vom 05.12.2023, C-807/21, Deutsche Wohnen](#), in dem der EuGH festgestellt hat, dass eine im deutschen Recht bestehende ähnliche Regelung der Haftung juristischer Personen den Bestimmungen der DSGVO widerspricht, auf den vorliegenden Fall übertragbar ist.

Die Generalanwältin hat erwogen: Die **Geldwäsche-RL** verlangt, dass Mitgliedstaaten sicherstellen, dass juristische Personen für Verstöße gegen geldwäscherechtliche Verpflichtungen verantwortlich gemacht werden können. Sie unterscheidet zwischen der **Haftung juristischer** und natürlicher **Personen** und sieht vor, dass Sanktionen gegen juristische Personen über die **Zurechnung** des Verhaltens einer natürlichen Person in einer Führungsposition verhängt werden können. Die österreichische Regelung, die eine Sanktionierung der juristischen Person nur zulässt, wenn zuvor die schuldhafte Pflichtverletzung einer konkret benannten natürlichen Person festgestellt wurde, steht nicht im Widerspruch zur RL. Diese verlangt nämlich nicht, dass die Schuld einer natürlichen Person zwingend festgestellt werden muss, schließt dies aber auch nicht aus. Die Mitgliedstaaten dürfen einen gewissen Grad an Verschulden einer **natürlichen Person**

**in Führungsposition** verlangen, solange die Haftung der juristischen Person in allen relevanten Fällen sichergestellt bleibt.

Die formellen Anforderungen des österreichischen Rechts, wonach die (i) verantwortliche natürliche Person im Verfahren Partei sei, (ii) im Spruch des Straferkenntnisses namentlich benannt werden muss, und (iii) ihr Verhalten der juristischen Person zugerechnet werden muss, sind mit der RL vereinbar. Das Urteil des EuGH in der Rs *Deutsche Wohnen* zur DSGVO ist **nicht übertragbar**, weil die DSGVO eine unmittelbare Haftung der juristischen Person vorsieht, während die Geldwäsche-RL ausdrücklich die Zurechnung über eine natürliche Person in einer Führungsposition regelt.

Die Festlegung angemessener **Verjährungsfristen** liegt im **Ermessen** der Mitgliedstaaten, solange die Ausübung durch das Unionsrecht verliehener Rechte nicht praktisch unmöglich oder übermäßig erschwert wird. Verjährungsfristen von **drei und fünf Jahren** sind mit dem Effektivitätsgrundsatz des Unionsrechts vereinbar.

EuGH 03.07.2025, C-529/23 P, *Parliament/TC*

#### **Parteienghör, Akteneinsicht, Datenspeicherung im Konfliktfall, Personalakte**

- Das Europäische Parlament (EP) forderte von einem Abgeordneten die Rückzahlung von Beträgen, die zu Unrecht für die Beschäftigung seines akkreditierten parlamentarischen Assistenten gezahlt worden seien. Zur Verteidigung ersuchte der Abgeordnete das EP um die Übermittlung von Unterlagen, darunter die Personalakte und E-Mail-Korrespondenz mit dem Assistenten. Das EP verweigerte dies, woraufhin der Abgeordnete Klage auf Nichtigerklärung des Rückforderungsbeschlusses und der Zahlungsaufforderung erhob. Das EuG gab der Klage statt. Das EP habe seine Weigerung nicht ausreichend begründet und dem Abgeordneten damit das Recht auf Anhörung im Rückforderungsverfahren verwehrt. Zudem hätte das EP E-Mails aufbewahren und die beantragten Dokumente übermitteln müssen. Gegen dieses Urteil legte das EP ein erfolgreiches Rechtsmittel beim EuGH ein.

Der EuGH hat erwogen: Das **Recht auf Anhörung** (Parteienghör) ist in allen Verfahren zu wahren, die zu einer beschwerenden Maßnahme führen können. **Das Recht auf Aktenzugang** (Akteneinsicht) gewährleistet, dass dem Betroffenen die Möglichkeit gegeben wird, alle Schriftstücke **in der Ermittlungsakte** zu prüfen, die für seine Verteidigung erheblich sein könnten. Dazu gehören sowohl belastende als auch entlastende Schriftstücke mit Ausnahme von Geschäftsgeheimnissen, internen Schriftstücken des betreffenden Organs und anderen vertraulichen Informationen. Der Betroffene

kann daher Zugang zu allen Unterlagen beantragen und erhalten, bevor er in Ausübung seines Rechts auf Anhörung Stellung nimmt. Dieses Recht ist unter Wahrung des berechtigten Interesses der **Vertraulichkeit** sowie des **Berufs- und Geschäftsgeheimnisses** zu gewähren.

Dies gilt jedoch nicht für Dokumente, die nicht in dieser Akte enthalten sind, sich aber im Besitz des betreffenden Organs befinden. Ein Abgeordneter, der Ausgaben für einen Assistenten rechtfertigen muss, kann auf **Beweismittel** verweisen, die sich möglicherweise im Besitz des EP befinden. Ein solcher Verweis muss aber hinreichend genau sein, damit das EP die entsprechenden Beweisstücke identifizieren und prüfen kann. Das EP ist nicht verpflichtet, dem Abgeordneten sämtliche potenziell relevanten Unterlagen zu übermitteln, ohne dass dieser angibt, welche Beweise er meint und welche Tatsachen er damit beweisen will. Von einem Organ kann auch nicht verlangt werden, Beweisstücke in die Akte eines Verwaltungsverfahrens aufzunehmen, die nicht (mehr) vorhanden sind.

Das EP war nicht verpflichtet, E-Mails zwischen dem Abgeordneten und seinem Assistenten **dauerhaft zu speichern**. Die **Kenntnis von einem Konflikt** kann es nicht rechtfertigen, dass das Parlament von seiner internen Richtlinie, nach der E-Mails nach 90 Tagen automatisch gelöscht werden, abweicht. Dies gilt umso mehr, als das EP eine **Sortierung der E-Mails** hätte vornehmen müssen, was einen erheblichen und ungerechtfertigten Eingriff in die Privatsphäre des Abgeordneten und seines Assistenten gewesen wäre. Zudem sind die E-Mails, die von einem Abgeordneten versendet oder empfangen werden, keine Dokumente des Parlaments, sie gehören dem Abgeordneten selbst. Für das Rückforderungsverfahren war es auch nicht erforderlich, die E-Mails vorsorglich aus eigener Initiative zu speichern. Das EP konnte sich auf die Erklärungen der Betroffenen und die von ihnen vorgelegten Beweise stützen. Die Beweislast für die Tätigkeit der Assistenten liegt beim Abgeordneten.

Ein **Rückforderungsverfahren** erfüllt unter Wahrung der Verteidigungsrechte des Abgeordneten einen bestimmten, im öffentlichen Interesse liegenden Zweck. Art 9 Abs 1 lit b der Verordnung 2018/1725 ("*Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union*") steht dem **Zugang zu personenbezogenen Daten** durch den betroffenen Abgeordneten **nicht entgegen**, sofern dies unter Wahrung der Vertraulichkeit erfolgt.

Die **Übermittlung der Personalakte** des Assistenten an den Abgeordneten verstößt

allerdings gegen Art 26 des Abgeordnetenstatuts. Die Personalakte darf nur in den Diensträumen des Parlaments oder auf einem gesicherten Datenträger eingesehen werden.

### Rechtsprechung des VfGH

#### Aus der Rechtsprechung des VfGH:

- Eingriffe **staatlicher Behörden** in das Grundrecht auf Datenschutz sind nur aufgrund von Gesetzen zulässig, die ausreichend präzise und für jedermann vorhersehbar regeln, unter welchen Voraussetzungen das Ermitteln und Verwenden personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben erlaubt ist. Die **§§ 13 und 17 ORF-Beitrags-Gesetz 2024** normieren eine entsprechende Regelung für die Datenerhebung, -verwendung und -weitergabe durch die **ORF-Beitrags Service GmbH**. Diese **gesetzliche Ermächtigung** dient dem Erheben von Beiträgen zur Finanzierung des öffentlich-rechtlichen Rundfunks. Sie ist zum Erreichen dieses Ziels **geeignet** und **erforderlich** und – unter Berücksichtigung ihrer Ausgestaltung – auch **verhältnismäßig** ([VfGH 24.06.2025, E4624/2024](#)). **Anm: Der VfGH hat erstmals seit neun Jahren ein sogenanntes Massenverfahren eingeleitet. Wir haben im Datenschutzmonitor 12/2025 vom 26.03.2025 berichtet. Die Beantwortung der im Massenverfahren kundgemachten Rechtsfragen wurde nunmehr auch im Bundesgesetzblatt veröffentlicht, BGBl II 2025/153. Die aufgrund des Massenverfahrens ausgesetzten Beschwerdefverfahren vor dem BVwG werden von Amts wegen fortgesetzt werden.**

### Rechtsprechung der Justiz

OLG Graz 16.05.2025, 5R25/25y

#### **Berichterstattung, Persönlichkeitsrecht, Bildnisschutz**

- Ein Künstlermanager klagte die Verlegerin und Medieninhaberin eines Boulevardmagazins, die in einem Artikel über den Tod der Ehefrau eines von ihm betreuten Musikers ohne tatsächliche Grundlage einen Mordverdacht in den Raum gestellt hatte. Zugleich veröffentlichte die Zeitschrift ohne dessen Zustimmung ein Lichtbild des Managers. Der Manager verlangte neben Unterlassung auch Schadenersatz, weil er durch die Falschberichterstattung in seinem Recht am eigenen Bild nach § 78 UrhG verletzt worden sei und berufliche Nachteile befürchte. Ein berechtigtes Veröffentlichungsinteresse an seinem Bild bestehe nicht. Das Erstgericht gab der Klage statt. Dagegen erhob die Medieninhaberin (erfolglos) Berufung.

Das OLG Graz hat erwo-gen: Durch § 78 UrhG soll jedermann gegen einen

Missbrauch seiner Abbildung in der Öffentlichkeit geschützt werden. § 78 UrhG normiert dabei keinen absoluten **Bildnisschutz**, sondern geht von einem **flexiblen Interessenprinzip** aus. Eine nicht genehmigte Verbreitung eines Bildnisses ist zulässig, solange die berechtigten Interessen des Abgebildeten nicht verletzt werden. Bei der Beurteilung ist darauf abzustellen, ob Interessen des Abgebildeten bei objektiver Prüfung als schutzwürdig anzusehen sind. Entscheidend ist, ob die Person des Abgebildeten durch die Veröffentlichung in einen nicht den Tatsachen entsprechenden Zusammenhang gestellt wurde. Es reicht schon die bloße Möglichkeit von Missdeutungen aus.

Für den unvoreingenommenen Betrachter des Artikels wird der Manager ohne jeden sachlichen Anknüpfungspunkt in einen assoziativen Zusammenhang mit einem unbegründeten Mordverdacht gestellt. Eine Rechtsverletzung ist daher zu bejahen. Diese ist auch nicht durch das Recht auf **freie Meinungsäußerung** gerechtfertigt.

#### Aus der Rechtsprechung der Justiz:

- Lehnt der Netzbenutzer den Austausch eines **"eichfälligen"** Zählers gegen ein intelligentes Messgerät ("**Smart Meter**") ab, darf der Netzbetreiber keine **Stromabschaltung** androhen. Dem Netzbetreiber steht es aber offen, gerichtliche Hilfe bei der Durchsetzung seines Interesses auf Tausch des Stromzählers in Anspruch zu nehmen. Die vom Rekursgericht erlassene **einstweilige Verfügung** zugunsten des Netzbenutzers wird bestätigt. Sie wird jedoch ungültig, wenn der Netzbenutzer beim Erstgericht keine **Sicherheitsleistung** iHv EUR 10.000 erlegt ([OGH 28.05.2025, 3Ob30/25w](#); [03.06.2025, 2Ob31/25k](#)).

### Rechtsprechung des BVwG

BVwG 02.05.2025, W137 2301309-1

#### **Universität, Videoaufnahme, Verordnung**

- Ein außerordentlicher Univ-Professor an einer österreichischen Universität nahm an einer verpflichtenden Departmentsitzung teil. Die Leiterin des Departments zeichnete diese Sitzung ohne vorherige Information an die Teilnehmer mittels Laptops auf. Die Audioaufnahme wurde dem Protokollführer zur Erstellung des Sitzungsprotokolls übermittelt und nachträglich gelöscht. Das Rektorat der Universität beschloss danach eine Änderung der Richtlinie zu den Kommunikations- und Meinungsbildungsprozessen, welche die Audioaufzeichnungen zu Protokollierungszwecken erlaubte, sowie einen Verhaltenskodex mit gleichlautendem Inhalt. Eine weitere Aufnahme erfolgte in einer späteren Sitzung, wobei der Professor dieser nicht beiwohnte.



Der Professor erhob Datenschutzbeschwerde bei der DSB. Diese stellte fest, dass die Universität durch die **Audioaufnahme** sowie deren Weiterleitung sein Recht auf Geheimhaltung verletzt habe. Die DSB sprach überdies eine Verwarnung hinsichtlich der zweiten Aufnahme aus (Art 58 Abs 2 lit b DSGVO), lehnte jedoch den Antrag auf Verhängung einer Geldbuße ab. Die darauffolgende Bescheidbeschwerde der Universität an das BVwG blieb erfolglos.

Das BVwG hat erwogen: Die Verarbeitungstätigkeiten von Behörden in Erfüllung ihrer Aufgaben können laut Art 6 Abs 1 letzter Satz DSGVO nicht auf die Wahrnehmung berechtigter Interessen gestützt werden. Der **"Code of Conduct"** und die **Änderung der Richtlinie des Rektorats** scheiden bereits aufgrund der **zeitlichen Divergenz** als mögliche Rechtsgrundlage gemäß Art 6 Abs 1 lit e DSGVO aus. Mangels der Qualifikation der Departmentsitzung als "vom Senat eingerichtetes Kollegialorgan" ist auch die Heranziehung einer entsprechenden Bestimmung der Geschäftsordnung des Senats ausgeschlossen.

Als zentrales Element einer **Verordnung** gilt die **Außenwirkung**. Da die Beschlüsse vom Rektorat – und nicht vom Senat – erlassen wurden, kann es sich bei diesen nicht um Teile der Satzung der Universität handeln. Es ist somit davon auszugehen, dass das Rektorat eine **Verwaltungsverordnung** für alle Departments bzw die Departmentleitungen geschaffen hat, um eine einheitliche **interne Kommunikation zu gewährleisten**. Aufgrund derselben Überlegungen bildet auch der **"Verhaltenskodex"** keine ausreichende rechtliche Grundlage für die Datenverarbeitung.

Der Änderung der Richtlinie des Rektorats und dem Code of Conduct **fehlt** es am **notwendigen Verordnungscharakter**, um eine rechtliche Grundlage iSd Erlaubnistatbestands des Art 6 Abs 1 lit e DSGVO bilden zu können.

BVwG 28.04.2025, W211 2289521-1

#### **Rechtsanwalt, Exekution, justizielle Tätigkeit**

- Eine Rechtsanwaltskanzlei führte gegen einen Schuldner ein Exekutionsverfahren und brachte gegen diesen auch mehrere Strafanträge ein. Der Schuldner erachtete die darin vorgebrachten Tatsachen als unrichtig, weil es die Anwaltskanzlei in den Verfahren aus seiner Sicht unterlassen hat, relevante Informationen über ihn gegenüber dem Gericht mitzuteilen. Er erhob Datenschutzbeschwerde bei der DSB. Die DSB wies die Datenschutzbeschwerde zurück. Die Bescheidbeschwerde des Schuldners an das BVwG war erfolgreich.

Das BVwG hat erwogen: Im Fall der Zurückweisung einer Datenschutzbeschwerde durch die DSB ist **Sache** des Beschwerdeverfahrens lediglich die Frage der **Rechtmäßigkeit der Zurückweisung**. Jede Betroffene hat nach Art 77 DSGVO das Recht auf Datenschutzbeschwerde bei einer Aufsichtsbehörde, wenn ihrer Ansicht nach die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt. Die **Beschwerdelegitimation** ist schon dann gegeben, wenn **denkmöglich eine Datenverarbeitung** vorliegt und dadurch rechtswidrig sein kann. Eine **Datenschutzbeschwerde**, die sich gegen eine denkmöglich rechtswidrige Datenverarbeitung richtet, ist von der DSB **inhaltlich zu prüfen** und kann nicht wegen des Fehlens einer Datenverarbeitung zurückgewiesen werden.

Die gerichtliche Tätigkeit in Art 55 DSGVO ist weit zu verstehen. Auch eine **Zustellverfügung**, die Tätigkeit eines **gerichtlichen Sachverständigen** und die Tätigkeit des **Gerichtsvollziehers** in Exekutionssachen fallen darunter. Das Einschreiten eines Rechtsanwalts für seinen Mandanten fällt **mangels gerichtlicher Beauftragung** jedoch nicht darunter. Die Datenverarbeitung durch den Rechtsanwalt unterliegt der Kontrolle der DSB. Die DSB hätte daher die Datenverarbeitung bezüglich der Exekutions- und Strafanträge des Rechtsanwalts inhaltlich zu prüfen gehabt.

Die Beurteilung der Frage, ob Aussagen in Anträgen inhaltlich richtig oder unrichtig sind, fällt allerdings in die **Zuständigkeit** der ordentlichen Gerichte. Eine Datenschutzbeschwerde dient nicht dazu, über die in die Zuständigkeit der Gerichte fallenden Fragen zu entscheiden.

BVwG 30.04.2025, W171 2298465-1

#### **Krankentransport, Spendenbrief, Gesundheitsdaten, Zweckänderung**

- Ein Rettungsdienst erhob im Rahmen eines **Krankentransports** die Daten eines Patienten zur Verrechnung der Kosten mit dem Sozialversicherungsträger und zur Dokumentation. In Folge verwendete der Rettungsdienst den Namen und die Anschrift des Patienten, um diesem einen **Spendenbrief** zuzusenden. Der Patient hatte keine Einwilligung zur Weiterverarbeitung seiner Daten für diesen Zweck erteilt. Er erhob daher eine Datenschutzbeschwerde bei der DSB, weil er sich in seinem Recht auf Geheimhaltung verletzt sah. Die DSB stellte fest, dass die Weiterverarbeitung der Daten zur Erstellung des Spendenbriefs rechtswidrig war und gab der Datenschutzbeschwerde statt. Daraufhin erhob der Rettungsdienst eine (erfolglose) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Der Name und die Adresse des Patienten sind personenbezogene Daten. Zusätzlich wurde auch die Information darüber, dass der Patient im Zuge eines Rettungseinsatzes betreut wurde, als Datum verarbeitet. Da sich daraus die eingeschränkte Gesundheit des Patienten ableiten lässt, liegt eine Verarbeitung von **Gesundheitsdaten** iSd Art 4 Z 15 DSGVO vor.

In Art 9 Abs 1 DSGVO ist ein **Verarbeitungsverbot** von gesundheitsbezogenen Daten normiert. Eine Verarbeitung ist nur zulässig, wenn einer der **Ausnahmetatbestände** des Art 9 Abs 2 DSGVO erfüllt ist. Der Patient hat in die Verarbeitung nicht eingewilligt. Auch dient die Verarbeitung nicht der Geltendmachung arbeits- oder sozialrechtlicher Ansprüche, schützt keine lebenswichtigen Interessen, bezieht sich nicht auf offensichtlich öffentlich gemachte Daten, ist nicht zur Rechtsverfolgung erforderlich und steht nicht im öffentlichen Interesse. Auch die weiteren Ausnahmetatbestände des Art 9 Abs 2 DSGVO greifen nicht. Die **Primärverarbeitung** der Daten zur Abrechnung mit dem Sozialversicherungsträger war rechtmäßig. Die **Weiterverarbeitung** der Daten zur Versendung eines Spendenbriefs überschreitet jedoch den ursprünglichen Zweck und findet in der DSGVO keine Rechtfertigung.

BVwG 28.04.2025, W211 2283135-1

### **Exzess, Missbrauchsabsicht, Ressourcen**

- Zwei Personen erwarben im Rahmen einer Zwangsversteigerung Eigentum an einer Wohnung. Die Hausverwaltung, welche die Wohnungseigentümergeinschaft vertritt, organisierte die jährliche Ablesung der Verbrauchszähler. Bei Nichtgewährung des Zutritts oder Verweigerung des Zählertauschs erfolgten Hochrechnungen des Verbrauchs. Die Hausverwaltung erhielt von der Ablesefirma eine Gesamtkostenaufstellung und erstellte auf dieser Basis Einzelabrechnungen für die Bewohner. Die (nunmehrigen) Eigentümer wendeten sich zunächst an die Schlichtungsstelle und anschließend (erfolglos) an die ordentlichen Gerichte, weil sie die Abrechnungen als fehlerhaft ansahen. In der Folge brachten sie innerhalb von 50 Monaten insgesamt 19 Datenschutzbeschwerden gegen die Hausverwaltung bei der DSB ein und gaben an, dass ihre personenbezogenen Daten über einen Zeitraum von rund 15 Jahren ohne Rechtsgrundlage und ohne Einwilligung verwendet wurden, um Verbrauchswerte hochzurechnen und falsche Abrechnungen zu erstellen. Die DSB lehnte die Behandlung der letzten Datenschutzbeschwerde ab und begründete dies mit einer exzessiven und rechtsmissbräuchlichen Inanspruchnahme ihrer Tätigkeit. Dagegen

erhoben die Eigentümer eine (erfolgreiche) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Bei offenkundig unbegründeten oder **exzessiven** Datenschutzbeschwerden darf die DSB eine Gebühr verlangen oder sich weigern, tätig zu werden (Art 57 Abs 4 DSGVO). Datenschutzbeschwerden können jedoch nicht allein aufgrund ihrer Zahl als exzessiv eingestuft werden. Die DSB muss das Vorliegen einer **Missbrauchsabsicht** der anfragenden Person nachweisen.

Eine **Missbrauchsabsicht** liegt vor, wenn Datenschutzbeschwerden eingereicht werden, ohne dass dies objektiv erforderlich ist, um die Rechte aus der DSGVO zu schützen. Im Streitfall hat eine einzelfallbasierte Abwägung zwischen dem Rechtsschutzinteresse des Betroffenen sowie dem Interesse an **Ressourcenschonung** der DSB zu erfolgen. Bei einer durchschnittlichen Einbringung einer einzelnen Datenschutzbeschwerde alle zwei bis drei Monate kann nicht von einer übermäßigen Ausübung des **Beschwerderechts** ausgegangen werden. Auch der Umstand, dass die Datenschutzbeschwerden sich wiederholt gegen den gleichen Verantwortlichen richten, führt isoliert betrachtet nicht bereits zur Exzessivität iSd Art 57 Abs 4 DSGVO. Es ist offensichtlich, dass die Eigentümer nicht wahllos Datenschutzbeschwerden erhoben haben. Weiters ist die erstmalige Geltendmachung von Betroffenenrechten kein unlauteres Motiv. Die Eigentümer verfolgen mit ihren Datenschutzbeschwerden nachvollziehbar den Schutz ihrer Rechte aus der DSGVO.

### Aus der weiteren Rechtsprechung des BVwG:

- Bei grenzüberschreitenden Verarbeitungen ist ein sogenanntes **Kohärenzverfahren** durchzuführen. Dabei wird eine **federführende Aufsichtsbehörde** bestimmt, die für die Verfahrensführung zuständig ist. Während des Kohärenzverfahrens ist die sechsmonatige **Entscheidungsfrist** der DSB **gehemmt**. Die Durchführung des Kohärenzverfahrens liegt nicht im Ermessen der DSB. Daher wird das Kohärenzverfahren bei Vorliegen der gesetzlichen Voraussetzungen **automatisch** beim Einbringen der Datenschutzbeschwerde in Gang gesetzt. Die Entscheidungsfrist wird daher bereits beim Einbringen der Datenschutzbeschwerde gehemmt ([BVwG 29.04.2025, W101 2308679-1](#)). **Anm: Diese Entscheidung folgt der ständigen Rechtsprechung des BVwG.**
- Wird eine Datenschutzbeschwerde von der DSB nicht bearbeitet, steht den Betroffenen gem Art 78 Abs 2 DSGVO eine **Untätigkeitsklage** zur Verfügung. Nach dem nationalen Recht ist dafür die Säumnisbeschwerde vorgesehen. In einem grenzüberschreitenden Sachverhalt ist die

- Untätigkeitsklage bzw Säumnisbeschwerde jedoch gegen die **federführende Aufsichtsbehörde** zu richten, weil diese für die Entscheidung zuständig ist (**Kohärenzverfahren**). Die **Frist** für die Entscheidung der DSB ist während der federführenden Zuständigkeit der ausländischen Aufsichtsbehörde **gehemmt**. Die Untätigkeit der DSB kann allerdings in einer Verletzung der **Unterrichtungspflicht** über den Stand des Verfahrens sowie im **Nichtweiterleiten der Datenschutzbeschwerde** an die zuständige (federführende) Aufsichtsbehörde bestehen. Holt die DSB diesen Verfahrensschritt nach und leitet sie die Datenschutzbeschwerde via der IT-Kooperationsplattform "**Internal Market Information System**" an die zuständige Aufsichtsbehörde weiter, liegt die Säumnis aber nicht mehr vor ([BVwG 23.04.2025, W605 2307742-1](#)). **Anm: Das BVwG weicht in dieser Entscheidung von seiner oben angeführten Rechtsprechung ab, wonach die Durchführung eines Kohärenzverfahrens beim Einbringen einer Datenschutzbeschwerde automatisch in Gang gesetzt wird und damit die Entscheidungspflicht der DSB sogleich gehemmt ist.**
- Identität der Sache ist dann gegeben, wenn sich der für die Entscheidung maßgebende Sachverhalt, der dem rechtskräftigen **Vorbescheid** zugrunde lag, nicht geändert hat (**res iudicata**). Weist die DSB eine Datenschutzbeschwerde ohne inhaltliche Auseinandersetzung wegen **Präklusion** zurück, steht dieser zurückweisende Vorbescheid einer neuerlichen Behandlung derselben Datenschutzbeschwerde jedoch nicht entgegen, weil keine inhaltliche Auseinandersetzung mit dem Parteienbringen stattgefunden hat. Die Datenschutzbeschwerde ist daher erneut wegen Präklusion zurückzuweisen ([BVwG 24.04.2025, W298 2309933-1](#)).
  - Der Betroffene beantragte die **Berichtigung** der Daten zu seiner Geschlechtsidentität von "unbekannt" auf "divers". Der Verantwortliche ersetzte sein vormaliges Kundenverwaltungssystem **während des laufenden Verfahrens** durch eine neue Buchungsplattform, in der keine Daten zur Geschlechtsidentität verarbeitet werden. Dadurch wurde zwar streng genommen dem Ersuchen des Betroffenen nicht iSd **§ 24 Abs 6 DSGVO** entsprochen, der Verantwortliche verarbeitet aber auch keine Daten mehr, die der Geschlechtsidentität des Betroffenen widersprechen und somit unrichtig sind. Die **Feststellung einer vergangenen Verletzung des Rechts auf Berichtigung** ist nicht vorgesehen ([BVwG 23.04.2024, W605 2283487-1](#)).
  - Die Datenschutzbeschwerde wurde von der DSB aufgrund inhaltlicher Mängel und unterlassener Verbesserung **zurückgewiesen**. In der dagegen gerichteten **Beschreibeschwerde** führte der Betroffene nur aus,

dass er mit dem Zurückweisungsbescheid der DSB unzufrieden sei und diesen beeinträchtige. Eine so ausgeführte Bescheidbeschwerde ist mangelhaft. Folgt der Betroffene auch dem Verbesserungsauftrag des BVwG nicht, ist die Bescheidbeschwerde **zurückzuweisen** ([BVwG 02.05.2025, W256 2275267-1](#)).

- Die **Vollständigkeit** der erteilten Auskunft während des laufenden Verfahrens ist nicht zu prüfen, wenn Gegenstand des Verfahrens nur das **Nichterteilen der Auskunft** war. Ein Recht auf die Feststellung einer allfälligen **Verspätung der Auskunftserteilung** besteht nicht, weil der Betroffene durch Erhalt der Auskunft sein Rechtsschutzziel erreicht hat ([BVwG 06.05.2025, W256 2307865-1](#)).

### **EU-Rechtsakte**

- Am **02.07.2025** wurde die "*Delegierte Verordnung (EU) 2025/532 der Kommission vom 24. März 2025 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung der Aspekte, die ein Finanzunternehmen bei der **Untervergabe von IKT-Dienstleistungen** zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss*", [ABI L 2025/532](#), veröffentlicht. Mit dieser delegierten Verordnung wird die Verordnung über die digitale operationale Resilienz im Finanzsektor (**DORA**) durch technische Regulierungsstandards bei der Untervergabe von IKT-Dienstleistungen ergänzt.
- Am **02.07.2025** wurden Art 13 Abs 8 und Art 64 Abs 10 der **Cyberresilienz-VO (EU) 2024/2847** in der deutschen Fassung **redaktionell berichtigt**, [ABI L 2025/90555](#).
- Am **01.07.2025** erließ die Kommission den Entwurf für eine "*Delegierte Verordnung über den Zugang zu Daten gemäß dem Gesetz über digitale Dienste (DSA)*", [C\(2025\) 4340 final](#). Mit diesem Rechtsakt wird das **DSA-Datenzugangsportal** eingerichtet, über das geprüfte Forscher auf bestimmte Daten zugreifen können, die von sehr großen Online-Plattformen (VLOPs) und Suchmaschinen (VLOSEs) verarbeitet werden.

### **Nationale Rechtsakte**

- Am **01.07.2025** wurde das "*Bundesgesetz, mit dem das Universitätsgesetz 2002 und das **Bildungsdokumentationsgesetz 2020** geändert werden*", [BGBl I 2025/28](#), kundgemacht. Geschaffen wurden die Rechtsgrundlagen für die Weiterentwicklung des **Datenverbundes der Universitäten und Hochschulen (DVUH)** und des **Austrian Higher Education Systems Networks (AHESN)**, sowie für die Etablierung

eines **Studierendenregisters** und die Bereitstellung des **digitalen Studierenden- ausweises**. Der **Register- und System- verbund (RSV)** wird bei der Bundesrechen- zentrum GmbH (BRZ) angebunden.

- Am **30.06.2025** veröffentlichte die **DSB** ihren [Leitfaden zum Informationsfreiheitsge- setz](#). Die DSB informiert darin über das Ver- hältnis zwischen dem **Datenschutzrecht** und der **Informationsfreiheit** und bettet ihre erläuternden Überlegungen in den Ge- samtkontext des IFG sowie der Bundesver- fassung ein.

to the point

# Datenschutzmonitor. 28/2025 vom 16.07.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 10.07.2025, 64753/14, *Gulotti/Italien* (Überwachung, Briefverkehr, Haft)

EGMR 10.07.2025, 2599/16, *Korniyets/Ukraine* (Hausdurchsuchung, wirksamer Rechtsbehelf)

- **Rechtsprechung des EuGH**

EuGH 10.07.2025, C-367/24, *Telekom România* (Internetzugangsdienst, Netzneutralität, Video-streaming)

- **Rechtsprechung des VwGH**

VwGH 05.06.2025, Ra 2024/04/0008 (AMS, Beschwerdegegner, Verantwortlicher)

VwGH 17.06.2025, Ra 2025/04/0146 (Kohärenzverfahren, Säumnis)

VwGH 28.05.2025, Ro 2025/13/0001; 28.05.2025, Ro 2024/13/0022 (Kontenregister, Erbschaft)

- **Rechtsprechung der Justiz**

OLG Wien 20.03.2025, 1R22/25z (Auskunft, Beweismaterial, Spielverluste)

- **Rechtsprechung des BVwG**

BVwG 08.05.2025, W274 2264017-1 (Vollstreckung, ausländische Geldbuße, Inkasso)

BVwG 06.05.2025, W252 2271318-1 (CAPTCHA, Zuständigkeit, Barrierefreiheit)

BVwG 06.05.2025, W252 2293098-1 (Staatsanwaltschaft, Akteneinsicht, Beschränkung)

BVwG 07.05.2025, W176 2273922-1 (Gerichtsverfahren, Rechtsanspruch, berechtigtes Interesse)

BVwG 08.05.2025, W274 2257892-1 (Datenweitergabe, Datenminimierung, gelindere Mittel)

BVwG 12.05.2025, W292 2311008-1 (Beschwer, Rechtsschutzinteresse)

BVwG 08.05.2025, W292 2310611-1 (Beschwer)

BVwG 02.05.2025, W292 2285392-1; 02.05.2025, W292 2285923-1 (Zurückziehung der Bescheidbeschwerde)

- **EU-Rechtsakte**

KI-Verhaltenskodex für allgemeine Zwecke

## To the Point:

### Rechtsprechung des EGMR

Aus der Rechtsprechung des EGMR:

- Die **Überwachung** und Beschränkung des **Briefverkehrs** von einem **Häftling**, der Anführer eines Mafia-Clans ist, ist im Lichte des Art 8 EMRK grundsätzlich zulässig, sofern sie auf einer gesetzlichen Grundlage beruht, einem legitimen Ziel dient und verhältnismäßig ist. Wird die Beschränkung verlängert, muss das Gericht die konkreten Umstände des Einzelfalls berücksichtigen und die Gründe für die Verlängerung nachvollziehbar darlegen. Eine bloße Bezugnahme auf einen Ministerialerlass, der eine generelle Verlängerung zulässt, oder auf die allgemeinen Ermittlungsakten des Häftlings reichen nicht aus. Fehlt es in der gerichtlichen Entscheidung an konkreten Hinweisen, die die Beschränkung rechtfertigen, liegt eine Verletzung des Rechts auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK vor ([EGMR 10.07.2025, 64753/14, Gulotti/Italien](#)).
- Ein Eingriff in das Recht auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK ist gerechtfertigt, wenn er im Einklang mit dem Gesetz erfolgt, legitime Ziele verfolgt und notwendig ist. Da eine **Hausdurchsuchung** ein **schwerwiegender Eingriff** in das Privatleben ist, muss sie auf **besonders präzisen Gesetzen** beruhen. Darüber hinaus muss ein **wirksames Rechtsmittel** zur Verfügung stehen, um die Rechtmäßigkeit der Durchsuchung überprüfen zu lassen. Nach ukrainischem Recht sind Hausdurchsuchungen in dringenden Fällen auch ohne vorherigen richterlichen Beschluss zulässig. Den Betroffenen steht jedoch keine Möglichkeit offen, einen **Durchsuchungsbefehl** anzufechten, unabhängig davon, ob dieser zuvor erlassen oder die Durchsuchung nachträglich genehmigt wurde. Mangels wirksamer Rechtsbehelfe liegt daher eine Verletzung von Art 8 iVm Art 13 EMRK vor ([EGMR 10.07.2025, 2599/16, Korniyets/Ukraine](#)).

### Rechtsprechung des EuGH

[EuGH 10.07.2025, C-367/24, Telekom România](#)

#### **Internetzugangsdienst, Netzneutralität, Videostreaming**

- Der EuGH hat aufgrund eines Vorabentscheidungsersuchens über die Vereinbarkeit einer von einem **Internetzugangsdienst** angebotenen **Tarifoption** mit der Verordnung (EU) 2015/2120 (**Netzneutralitäts-VO**) entschieden. Die Tarifoption ermöglichte es Endkunden, **Videostreamingdienste** unbegrenzt zu nutzen, ohne dass das für diese Streamingdienste verbrauchte Datenvolumen auf das im Grundtarif enthaltene

Datenvolumen angerechnet wurde. Gleichzeitig wurde die Bandbreite für Videostreaming auf 1,5 Mbps begrenzt, während für andere Verkehrskategorien eine deutlich höhere Geschwindigkeit (150 Mbps) zur Verfügung stand. Die rumänische Regulierungsbehörde beanstandete diese Praxis als Verstoß gegen die unionsrechtlichen Vorgaben zur Gleichbehandlung des Datenverkehrs.

Nach Art 1 Abs 3 Netzneutralitäts-VO haben Anbieter von Internetzugangsdiensten den gesamten Verkehr bei der Erbringung von Internetzugangsdiensten ohne Diskriminierung, Beschränkung oder Störung, sowie unabhängig von Sender und Empfänger, den abgerufenen oder verbreiteten Inhalten, den genutzten oder bereitgestellten Anwendungen oder Diensten oder den verwendeten Endgeräten gleich zu behandeln. Das vorliegende Gericht legte dem EuGH eine Frage zur Auslegung der Gleichbehandlungsvorschrift der Verordnung vor.

Der EuGH hat erwogen: Die Anbieter von **Internetzugangsdiensten** müssen den gesamten Datenverkehr gleich, ohne Diskriminierung, Beschränkung oder Störung behandeln. Diese Verpflichtung besteht nicht nur darin, dass Anbieter von Internetzugangsdiensten keine Maßnahmen ergreifen dürfen, die eine Diskriminierung zwischen unterschiedlichen Wirtschaftsteilnehmern bewirken, die Inhalte bereitstellen. Sie besteht auch darin, sicherzustellen, dass sämtliche Inhalte sowie sämtliche genutzte oder zur Verfügung gestellte **Anwendungen** oder **Dienste gleich behandelt werden**.

Eine **Differenzierung der Bandbreite** für Videostreaming gegenüber anderen Verkehrskategorien ist eine **unzulässige Ungleichbehandlung** der verschiedenen Wirtschaftsteilnehmer. Die Möglichkeit, angemessene **Verkehrsmanagementmaßnahmen** des Datenverkehrs zu ergreifen, besteht nur, wenn diese auf objektiv unterschiedlichen technischen Anforderungen an die Dienstqualität und nicht auf kommerziellen Erwägungen beruhen.

Die Begrenzung der Bandbreite für Videostreams dient **kommerziellen Zwecken** und nicht technischen Notwendigkeiten. Die Maßnahme ist nicht auf einen **erforderlichen Zeitraum** beschränkt und fällt nicht unter die Ausnahmen, einer gesetzlichen Verpflichtung zu entsprechen, oder die Integrität oder Sicherheit des Netzes zu verhindern (**Netzüberlastung**). Die Tarifoption verstößt daher gegen die in Art 3 Abs 3 Netzneutralitäts-VO normierte Pflicht zur **Gleichbehandlung des Datenverkehrs**.

## Rechtsprechung des VwGH

VwGH 05.06.2025, Ra 2024/04/0008

### **AMS, Beschwerdegegner, Verantwortlicher**

- Eine Arbeitslose erachtete sich in ihrem Recht auf Geheimhaltung verletzt, weil das Arbeitsmarktservice (**AMS**) personenbezogene Daten, ua Gesundheitsdaten, auch in Zeiträumen verarbeite, in denen kein aufrechtes Betreuungsverhältnis bestand. Aufgrund dessen erhob sie Datenschutzbeschwerde gegen das Arbeitsmarktservice Wien (**AMS W**). Die Arbeitslose bezeichnete die Regionalstelle als Beschwerdegegnerin, dennoch qualifizierte die DSB das AMS als Verantwortlichen und damit als Beschwerdegegner, weil nur dieses – und nicht das AMS W – Rechtspersönlichkeit habe. Da die Datenverarbeitung rechtmäßig erfolgt sei, wies die DSB die Datenschutzbeschwerde ab. Daraufhin erhob die Arbeitslose Beschwerde an das BVwG. Dieses behob den Bescheid der DSB, weil dieser an das AMS und nicht an die Regionalstelle AMS W gerichtet war. Gegen dieses Erkenntnis richtete sich die erfolgreiche außerordentliche Revision des AMS.

Der VwGH hat erwogen: Das aufgrund einer Datenschutzbeschwerde geführte Verfahren ist **antragsgebunden**. Grundsätzlich liegt die Benennung des Beschwerdegegners in der Disposition des Antragstellers. Wenn die Benennung unzumutbar ist, hat die DSB den Beschwerdegegner durch Auslegung bzw eigene Ermittlungen zu bestimmen (§ 24 Abs 2 Z 2 DSG). Die DSB ist von einer **Unzumutbarkeit der Benennung** des Beschwerdegegners durch die Arbeitslose ausgegangen. Weiters hat die Arbeitslose in ihrer Beschwerde selbst von einer rechtswidrigen Verarbeitung ihrer Daten durch das AMS gesprochen. Sie wendete sich nicht dagegen, dass die DSB das Verfahren gegen das AMS führte. Die Arbeitslose brachte somit nicht unmissverständlich zum Ausdruck, dass sich ihre Datenschutzbeschwerde nicht zumindest auch gegen das AMS richten sollte.

Die ersatzlose Behebung des Bescheids der DSB durch das BVwG war rechtswidrig. Die gegen das AMS gerichtete Erledigung der DSB lag nicht außerhalb der Sache des durch die Datenschutzbeschwerde begründeten Verfahrens. Eine Auseinandersetzung mit der möglichen Stellung des AMS als (**gemeinsamer**) **Verantwortlicher** gemäß Art 4 Z 7 DSGVO für die Datenverarbeitung ist unterblieben.

Aus der **Verantwortlicheneigenschaft** der Stellung des AMS W folgt nicht automatisch die fehlende Eigenschaft des AMS als Verantwortlicher. § 25 AMSG enthält keine explizite Benennung des AMS als

datenschutzrechtlich Verantwortlicher hinsichtlich der Datenverarbeitung. Die Übertragung von Aufgaben und die Ermächtigung zur Verarbeitung damit zusammenhängender Daten kann eine **Stellung als Verantwortlicher** begründen. Diese Stellung könnte sich – abhängig von den dazu im fortgesetzten Verfahren zu treffenden Feststellungen zur Rolle bzw zum Beitrag des AMS – auch auf die Datenverarbeitungen erstrecken.

### Aus der weiteren Rechtsprechung des VwGH:

- In einem **Kohärenzverfahren** hielt das BVwG über eine **Säumnisbeschwerde** fest, dass die Säumnis der DSB auch im **Nichtweiterleiten** der Datenschutzbeschwerde an die **federführende Aufsichtsbehörde** bestehen kann. Die Datenschutzbeschwerde sei in der Zwischenzeit jedoch von der DSB an die federführende Aufsichtsbehörde weitergeleitet worden, weshalb die Säumnisbeschwerde zurückzuweisen war. Die gegen diesen Beschluss des BVwG erhobene Amtsrevision der DSB ist zurückzuweisen, weil durch die Zurückweisung der Säumnisbeschwerde das **Rechtsschutzinteresse** der DSB auch dann weggefallen ist, wenn die DSB eine andere Begründung des BVwG-Beschlusses bevorzugt hätte ([VwGH 17.06.2025, Ra 2025/04/0146](#)).
- Die Bestimmung des **§ 4 Abs 4 KontRegG** ist eine spezialgesetzliche Ausformung des höchstpersönlichen datenschutzrechtlichen Auskunftsrechts. **Betroffene** iSd KontRegG sind auch **Unternehmer**. Der zu Lebzeiten bestandene Auskunftsanspruch des Rechtsvorgängers geht auf den **Rechtsnachfolger (Erben)** jedoch nicht über. Auch auf die **Verlassenschaft** geht der Rechtsanspruch nicht über. Es liegt im rechtspolitischen Gestaltungsspielraum des Gesetzgebers, wenn er Auskünfte aus dem **Kontenregister** nicht auch zur leichteren Durchsetzbarkeit erbrechtlicher Ansprüche vorsieht. Entsprechende Anregungen der Notariatskammer im Gesetzgebungsprozess griff der Gesetzgeber nicht auf (VwGH [28.05.2025, Ro 2025/13/0001](#); [28.05.2025, Ro 2024/13/0022](#)).

### Rechtsprechung der Justiz

#### Aus der Rechtsprechung der Justiz:

- Das auf Art 15 Abs 1 und Abs 3 gestützte **Auskunftersuchen** dient auch dann einem legitimen Zweck, wenn es darauf abzielt, **Beweismaterial** für eine spätere Prozessführung zu besorgen. Ein **Rechtsmissbrauch** ist selbst bei einem ausschließlich **datenschutzfremden Zweck** nicht evident. Die Rechtsposition der Beklagten wird zudem nicht geschwächt, weil der Kläger auch im Wege eines

**Rechnungslegungsbegehrens** gemäß Art XLII EGZPO eine entsprechende Auskunft erzwingen könnte. Auch besteht kein "Geheimnis" der Beklagten, weil der Kläger nur Daten aus einer **gemeinsamen Geschäftsverbindung** begehrt. Das behauptete Motiv des Klägers, seine **erlittenen Spielverluste** zurückfordern zu wollen, ist nicht unlauter ([OLG Wien 20.03.2025, 1R22/25z](#)).

### **Rechtsprechung des BVwG**

[BVwG 08.05.2025, W274 2264017-1](#)

#### **Vollstreckung, ausländische Geldbuße, Inkasso**

- Ein Betroffener erhielt ein Schreiben eines österreichischen Inkassounternehmens zur Eintreibung einer von einer italienischen Behörde verhängten Verkehrsstrafe. Der Betroffene antwortete, dass die Verwaltungsübertretung nicht nachvollziehbar sei und keine Zahlung geleistet werde. Ferner ersuchte er um Löschung seiner Daten im Zusammenhang mit dem Inkassovorgang. Es handle sich um eine Strafe nach dem EU-Verwaltungsstrafvollstreckungsgesetz (**EU-VStVG**), weshalb eine Vollstreckung von Geldstrafen durch private Inkassounternehmen nicht in Betracht komme. Das Inkassounternehmen verweigerte die Löschung. Die Zuhilfenahme privater Dienstleister bei der Einmahnung offener Bußgeldforderungen sei zulässig. Die Datenverarbeitung stütze sich auf das berechtigte Interesse der italienischen Strafbehörde.

Aufgrund der Datenschutzbeschwerde des Betroffenen stellte die DSB eine Verletzung im Recht auf Geheimhaltung fest. Die Vorgehensweise zur Eintreibung ausländischer Verwaltungsstrafen erfolge nach dem EU-VStVG. Die Datenverarbeitung durch ein privatwirtschaftliches Inkassounternehmen könne durch keinen Erlaubnistatbestand des Art 6 DSGVO gerechtfertigt werden. Dagegen erhob das Inkassounternehmen (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Das EU-VStVG ermöglicht auf einfache Weise die **Vollstreckung** von **ausländischen Verwaltungsentscheidungen** samt der Verpflichtung zur Zahlung einer Geldbuße im Wege des Verwaltungsvollstreckungsgesetzes (**VVG**) zu bewirken. Schon aus dem **Legalitätsprinzip** (Art 18 Abs 1 B-VG) folgt, dass eine **Bezirksverwaltungsbehörde** kein Inkassobüro zur Betreibung von Geldstrafen einschalten darf, sondern die gesetzlich vorgesehenen Mittel der Eintreibung nutzen muss. Nach dem erkennbaren Willen des Gesetzgebers sollen daher keine **"außerbehördlichen" Betreibungen** von hoheitlich verhängten Geldstrafen stattfinden. Zur Wahrung der berechtigten Interessen der italienischen Strafbehörde war es daher nicht

erforderlich, ein privates Inkassounternehmen zu beauftragen. Die Verarbeitung **strafrechtlich relevanter Daten** durch Private kommt nur ausnahmsweise unter den gesetzlich vorgesehenen Bedingungen in Frage. Eine solche Zulässigkeit war hier zu verneinen.

[BVwG 06.05.2025, W252 2271318-1](#)

#### **CAPTCHA, Zuständigkeit, Barrierefreiheit**

- Ein Websitebetreiber nutzte einen **CAPTCHA-Dienst**, der Cookies ohne Einwilligung setzte, um sich vor Spam zu schützen, als Schutz vor Überlastungsangriffen (**[D]DoS-Attacken**) und um die Website **barrierefrei** zu gestalten. Das Setzen der Cookies sei technisch notwendig, weil sonst ein Zugriff auf die Website unmöglich sei. Die Cookies erhoben die IP-Adressen, Nutzer-Identifikations-Nummern sowie Browserdaten. Ein Websitenutzer erachtete sich durch das Setzen der Cookies in seinem Recht auf Geheimhaltung verletzt und brachte Datenschutzbeschwerde bei der DSB ein. Die DSB gab der Datenschutzbeschwerde statt. Dagegen erhob der Websitebetreiber (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die DSGVO gilt für die Verarbeitung personenbezogener Daten, die **nicht** von der RL 2002/58/EG (**ePrivacyRL**, umgesetzt mit dem **TKG**) umfasst sind. Die DSGVO ist **lex generalis** für Sachverhalte, die nicht in der ePrivacyRL und dem TKG als **lex specialis** eigens geregelt sind. Für die Einhaltung des TKG ist gemäß § 191 ff TKG die **Fernmeldebehörde**, das **Fernmeldebüro** bzw die **RTR-GmbH**, nicht aber die DSB zuständig.

Fällt ein Sachverhalt unter beide Rechtsakte, sind die konkreten **Verarbeitungsvorgänge** zu **identifizieren** und den jeweiligen Bestimmungen **zuzuordnen**. Die DSB kann in Ausübung ihrer Zuständigkeit nach der DSGVO Bestimmungen des TKG nicht durchsetzen. Sie kann aber **vor** oder **nachfolgende Verarbeitungen**, für die keine spezielle Vorschrift nach der ePrivacyRL bzw dem TKG besteht, aufgreifen. Im Fall des CAPTCHA-Cookies sind die Token-Weitergabe, Risikoanalyse, Rückmeldung des Scores und daraus folgende Reaktionen Verarbeitungsvorgänge, die unter die DSGVO fallen.

Ein nachgelagerter Verarbeitungsvorgang kann nur rechtmäßig iSd DSGVO sein, wenn die Voraussetzungen des § 165 TKG erfüllt sind. Die Erfüllung der Voraussetzungen des TKG ist von der DSB als **Vorfrage** gemäß § 38 AVG nach eigener Anschauung zu beurteilen.

Die **Speicherung** und der **Zugriff** auf Informationen im Endgerät eines Teilnehmers oder Nutzers verlangt entweder eine **Einwilligung** oder ist nur erlaubt, wenn sie



**unbedingt erforderlich** ist. Unbedingt erforderlich ist der Zugriff/die Speicherung, um einen vom Teilnehmer **ausdrücklich gewünschten Dienst** zur Verfügung stellen zu können. Dabei handelt es sich um eine technisch-funktionale Anforderlichkeit. Entscheidend ist, ob sich der ausdrücklich gewünschte Dienst auch mit **weniger ein-griffsintensiven** Mitteln bereitstellen lässt, die technisch unbedingt notwendig sind.

Der Websitebetreiber hätte auf einen **datenschutzfreundlicheren CAPTCHA-Dienst** zurückgreifen können. Ein **barrierefreier Modus** lässt sich alternativ über einen Umschalt-Button aktivieren. Da die betroffene Person keine barrierefreie Version benötigte, war der Einsatz des Cookies nicht unbedingt erforderlich. Die Verarbeitung war daher ohne Einwilligung unzulässig. **Anm: Man könnte auch zum gegenteiligen Ergebnis gelangen. Der Einsatz des Umschalt-Buttons würde nämlich bedeuten, dass bei Nutzung dieses Buttons auf eine wahrscheinliche Behinderung (Gesundheitsdatum) des Nutzers geschlossen werden könnte. Da ohne Umschalt-Button diese Unterscheidung zwischen Nutzern nicht möglich ist, verstieße der Websitebetreiber gegen den Grundsatz der Datenminimierung. Überhaupt ist eine Rechtsprechung, die von Websitebetreibern verlangt, zwischen grundsätzlich geeigneten Diensten noch weiter zu differenzieren, kritisch zu sehen.**

BVwG 06.05.2025, W252 2293098-1

### **Staatsanwaltschaft, Akteneinsicht, Beschränkung**

- Strafrechtlich Beschuldigte erhoben Datenschutzbeschwerde, weil im Zusammenhang mit einer durch andere Beschuldigte erfolgten Akteneinsicht in den Ermittlungsakt der Staatsanwaltschaft auch ihre ungeschwärzten personenbezogenen Daten offengelegt wurden. Die Datenschutzbeschwerde wurde von der DSB mit der Begründung abgewiesen, dass einem Beschuldigten in einem Strafverfahren grundsätzlich das Recht auf Akteneinsicht zukomme. Eine Einschränkung bzw Verweigerung dieses Rechts sei im konkreten Fall nicht gerechtfertigt. Die Bescheidbeschwerde der Beschuldigten an das BVwG blieb erfolglos.

Das BVwG hat erwogen: Bei der Gewährung von **Akteneinsicht** durch die Staatsanwaltschaft liegt eine Verarbeitung personenbezogener Daten im Anwendungsbereich der Richtlinie (EU) 2016/680 (**DSRL**) vor. Die Umsetzung der DSRL erfolgte im 4. Abschnitt des 2. Hauptstückes sowie im 3. Hauptstück des **DSG**. Die **DSGVO ist nicht anwendbar**.

Da die **Staatsanwaltschaften** keine unabhängigen Justizbehörden bzw Gerichte iSd Art 45 Abs 2 DSRL sind, ist die **DSB** für die

Überprüfung von Datenverarbeitungen durch die Staatsanwaltschaften **zuständig**.

Die Staatsanwaltschaft darf gemäß **§ 74 Abs 1 erster Satz StPO** im Rahmen ihrer Aufgaben die hierfür erforderlichen personenbezogenen Daten verarbeiten. Die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen gehen **als leges speciales** den allgemeinen Regelungen des 3. Hauptstücks des DSG vor. Die Regelungen der StPO über Akteneinsicht oder Verständigungspflichten sind als derartige leges speciales anzusehen.

Die zulässigen **Beschränkungen** der Akteneinsicht bei Beschuldigten sind **abschließend** in **§ 51 Abs 2 StPO** geregelt. Eine Beschränkung ist demnach insbesondere nur insoweit zulässig, als aufgrund bestimmter Tatsachen zu befürchten ist, dass ein Zeuge oder ein Dritter durch die Kenntniserlangung des Beschuldigten von aktenmäßig festgehaltenen, somit nach § 53 Abs 1 StPO zugänglichen, personenbezogenen Daten und anderen Umständen (auch Textzusammenhängen), die Rückschlüsse auf die Identität oder die höchstpersönlichen Lebensumstände gefährdeter Personen zulassen, **einer ernststen Gefahr für Leben, Gesundheit, körperliche Unversehrtheit oder Freiheit** ausgesetzt würde.

Da die Beschuldigten **keine Umstände vorgebracht**, weshalb sie durch die Offenlegung einer solchen Gefahr ausgesetzt wären und diesbezügliche Anhaltspunkte auch sonst nicht hervorkamen, war kein Umstand ersichtlich, der eine Beschränkung der Akteneinsicht rechtfertigen würde. Die Offenlegung war daher rechtmäßig.

BVwG 07.05.2025, W176 2273922-1

### **Gerichtsverfahren, Rechtsanspruch, berechtigtes Interesse**

- Eine Exfrau führte einen Prozess über **Detektivkosten** gegen die neue Partnerin ihres Exmannes und beantragte **Verfahrenshilfe**. Dabei legte sie persönliche und wirtschaftliche Informationen offen, darunter Angaben zu ihrer psychischen Gesundheit. Die neue Partnerin leitete diese Unterlagen sowie einen Detektivbericht, der anlässlich des Scheidungsverfahrens erstellt wurde, per E-Mail an den Exmann weiter, um die Vermögensverhältnisse der Exfrau zu prüfen und gegebenenfalls eine Erschleichung der Verfahrenshilfe aufzudecken. Die Exfrau erachtete sich in ihrem Recht auf Geheimhaltung verletzt und erhob Datenschutzbeschwerde. Diese wurde in Bezug auf die Weitergabe des Detektivberichts abgewiesen. Hinsichtlich der Weiterleitung des Verfahrenshilfeantrags an den Exmann gab die DSB der Datenschutzbeschwerde teilweise statt. Es wäre ausreichend gewesen, eine Abklärung hinsichtlich der Vermögensverhältnisse

anhand der sich im Bewilligungsbeschluss befindlichen Daten vorzunehmen. Die neue Partnerin erhob Bescheidbeschwerde an das BVwG. Dieses gab der Bescheidbeschwerde Folge, hob den angefochtenen Bescheid im angefochtenen Umfang auf und verwies die Angelegenheit zur Erlassung eines neuen Bescheids an die DSB zurück. Der VwGH hob diesen Beschluss wegen Rechtswidrigkeit auf, weil das BVwG von der Rechtsprechung des VwGH zum Vorliegen der Voraussetzungen für eine Zurückverweisung abgewichen sei. Das BVwG gab der Bescheidbeschwerde daraufhin Folge und änderte den Bescheid der DSB dahingehend ab, dass die Datenschutzbeschwerde der Exfrau auch hinsichtlich der Weiterleitung des Verfahrenshilfeantrags abgewiesen wird.

Das BVwG hat erwogen: Die DSGVO ist anwendbar, weil die Datenweitergabe nicht ausschließlich persönlichen oder familiären Zwecken diene, sondern zur Unterstützung eines Scheidungsverfahrens und zur Beweissicherung erfolgte. Somit fiel die Datenverarbeitung nicht unter die **Haushaltsausnahme**.

Die Prüfung der Angaben zur Erhebung von Rechtsmitteln ist ein berechtigtes Interesse. Werden besondere Kategorien von Daten iSd Art 9 Abs 1 DSGVO verarbeitet, muss ein Erlaubnistatbestand des Art 9 Abs 2 DSGVO vorliegen. Art 9 verdrängt nicht Art 6 DSGVO, sondern formuliert erhöhte Rechtmäßigkeitsvoraussetzungen. **Art 9 Abs 2 lit f DSGVO** ist ein **Sonderfall** des allgemeinen Erlaubnistatbestands des **berechtigten Interesses**. Dadurch wird dem Recht des Einzelnen auf die effektive Rechtsdurchsetzung Vorrang vor den Interessen betroffener Personen am Schutz ihrer Daten eingeräumt, andernfalls der Einzelne an der Durchsetzung seiner Rechte und die Justiz an der Wahrnehmung ihrer Aufgaben gehindert wäre. Die Erforderlichkeit ist aus einer *ex-ante*-Sicht zu beurteilen, woraus sich ein gewisser Beurteilungsspielraum ergibt.

Im (gerichtlichen) Verfahren ist für eine erfolgreiche Prozessführung bzw Rechtsdurchsetzung oder -verteidigung die Vorlage von Beweismitteln erforderlich. Es liegt in der Natur der Sache, dass zur effektiven und zielführenden Prozessführung Daten der Gegenpartei verarbeitet werden (müssen). Die **Übermittlung des Verfahrenshilfeantrags** samt der darin enthaltenen personenbezogenen Daten an den Exmann, der die Angaben überprüfen konnte und dem diese auch bereits bekannt waren, war jedenfalls denkmöglich zur Verteidigung in einem Rechtsstreit und somit zur Verteidigung eines Rechtsanspruchs geeignet, zumal die Ermittlung der nötigen Beweismittel und deren Anbieten grundsätzlich den Verfahrensparteien obliegt.

Für die **Beurteilung der Rechtmäßigkeit** der Datenverarbeitung zur Durchsetzung zivilrechtlicher Ansprüche kommt es auch nicht darauf an, ob sich *ex post* herausstellt, dass die Datenverarbeitung im Prozess nicht zum Erfolg gereicht hat, sondern lediglich darauf, ob die vorgelegten Unterlagen *ex ante* denkmöglich als Beweismittel geeignet waren. **Gelindere Mittel** sind nicht ersichtlich. Eine Übermittlung bloß des Gerichtsbeschlusses, in dem über die Verfahrenshilfe abgesprochen wurde, wäre nicht ausreichend gewesen, weil darin nicht alle Angaben enthalten waren, die zur Beurteilung, ob die beantragte Verfahrenshilfe der Exfrau auch zusteht, notwendig sind.

Da die Daten dem Exmann bereits bekannt waren, ist das **Geheimhaltungsinteresse** der Exfrau nur **gering**. Die Interessenabwägung fällt daher zugunsten der neuen Partnerin aus. Der Eingriff in das Recht auf Datenschutz der Exfrau ist verhältnismäßig. Die Beschränkung des Geheimhaltungsanspruchs der Exfrau ist zur Wahrung überwiegender berechtigter Interessen der neuen Partnerin gemäß Art 6 Abs 1 lit f und Art 9 Abs 2 lit f DSGVO gerechtfertigt und damit zulässig. Auch der Grundsatz **der Datenminimierung** wurde eingehalten, weil nur solche Daten übermittelt wurden, die zur Zielerreichung nötig waren.

#### Aus der weiteren Rechtsprechung des BVwG:

- Ein Betroffener verlangte die Herausgabe eines Passworts von einem Unternehmer, der dieses Passwort nicht hatte und auch nicht mit **legalen Mitteln** erlangen konnte. Daraufhin leitete der Unternehmer die E-Mail-Adresse des Betroffenen zu den Zwecken der Kundenzufriedenheit und der Passwortherausgabe an jenen Dritten weiter, der das Passwort hatte und dem Betroffenen bereitstellen konnte. Da dem Unternehmer **kein gelinderes Mittel** zur Verfügung stand und die Weiterleitung der E-Mail-Adresse zur Herausgabe des Passworts erforderlich war, verstieß der Unternehmer nicht gegen den Grundsatz der **Datenminimierung**. Die **Datenweitergabe** war rechtmäßig ([BVwG 08.05.2025, W274 2257892-1](#)).
- Behebt die DSB einen Zurückweisungsbescheid, weil einem Mangelbehebungsauftrag – anders als ursprünglich angenommen – rechtzeitig entsprochen wurde, entfällt die **Beschwer** des Betroffenen. Da somit kein **objektives Rechtsschutzinteresse** des Betroffenen vorliegt, ist die Bescheidbeschwerde an das BVwG zurückzuweisen ([BVwG 12.05.2025, W292 2311008-1](#)).
- Hat der Bescheid der DSB dem Antrag des Betroffenen **vollinhaltlich entsprochen**, ist die Bescheidbeschwerde an das BVwG **mangels Beschwer** zurückzuweisen ([BVwG 08.05.2025, W292 2310611-1](#)).

- Wird die **Bescheidbeschwerde** an das BVwG **zurückgezogen**, ist das Verfahren mit Beschluss **einzustellen** (BVwG [02.05.2025, W292 2285392-1](#); [02.05.2025, W292 2285923-1](#)).

### **EU-Rechtsakte**

- Am **10.07.2025** wurde der "[KI-Verhaltenskodex für allgemeine Zwecke](#)" veröffentlicht. Der Verhaltenskodex ist in die drei Kapitel **Sicherheit und Gefahrenabwehr, Transparenz** und **Urheberrecht** unterteilt. Der Verhaltenskodex wurde von unabhängigen Experten ausgearbeitet und wird in den folgenden Wochen von den Mitgliedstaaten und der Europäischen Kommission auf ihre Angemessenheit bewertet werden.

to the point

# Datenschutzmonitor. 29/2025 vom 23.07.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuG**

EuG 16.07.2025, T-183/23, *Ballmann/EDSA* (EDSA, Aktenzugang, Kohärenzverfahren)

- **Rechtsprechung des VwGH**

VwGH 25.06.2025, Ra 2024/12/0115 (Auskunftersuchen, Auslegung, Revision)

- **Rechtsprechung der Justiz**

OLG Linz 10.04.2025, 1R32/25v (Videoüberwachung, § 12 DSG, Überwachungsdruck)

OLG Wien 27.01.2025, 16R43/24x (Auskunft, Rechtsmissbrauch, Prozessposition)

- **Rechtsprechung des BVwG**

BVwG 16.05.2025, W296 2310875-1 (Datenzugriff, Amtsmissbrauch, Verjährung)

BVwG 13.05.2025, W258 2224654-1 (Obsorge, Verwaltungshandeln, Personenstand)

BVwG 09.05.2025, W291 2301858-1 (Auskunftsrecht, Auskunftersuchen)

BVwG 08.05.2025, W171 2251246-1 (Auskunft, aufschiebende Wirkung)

BVwG 06.05.2025, W298 2309832-1 (Zuständigkeit, justizielle Tätigkeit, Kostenersatz)

- **Rechtsprechung der BDB**

BDB 07.05.2025, 2024-0.832.779 (Polizei, Abfrage, Zentrales Melderegister)

BDB 29.04.2025, 2025-0.175.429 (Aktenverwaltungssystem der Polizei, Abfrage)

- **EU-Rechtsakte**

Angemessenheitsbeschluss (EU) 2025/1382 für die Europäische Patentorganisation

Durchführungsverordnung (EU) 2025/1410 betreffend die Kennzeichnung und Transparenzbeachtmachung politischer Werbung

Durchführungsverordnung (EU) 2025/1420 zur Einrichtung und Betrieb von Interoperabilitäts-Reallaboren

- **Nationale Rechtsakte**

Burgenländisches Informationsfreiheits-Anpassungsgesetz

Kärntner Informationsfreiheits-Anpassungsgesetz

## To the Point:

### Rechtsprechung des EuG

EuG 16.07.2025, T-183/23, Ballmann/EDSA

#### **EDSA, Aktenzugang, Kohärenzverfahren**

- Eine Nutzerin reichte eine Datenschutzbeschwerde bei der DSB gegen (damals Facebook und nunmehr) Meta ein. Die DSB leitete die Datenschutzbeschwerde an die irische Aufsichtsbehörde weiter, weil sie der Ansicht war, dass diese als federführende Aufsichtsbehörde zuständig war. Die irische Aufsichtsbehörde legte den Aufsichtsbehörden der anderen Mitgliedstaaten des EWR-Raumes einen Beschlussentwurf vor, gegen den mehrere Aufsichtsbehörden begründeten Einspruch erhoben.

Dieser Beschlussentwurf wurde der Nutzerin von der irischen Aufsichtsbehörde übermittelt. Anschließend kam es jedoch zu einer Meinungsverschiedenheit zwischen der Nutzerin und der irischen Aufsichtsbehörde. Die Nutzerin erhielt daher weder Zugang zu den Einsprüchen der anderen Aufsichtsbehörden noch zur Stellungnahme von Meta.

Die irische Aufsichtsbehörde leitete das **Kohärenzverfahren** ein, damit der **Europäische Datenschutzausschuss (EDSA)** zu den Einsprüchen Stellung nehme, woraufhin die Nutzerin Akteneinsicht vom EDSA verlangte. Der EDSA teilte der Nutzerin daraufhin mit, dass Akteneinsicht nur jenen Parteien gewährt wird, die vom verbindlichen Beschluss des EDSA **nachteilig betroffen** sein könnten. Die Nutzerin könne von diesem Beschluss nicht nachteilig betroffen werden, weshalb ihr keine Akteneinsicht gewährt wird. Im anschließend erlassenen verbindlichen Beschluss 3/2022 bekräftigte der EDSA erneut, dass der Nutzerin kein Parteiengehör und kein Aktenzugang zu gewähren war.

Nachdem die Nutzerin erneut Aktenzugang verlangte, wurden ihr zwar begründete Einsprüche einzelner Aufsichtsbehörden, aber nicht der gesamte Akteninhalt zur Verfügung gestellt. Der EDSA entschied, der Nutzerin keinen vollständigen Aktenzugang zu gewähren. Gegen diese **Entscheidung des EDSA** richtete sich die erfolgreiche Klage der Nutzerin.

Das EuG hat erwogen: Strittig zwischen den Parteien ist, ob Aktenzugang nur einer Person zu gewähren ist, die von einem Verfahren **nachteilig betroffen** ist, oder jeder Person, die von einem Verfahren **betroffen** ist. Die Nutzerin stellte ihren **Antrag auf Aktenzugang**, nachdem die Verfahren vor dem EDSA und der irischen Aufsichtsbehörde abgeschlossen waren. Ihr ging es somit nicht um das Parteiengehör, sondern um die Informationen im Akt.

Das **Recht auf Parteiengehör** gemäß Art 41 Abs 2 lit a GRC ist zwar tatsächlich auf Verfahren beschränkt, in welchen die Person nachteilig betroffen sein kann. Das Recht auf Aktenzugang gemäß Art 41 Abs 2 **lit b** GRC ist jedoch nicht in derselben Weise beschränkt und kann über das Recht auf Parteiengehör hinausgehen. Jede Person hat daher ein Recht auf Zugang zu den **sie betreffenden Akten**, auch wenn sie durch die Entscheidung in diesem Verfahren nicht nachteilig betroffen sein kann.

Zu prüfen ist daher, ob die Nutzerin durch den Akt **betroffen** war. Der **EDSA** ist im Kohärenzverfahren ein Vermittler, der Meinungsverschiedenheiten zwischen der federführenden Aufsichtsbehörde und beteiligten Aufsichtsbehörden beilegt. Der Verfasser einer Datenschutzbeschwerde ist förmlich keine Partei des Verfahrens vor dem EDSA. Die Datenschutzbeschwerde spielt im Verfahren vor dem EDSA jedoch eine wesentliche Rolle, weil der EDSA bei seiner Entscheidung die Tatsachen und Argumente in der Datenschutzbeschwerde zumindest berücksichtigt. Dementsprechend bezog sich der EDSA in seinem verbindlichen Beschluss 3/2022 mehrfach auf die Datenschutzbeschwerde und auch auf die Nutzerin. Der Akt des EDSA zur Vorbereitung des Erlasses des verbindlichen Beschlusses 3/2022 **betrifft** somit die Nutzerin. Ihr ist daher **Aktenzugang** zu gewähren.

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Die **Auslegung eines Auskunftersuchens** ist keine Rechtsfrage von grundsätzlicher Bedeutung und ist somit **nicht revisibel**, soweit nicht aufgezeigt wird, dass weitere Ermittlungen zur Festlegung des Inhalts des Auskunftersuchens erforderlich gewesen wären ([VwGH 25.06.2025, Ra 2024/12/0115](#)).

### Rechtsprechung der Justiz

OLG Linz 10.04.2025, 1R32/25v

#### **Videoüberwachung, § 12 DSG, Überwachungsdruck**

- Ein Kommunikationsnetzbetreiber montierte auf einem Grundstück eine Überwachungskamera. Der Geschäftsführer des Unternehmens war zugleich Eigentümer der Liegenschaft. Die Kamera diente der Überwachung des Gebäudes und der E-Ladestation, erfasste jedoch auch öffentliche Verkehrsflächen sowie den Bereich vor dem Lieferanteneingang eines benachbarten Geschäftsgebäudes. Dieses stand im Eigentum einer GmbH. Deren Geschäftsführer sowie die GmbH begeherten die Beseitigung der Kamera sowie die Unterlassung der

Überwachung. Das LG Salzburg stellte fest, dass ein Eingriff in die Privatsphäre vorliege, weil die Kamera den Bereich bis knapp vor die Hausmauer der GmbH wie auch den Bereich vor dem Lieferanteneingang und öffentlich zugängliche Orte filme. Diese unterlägen nicht dem Hausrecht des Grundstückseigentümers. Dagegen erhob der Kommunikationsnetzbetreiber (erfolglos) Berufung an das OLG Linz.

Das OLG Linz hat erwogen: Die Bestimmung des **§ 12 DSGVO** regelt die Zulässigkeitserfordernisse für eine **Bildaufnahme**. In § 12 Abs 3 DSGVO wird die **Interessenabwägung** bereits auf gesetzlicher Ebene für "*quasi massenhaft auftretende Fallkonstellationen*" vorgenommen. Von den dort normierten Tatbeständen kommt jener des § 12 Abs 3 Z 1 DSGVO (vorbeugender Schutz von Personen oder Sachen auf privaten Liegenschaften) schon deshalb nicht in Betracht, weil der überwiegend durch die Kamera überwachte Bereich nicht Schutzziel ist und zum Großteil Flächen umfasst, die als öffentliche Verkehrsflächen genutzt werden.

Eine schwerwiegende **Beeinträchtigung der Privatsphäre** liegt bereits dann vor, wenn sich die Person durch die Überwachungsmaßnahme einer Videokamera kontrolliert fühlen musste. Dabei ist auf den **Überwachungsdruck** abzustellen, den der Überwachte empfindet.

Der **Aufnahmebereich der Kamera** geht über den Nahbereich der E-Ladestation hinaus. Der Kommunikationsnetzbetreiber hat kein berechtigtes Interesse daran, zu erfahren, wann und wie oft Lieferanten oder sonstige Nutzer die Liegenschaft über den Lieferanteneingang der GmbH betreten oder verlassen. **Anm: Hinsichtlich der §§ 12 und 13 DSGVO (Bildverarbeitung, insb Videoüberwachung) besteht eine Judikaturdivergenz zwischen den Rechtsprechungen im Zivil- und Verwaltungsrechtsweg. Die DSB und das BVwG lassen diese Bestimmungen wegen (vermeintlichem) Vorrang des Unionsrechts unangewendet. Die Zivilgerichte wenden diese Bestimmungen an.**

OLG Wien 27.01.2025, 16R43/24x

### **Auskunft, Rechtsmissbrauch, Prozessposition**

- Eine Spielerin war Kundin eines **Online-Glücksspielunternehmens**, welches über keine österreichische Glücksspielkonzession verfügte. Das Glücksspielunternehmen bot ihre Website auf deutscher Sprache an und die Website war in Österreich abrufbar. Nach Löschung ihres Accounts stellte die Spielerin ein schriftliches Auskunftsersuchen an das Glücksspielunternehmen und verlangte eine richtige und vollständige Aufstellung ihrer sämtlichen Gewinne und Verluste, die sie auf der Website erzielt oder erlitten hatte.

Nachdem das Glücksspielunternehmen dem Ersuchen nicht vollständig nachkam, brachte sie eine **Auskunftsklage** ein und begehrte eine Kopie sämtlicher ihrer Daten. Gegen das dem Klagebegehren stattgebende Urteil des Erstgerichts legte das Glücksspielunternehmen eine (erfolglose) Berufung beim OLG Wien ein. Das Glücksspielunternehmen argumentierte, das Auskunftsersuchen sei rechtsmissbräuchlich, weil die Spielerin damit bloß ein Beweismittel für einen Zivilprozess gegen das Unternehmen erlangen wolle.

Das OLG Wien hat erwogen: Der Zweck des Auskunftsrechts liegt darin, in Erfahrung zu bringen, ob und welche Daten der Verantwortliche über die Betroffene verarbeitet und ob dies rechtmäßig geschieht. Das Auskunftsrecht steht unter **keinen Voraussetzungen** und muss nicht mit **einem Rechtsschutzinteresse** begründet werden. Der Verantwortliche darf das Motiv des Auskunftsersuchens nicht prüfen. Rechtsmissbrauch liegt nur vor, wenn zwischen den verfolgten eigenen Interessen und den beeinträchtigten Interessen des anderen ein **krasses Missverhältnis** besteht. Es muss der Schädigungszweck bzw das unlautere Motiv der Rechtsausübung im Vordergrund stehen.

Die Geltendmachung von erlittenen Spielverlusten durch einen Kläger ist weder ein unlauteres Verhalten noch tritt das Auskunftsrecht hinter ein allenfalls berechtigtes Geheimhaltungsinteresse des Beklagten zurück. Eine **Auskunftspflicht** besteht auch dann, wenn das Auskunftsersuchen keinem der in ErwGr 63 DSGVO genannten Zwecke (Überprüfung der Rechtmäßigkeit, Bewusstsein der Verarbeitung) dient. Die Auskunftserteilung kann nicht bloß deshalb abgelehnt werden, weil damit primär die **Beweismittelbeschaffung** beabsichtigt wird. Ein Auskunftsersuchen ist auch nicht offenkundig unbegründet oder rechtsmissbräuchlich, wenn damit **datenschutzfremde Ziele** verfolgt werden.

Auch lässt sich **kein Schädigungszweck** erkennen. Das Einklagen von einem allfälligen **Saldo** ist ein legitimes Interesse der Spielerin. Ein berechtigtes Geheimhaltungsinteresse gemäß **§ 4 Abs 6 DSGVO** iVm Art 15 Abs 4 DSGVO aufgrund der durch die Informationsherausgabe drohenden Schwächung ihrer **Prozessposition** (gemeint in einem zukünftigen Leistungsverfahren wegen Glücksspielverlusten) kommt dem Glücksspielunternehmen nicht zu. Denn die Spielerin ersucht um die Herausgabe von Daten aus gemeinsamen Geschäftsbeziehungen, sodass **kein Geheimnis** des Glücksspielunternehmens gegenüber der Klägerin besteht. Das Glücksspielunternehmen kann die Auskunft nicht mit dem Argument verweigern,

die Daten seien nach Löschung des Accounts für die Klägerin "geheim".

## Rechtsprechung des BVwG

BVwG 16.05.2025, W296 2310875-1

### **Datenzugriff, Amtsmissbrauch, Verjährung**

- Ein Beamter griff ohne dienstliche Veranlassung 19-mal auf seine eigenen Steuerdaten und die Steuerdaten seiner Mutter zu. Wegen anderer dienstrechtlicher Verstöße waren bereits ein Disziplinarverfahren bei der **Bundesdisziplinarbehörde (BDB)** und ein Ermittlungsverfahren wegen des Verdachts des **Amtsmissbrauchs und Abgabenhinzerziehung** bei der **Staatsanwaltschaft (StA)** anhängig. Erst durch den im Ermittlungsverfahren der StA erstellten Bericht erlangte die Disziplinarbehörde Kenntnis von den 19 Zugriffen. Aufgrund der Anzeige der Disziplinarbehörde leitete die Bundesdisziplinarbehörde mit **Nachtragseinleitungsbeschluss** ein weiteres Disziplinarverfahren gegen den Beamten ein. Da der Beamte die Vorwürfe als **verjährt** erachtete, brachte er gegen den Beschluss erfolgreiche Bescheidbeschwerde an das BVwG ein, welches den Beschluss ersatzlos behob und das Disziplinarverfahren wegen Verjährung einstellte.

Das BVwG hat erwogen: Die **Verjährung** einer Dienstpflichtverletzung ist gemäß § 94 Abs 2 BDG unter anderem **gehemmt**, wenn der der Dienstpflichtverletzung zugrundeliegende Sachverhalt bei einem Verwaltungsgericht oder einem Strafverfahren nach der StPO anhängig ist. Ist eine Straftat im Zeitpunkt der Einstellung des Ermittlungsverfahrens der StA nicht bekannt, so ist sie nicht Gegenstand des strafgerichtlichen Ermittlungsverfahrens.

Eine **Verjährung** gemäß § 94 Abs 1 Z 3 BDG tritt nicht ein, wenn ein **fortgesetztes Delikt** vorliegt. Diesfalls beginnt die **Verjährungsfrist** von drei Jahren nach Beendigung der Dienstpflichtverletzung, somit nach der letzten Abfrage, zu laufen. Ein **fortgesetztes Delikt** liegt nach der Judikatur vor, wenn mehrere gesetzwidrige Einzelhandlungen mit gleichartiger Begehungsweise und vergleichbaren äußeren Begleitumständen innerhalb eines erkennbaren zeitlichen Zusammenhangs begangen werden. Diese müssen durch einen vorab gefassten Gesamtvorsatz zu einer Bewertungseinheit verbunden sein.

Der **Gesamtvorsatz** muss sich auf die sukzessive Verwirklichung eines in groben Zügen feststehenden Gesamtziels richten. Ein allgemeines Motiv, zB bei jeder Gelegenheit gleichartige strafbare Handlungen zu begehen, ist kein Gesamtvorsatz.

Die übrigen Voraussetzungen für ein fortgesetztes Delikt lagen zwar vor, ein Gesamtvorsatz konnte jedoch nicht festgestellt

werden. Daher liegt kein fortgesetztes Delikt vor, weshalb **Verjährung** eingetreten ist.

BVwG 13.05.2025, W258 2224654-1

### **Obsorge, Verwaltungshandeln, Personenstand**

- Ein Vater erachtete sich durch ein Stadtmagistrat in seinem Recht auf Geheimhaltung verletzt. Die Abteilung Gesundheitswesen habe ab dem Jahr 2011 personenbezogene Daten über ihn in mehreren Akten unzulässig verarbeitet, innerhalb des Stadtmagistrats weitergegeben und seinem früheren Arbeitgeber kommuniziert. Auch seien ein Bescheidentwurf und ein Schriftsatz der Magistratsabteilung an den Bürgermeister weitergeleitet worden.

Der Vater monierte weiters die Weitergabe (i) seiner Daten an den stellvertretenden Abteilungsleiter und an eine Mitarbeiterin der Abteilung Gesundheitswesen, (ii) des Beschlusses zur gerichtlichen Feststellung seiner Vaterschaft durch das Standesamt des Stadtmagistrats an die zuständige italienische Konsularbehörde, (iii) seiner Daten an ein Bundesland zur Einholung einer Rechtsauskunft über die Geburtsbeurkundung seines Sohnes sowie (iv) seiner Daten an seine frühere Allgemeinmedizinerin.

Die Datenschutzbeschwerde wurde neben dem Vater auch im Namen des minderjährigen Sohnes eingebracht. Die DSB wies die Datenschutzbeschwerde hinsichtlich des Vaters ab und hinsichtlich des Sohnes mangels Vertretungsvollmacht zurück. Daraufhin erhob der Vater eine (teilweise erfolgreiche) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die **Datenverarbeitungen** der Abteilung Gesundheitswesen des Stadtmagistrats waren durch **§ 34a Abs 1 lit m iVm lit a und l Rehabilitationsgesetz** gerechtfertigt. Ein Verstoß gegen § 6 Abs 1 Z 4 DSGVO 2000 lag nicht vor, weil die verwendeten Daten im Hinblick auf den Verwendungszweck sachlich richtig waren.

Die Beauftragung des stellvertretenden Abteilungsleiters durch die Leiterin der Magistratsabteilung und die Information der betroffenen Mitarbeiterin über die Vorwürfe waren nicht rechtswidrig. Diese Verarbeitung war durch das **öffentliche Interesse am Funktionieren der Verwaltung** gedeckt.

Die Vorlage von **Entwürfen an den Bürgermeister** zur Unterzeichnung ist gemäß Art 6 Abs 1 lit e DSGVO iVm §§ 6 und 13 AVG zulässig. Es bestand ein **öffentliches Interesse** an der Bearbeitung des Anbringens des Vaters sowie an der verwaltungsgerichtlichen Vertretung der Stadt.

Die Übermittlung von **Personenstandsurkunden** durch das Standesamt an die **Konsularabteilung der Italienischen**

**Botschaft** in Wien war gemäß **§ 52 Abs 1 Z 2 Personenstandsgesetz 2013** gerechtfertigt. Der Beschluss zur gerichtlichen Feststellung der Vaterschaft war für die Vervollständigung des Personenstandsregisters erforderlich.

Die Übermittlung eines Anbringens an das Bundesland zur **Einholung einer Rechtsauskunft** war gemäß **§ 64 Personenstandsgesetz 2013** sowie § 6 Abs 1 Z 3 DSG 2000 zulässig. Keine oder eine anonymisierte Übermittlung wäre nicht ausreichend gewesen.

Die Weitergabe personenbezogener Daten an die **frühere Allgemeinmedizinerin** des Vaters ist eine Übermittlung iSd § 4 Z 12 DSG 2000. Die Ärztin hat die betreffenden Informationen aus eigener Wahrnehmung in ihrer Funktion als Amtsärztin des Stadtmagistrats dokumentiert. Die Protokollierung diente der **Nachvollziehbarkeit des Verwaltungshandelns** und war gemäß § 8 Abs 1 Z 4 iVm Abs 3 Z 1 DSG 2000 gerechtfertigt. Zweck und Inhalt der Übermittlung bezogen sich auf die Feststellung einer möglichen Befangenheit im Rahmen eines bestehenden Behandlungsverhältnisses.

Nur die **Weitergabe** von Informationen an den **früheren Arbeitgeber** war rechtswidrig. Damit verletzte der Magistrat den **Grundsatz der Datenminimierung** (Art 5 Abs 1 lit c DSGVO), weil der Zweck auch mit einer Nachfrage beim Vater erreicht worden wäre.

**Prozessunfähige** können rechtswirksam nur durch ihren gesetzlichen Vertreter handeln. Anträge sind daher entweder vom gesetzlichen Vertreter einzubringen oder zu genehmigen. Dem Vater steht die **Obsorge** für seinen minderjährigen Sohn nicht zu. Er legte trotz des von der DSB erteilten Mängelbehebungsauftrags gemäß § 9 Abs 3 AVG keine **Genehmigung der Kindesmutter** zur Verfahrensführung vor. Die **Zurückweisung** hinsichtlich des minderjährigen Sohnes erfolgte somit zu Recht.

#### Aus der weiteren Rechtsprechung des BVwG:

- Der Betroffene soll das **Auskunftsrecht** gemäß Art 15 DSGVO "problemlos" und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung seiner personenbezogenen Daten bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Die DSGVO verlangt für das **Auskunftsersuchen** keine bestimmte Form, sodass der Antrag grundsätzlich mündlich oder schriftlich gestellt werden kann. Wird die Eigenschaft als Betroffene verneint, besteht jedoch keine Rechtsgrundlage für die DSB, einen Bescheid gegen den Verantwortlichen zu erlassen ([BVwG 09.05.2025, W2912301858-1](#)).

- Ein Ermittlungsverfahren, in dem (i) zu prüfen ist, ob eine Auskunftspflicht in internen **Personalsachen** besteht, (ii) zu ermitteln ist, ob und inwieweit **auskunftshindernde Gründe** (wie Verschwiegenheitspflichten, Datenschutz etc) bestehen und (iii) eine Interessenabwägung vorzunehmen ist, ist so aufwändig, dass der verpflichteten Behörde ein unverhältnismäßiger Nachteil droht, wenn erst im Revisionsverfahren zu klären wäre, ob ein solches Verfahren überhaupt durchzuführen ist. Die gesetzlichen Voraussetzungen für die **Zuerkennung der aufschiebenden Wirkung** liegen daher vor ([BVwG 08.05.2025, W1712251246-1](#) bzw [W2872251246-1](#)). **Anm: In der Evidenzstelle des BVwG dürften derzeit Unstimmigkeiten vorliegen. Immer wieder werden Entscheidungen im RIS unter einer anderen Geschäftszahl veröffentlicht als in der Entscheidung selbst angegeben. Zur besseren Auffindbarkeit zitieren wir daher die im RIS angeführten Geschäftszahlen.**
- Die datenschutzrechtliche Kontrolle des BVwG bei der Ausübung von Parteienrechten greift in die **justizielle Tätigkeit** des BVwG ein. Für die Behandlung einer Beschwerde wegen einer behaupteten Rechtswidrigkeit der Datenverarbeitung durch das BVwG ist die DSB daher **unzuständig**. Für Beschwerden wegen Verletzung der Unterrichtungspflicht ist **kein Kostenersatz** vorgesehen. Jede Partei hat im Verwaltungsverfahren ihre eigenen Kosten zu tragen ([BVwG 06.05.2025, W2982309832-1](#)).

#### Rechtsprechung der Bundesdisziplinarbehörde (BDB)

##### Aus der Rechtsprechung der BDB

- Exekutivbeamte der Polizei haben Zugriffsberechtigungen auf alle relevanten polizeilichen Datenbanken, wie das PAD, E-KIS und das **Zentrale Melderegister (ZMR)**. Die Mitarbeiter der Polizei haben zur Erfüllung ihrer Aufgaben umfangreiche Berechtigungen. Ohne dienstlichen Grund sind sie jedoch nicht berechtigt, in das ZMR Einsicht zu nehmen. Die Befriedigung eines privaten Informationsbedürfnisses berechtigt weder die Verwendung der dienstlichen IT-Ressourcen, noch die Abfrage von Daten aus dem Melderegister ([BDB 07.05.2025, 2024-0.832.779](#)).
- Die Polizeibehörden dürfen Anfragen im internen **Aktenverwaltungssystem der Polizei (PAD)** ausschließlich im Zusammenhang mit der Erfüllung der **dienstlichen Aufgaben** durchführen. Ein Missbrauch liegt immer dann vor, wenn eine Abfrage **ohne dienstliche Gründe** erfolgt. Durch die gesetz- und erlasswidrige PAD-Abfrage wird unberechtigt auf Datenbanken des BMI



### EU-Rechtsakte

- Am **18.07.2025** ist der "*Durchführungsbeschluss (EU) 2025/1382 der Kommission vom 15. Juli 2025 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die **Angemessenheit des Schutzes personenbezogener Daten durch die Europäische Patentorganisation***", [ABI L 2025/1382](#), kundgemacht worden. Neben der Übermittlung personenbezogener Daten in Drittländer bedarf auch die Übermittlung personenbezogener Daten an **internationale Organisationen** besonderer Garantien. Die höchste Rechtssicherheit unter den möglichen Garantien bieten die Angemessenheitsbeschlüsse der Europäischen Kommission. Während die Kommission für über ein Dutzend Drittstaaten entsprechende [Angemessenheitsbeschlüsse](#) erlassen hat, ist die **Europäische Patentorganisation** die erste internationale Organisation, die in den Genuss eines solchen Beschlusses kommt.
- Am **16.07.2025** ist die "*Durchführungsverordnung (EU) 2025/1410 der Kommission vom 9. Juli 2025 über das Format, das Muster und die technischen Spezifikationen der Kennzeichnungen und Transparenzbekanntmachungen politischer Anzeigen gemäß den Artikeln 11 und 12 der Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates*", [ABI L 2025/1410](#), kundgemacht worden. Mit dieser DurchführungsVO werden **technische Spezifikationen** für die **Kennzeichnung und Transparenzbekanntmachung von politischen Anzeigen** festgelegt. Besondere Anforderungen sind für (i) Anzeigen im Fernsehen und Radio, (ii) Printmedien und (iii) digitale Medien vorgesehen.
- Am **18.07.2025** ist die "*Durchführungsverordnung (EU) 2025/1420 der Kommission vom 17. Juli 2025 mit Durchführungsbestimmungen zur Verordnung (EU) 2024/903 des Europäischen Parlaments und des Rates hinsichtlich der Einrichtung und des Betriebs von **Interoperabilitäts-Reallaboren***", [ABI L 2025/1420](#), kundgemacht worden. Die "*Verordnung (EU) 2024/903 für ein interoperables Europa*" zielt auf die Stärkung der grenzüberschreitenden Interoperabilität von Netz- und Informationssystemen ab, die für die Erbringung oder **Verwaltung öffentlicher Dienste in der Union** verwendet werden. Mit der nunmehrigen DurchführungsVO wurde die Rechtsgrundlage für die **Einrichtung und den Betrieb von Interoperabilitäts-Reallaboren** geschaffen.

### Nationale Rechtsakte

- Am **17.07.2025** ist das **Burgenländische Informationsfreiheits-Anpassungsgesetz**, [LGBI 2025/58](#), kundgemacht worden. Mit dieser Sammelnovelle werden über 30 burgenländische Gesetze an das neue **Grundrecht auf Information**, das mit all seinen Einschränkungen die ehemalige Amtsverschwiegenheit ablöst, angepasst. Das neue Grundrecht auf Information bzw. auf Zugang zu Informationen wird ab **01.09.2025** verfassungsgesetzlich gewährleistet.
- Am **15.07.2025** ist das **Kärntner Informationsfreiheits-Anpassungsgesetz**, [LGBI 2025/47](#), kundgemacht worden. Mit dieser Sammelnovelle werden die **Kärntner Landesverfassung** und über 50 Kärntner Landesgesetze an das neue **Grundrecht auf Information** angepasst.

to the point

# Datenschutzmonitor. 30/2025 vom 30.07.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung der Justiz**

OGH 03.07.2025, 6Ob113/24x (Marketingklassifikationen, kein Schadenersatz ohne Schaden)

OGH 03.07.2025, 6Ob53/25z (Recht am eigenen Wort, Tonbandaufnahme, Beweismittel)

OGH 03.07.2025, 6Ob62/25y (Doppelgleisigkeit des Rechtsschutzes, Behörde, beliehenes Unternehmen, Unterlassungsanspruch)

- **Rechtsprechung des BVwG**

BVwG 06.05.2025, W271 2303184-1; 07.05.2025, W282 2303188-1; 08.05.2025, W179 2303090-1 (Cold Calling, Geldstrafe, Rechtsauskunft)

BVwG 20.05.2025, W256 2310929-1 (Zurückziehung der Säumnisbeschwerde)

BVwG 09.05.2025, W605 22985459-1 (Verfahrenseinstellung, gekürzte Ausfertigung)

- **Rechtsprechung des BFG**

BFG 27.06.2025, RV/3100085/2025 (Eingabengebühr, Verfahrenshilfe)

- **EU-Rechtsakte**

Erläuterung und Vorlage für die öffentliche Zusammenfassung von Schulungsinhalten für KI-Modelle mit allgemeinem Verwendungszweck

- **Nationale Rechtsakte**

Datenzugangsgesetz

Informationsfreiheits-Anpassungsgesetz

Änderung des Bankwesengesetzes

Änderung des Informationsordnungsgesetzes sowie des Parlamentsmitarbeiterinnen- und Parlamentsmitarbeitergesetzes

Änderung des Strafgesetzbuches

Änderung der Nummernübertragungsverordnung 2022

Änderung der Informationssicherungsverordnung

MiCAR-Emittenten-Meldeverordnung

Salzburger Informationsfreiheits-Anpassungsgesetz

Oö. Informationsfreiheits-Anpassungsgesetz

Oö. TDB-Begleitregelungsgesetz

Oö. Archivgesetz-Novelle 2025

## To the Point:

### Rechtsprechung der Justiz

OGH 03.07.2025, 6Ob113/24x

#### **Marketingklassifikationen, kein Schadenersatz ohne Schaden**

- Ein Rechtsanwalt erachtete sich durch einen Adressverlag in seiner Rechtssphäre beeinträchtigt. Der Adressverlag verarbeitete Daten über bestimmte Affinitäten des Rechtsanwalts (Bioaffinität, Nachtschwärmer, Heimwerkereigenschaft, Lebensphase, Investment-Affinität, Distanzhandels-Affinität und Kinderlosigkeit). Bei fünf dieser Zuordnungen entsprach die Einstufung der Realität; es wurde jedoch nicht festgestellt, bei welchen. Der Rechtsanwalt sah in der Verarbeitung der zutreffenden Affinitäten eine deutliche Beeinträchtigung seiner Rechtssphäre, in der Verarbeitung der unzutreffenden Affinitäten nur eine geringe. Er beehrte dafür **Schadenersatz wegen unrechtmäßiger Datenverarbeitung**. Das Erstgericht (LG Wels) wies die Klage ab, weil die Erheblichkeitsschwelle nicht erreicht sei. Das Berufungsgericht (OLG Linz) bestätigte dieses Urteil. Es hielt weiters fest, dass überhaupt kein Schaden vorliege. Daraufhin erhob der Rechtsanwalt (erfolglos) Revision an den OGH.

Der OGH hat erwogen: Die Affinitäten sind **Marketinginformationen und -klassifikationen iSd § 151 Abs 6 GewO**. Diese unterliegen der DSGVO, auch wenn sie aus statistischen Wahrscheinlichkeiten errechnet werden und insofern (nur) eine **Wahrscheinlichkeitsaussage** über bestimmte Interessen des Rechtsanwalts enthalten.

Der bloße Verstoß gegen die DSGVO reicht jedoch nicht aus, um einen **Schadenersatzanspruch** gemäß Art 82 DSGVO zu begründen. Erforderlich sind das i) Vorliegen eines **materiellen oder immateriellen Schadens**, ein ii) **Verstoß gegen die DSGVO** sowie ein iii) **Kausalzusammenhang** zwischen dem Schaden und dem Verstoß. Der Anspruch auf Ersatz eines immateriellen Schadens darf nicht von einem bestimmten **Erheblichkeitsgrad** des Schadens abhängig gemacht werden. Weiters hat der Schadenersatzanspruch nach Art 82 DSGVO keine Straf- oder Abschreckungs-, sondern nur eine **Ausgleichsfunktion**.

Ein **immaterieller Schaden** liegt nicht vor. Die Reaktion des Rechtsanwalts beschränkte sich auf das Erkennen und die rechtliche Qualifikation als Verstoß gegen die DSGVO. Ein **eingetretener Schaden** kann aus den Feststellungen nicht abgeleitet werden.

OGH 03.07.2025, 6Ob53/25z

#### **Recht am eigenen Wort, Tonbandaufnahme, Beweismittel**

- Ein Vater wollte alle Telefonate mit seiner Ex-Frau aufzeichnen, um die Ausübung seines Kontaktrechts mit der gemeinsamen Tochter im Streitfall beweisen zu können. Die Ex-Frau brachte gegen diese Vorgehensweise eine Unterlassungsklage ein und beantragte eine einstweilige Verfügung beim Bezirksgericht. Sowohl das Bezirksgericht als auch die Berufungsinstanz wiesen das Begehren ab. Mit Revisionsrekurs wandte sich die Ex-Frau erfolglos an den OGH.

Der OGH hat erwogen: Abgeleitet aus § 16 ABGB besteht analog zum Recht am eigenen Bild auch ein **Recht am eigenen Wort**. Dieses umfasst die Privatheit der Person und ihrer nicht für die Öffentlichkeit bestimmten Äußerungen. **Tonbandaufnahmen** von Besprechungen und Telefongesprächen ohne Zustimmung sind grundsätzlich rechtswidrig. Die Prüfung der Verletzung des Rechts auf Achtung der Privatsphäre erfolgt jedoch durch eine einzelfallbezogene Interessenabwägung. Das Anfertigen von Bild- oder Tonbandaufnahmen zur Erlangung von **Beweismitteln** für ein behördliches Verfahren kann zulässig sein.

Das Recht, **Telefonaufnahmen** als Beweismittel anzufertigen, ist im konkreten Fall **höher** zu bewerten als das Recht der Ex-Frau, nicht aufgenommen zu werden. Dies insb deshalb, weil die Ex-Frau einen Großteil der Kommunikation über WhatsApp vornahm.

Ob ein **Unterlassungsanspruch** auch ohne Geltendmachung des Rechts auf Löschung etwa mangels Rechtfertigung der Datenverarbeitung ausgeübt werden kann, muss nicht geklärt werden. Denn der Revisionsrekurs hat zwar eine Interessenabwägung iSd berechtigten Interesses nach Art 6 Abs 1 lit f DSGVO angeführt, aber nicht dargelegt, inwieweit das Geheimhaltungsinteresse der Ex-Frau das Interesse an der Aufnahme des Telefonats zu Beweis Zwecken überwiegen würde.

#### Aus der weiteren Rechtsprechung der Justiz:

- In der DSGVO ist die **Doppelgleisigkeit des Rechtsschutzes** vorgesehen. Betroffene können daher sowohl verwaltungsbehördlichen als auch gerichtlichen Rechtsschutz in Anspruch nehmen. Aufgrund des Vorrangs des Unionsrechts geht die Doppelgleisigkeit des Rechtsschutzes dem aus Art 94 Abs 1 B-VG abgeleiteten **Verbot von Parallelzuständigkeiten** vor. Adressat des gerichtlichen Rechtsbehelfs nach Art 79 DSGVO ist ein Verantwortlicher oder ein Auftragsverarbeiter. Verantwortlicher kann auch eine **Behörde** sein. Als Behörde ist jede Stelle zu

verstehen, die öffentliche Verwaltungstätigkeiten im Außenverhältnis zum Bürger wahrnimmt. Ein mit behördlichen Aufgaben **beliehenes Unternehmen**, das hoheitliche Tätigkeiten ausübt und mit Bescheid entscheidet, ist eine Behörde. Dem Gesetzgeber steht es trotz der Doppelgleisigkeit des Rechtsschutzes frei, den Rechtsschutz gegen die Handlungen und Unterlassungen einer Behörde – ausgenommen Ansprüche nach dem Amtshaftungsgesetz (AHG) – dem BVwG zu überantworten, denn das BVwG ist ein Gericht iSd Unionsrechts. Es steht daher im Einklang mit dem Unionsrecht, wenn der Gesetzgeber – abseits vom AHG – den ordentlichen Rechtsweg gegen Behörden ausschließt. Ein auf Datenschutz gestützter **Unterlassungsanspruch** kann gegen eine Behörde auf dem ordentlichen Rechtsweg nicht geltend gemacht werden ([OGH 03.07.2025, 6Ob62/25y](#)).

### **Rechtsprechung des BVwG**

[BVwG 06.05.2025, W271 2303184-1](#); [07.05.2025, W282 2303188-1](#); [08.05.2025, W179 2303090-1](#)

### **Cold Calling, Geldstrafe, Rechtsauskunft**

- Betroffene erhielten wiederholt Werbeanrufe von einer Telefonnummer, die einem Unternehmen zugeordnet werden konnte, welches Matratzen und Bettdecken vertreibt. Die Anrufe erfolgten von einer Telefonnummer, die im Internet als Quelle von Spamanrufen bekannt ist. Das Unternehmen betrieb Direktmarketing, indem es zu Werbezwecken eine große Kundendatenbank anrief und Matratzen bzw Bettdecken anbot. Der Geschäftsführer des Unternehmens bestritt die Verantwortung für die Anrufe. Nachdem mehrere Anzeigen beim zuständigen **Fernmeldebüro** einlangten, wurden gegen den Geschäftsführer des Unternehmens mehrere Straferkenntnisse wegen **Cold Calling** (§ 174 Abs 1 iVm § 188 Abs 6 Z 9 TKG 2021) erlassen. Zudem wurde jeweils die Solidarhaftung des Unternehmens ausgesprochen. Dagegen erhoben das Unternehmen und dessen Geschäftsführer mehrere Bescheidbeschwerden an das BVwG. Das BVwG wies alle Bescheidbeschwerden ab und verpflichtete den Geschäftsführer zusätzlich, je **20%** der verhängten Strafe als **Verfahrenskostenbeitrag** zu leisten.

Das BVwG hat erwogen: Für die Einhaltung der Verwaltungsvorschriften durch eine juristische Person ist der nach außen vertretungsbefugte Geschäftsführer verantwortlich, sofern keine verantwortlichen Beauftragten bestellt sind. § 174 Abs 1 TKG 2021 verbietet **Anrufe zu Werbezwecken** ohne vorherige Einwilligung des Betroffenen (Cold Calling). Der **Begriff der Werbung** ist weit auszulegen und erfasst jede Äußerung, die den Absatz von Waren oder die Erbringung

von Dienstleistungen fördert. Bereits der erstmalige Kontakt zur **Einholung einer Einwilligung für spätere Werbeanrufe** ist Werbung. Das bloße Ansprechen bezüglich der Produkte des Unternehmens gegenüber dem Betroffenen ist daher als Werbung zu qualifizieren.

Damit ein Werbeanruf zulässig ist, bedarf er einer **Einwilligung**. Dabei wird die Begriffsbestimmung des Art 4 Z 11 DSGVO herangezogen, wonach die Betroffene freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich durch eine Erklärung oder eine sonstige eindeutige bestätigende Handlung zu erkennen geben muss, dass sie mit der Verarbeitung ihrer personenbezogenen Daten einverstanden ist. Die Einwilligung muss ausdrücklich oder konkludent, eindeutig und unzweifelhaft vorliegen.

Die bloße **Veröffentlichung einer Telefonnummer** im Internet oder in Telefonbüchern ist keine Einwilligung zum Erhalt von Werbeanrufen. Der Betroffene hat keine Einwilligung erteilt, sondern das Unternehmen vielmehr darum gebeten, die Werbeanrufe zu unterlassen. Das Verbot des § 174 Abs 1 TKG 2021 schützt alle Empfänger von Werbeanrufen unabhängig davon, ob sie Verbraucher oder **Unternehmer** sind.

Für eine Strafbarkeit nach § 174 Abs 1 TKG 2021 genügt bereits Fahrlässigkeit. Der Geschäftsführer hat dafür zu sorgen, dass die gesetzlichen Vorgaben eingehalten werden. Er muss ein **Kontrollsystem** einrichten, Weisungen erteilen und die Einhaltung laufend kontrollieren. Dem Geschäftsführer wäre es ohne Weiteres zumutbar gewesen, vor den Werbeanrufen beim Fernmeldebüro eine **Rechtsauskunft** über deren Zulässigkeit einzuholen. Die einschlägigen Vorstrafen des Geschäftsführers und das **Geschäftsmodell des Unternehmens** sprechen für zumindest **bedingten Vorsatz**. Die vom Fernmeldebüro verhängte Geldstrafe ist daher schuld- und tatangemessen.

### Aus der weiteren Rechtsprechung des BVwG:

- Die **Zurückziehung** der **Säumnisbeschwerde** führt zum Erlöschen des Erledigungsanspruchs. Wird die Säumnisbeschwerde zurückgezogen, bevor das BVwG entschieden hat, ist das Verfahren mit Beschluss einzustellen ([BVwG 20.05.2025, W256 2310929-1](#)).
- Wird von den Parteien auf die Revision beim VfGH und die Beschwerde beim VfGH verzichtet oder wird die Ausfolgung der Niederschrift nicht beantragt, kann das Erkenntnis des BVwG in **gekürzter Form** ausgefertigt werden. Das datenschutzrechtliche Verwaltungsstrafverfahren wird gemäß § 41 Abs 1 VStG eingestellt ([BVwG 09.05.2025, W605 2285459-1](#) bzw W605 22985459-1).

## Rechtsprechung des BFG

Aus der Rechtsprechung des BFG:

- Für die **Refundierung der Eingabengebühren nach § 2 BuLVwG-EGebV** ist entscheidend, ob dem Antragsteller in den zugrunde liegenden Verfahren vor dem BVwG (zB gegen Bescheide der DSB) oder vor dem LVwG **Verfahrenshilfe gewährt** wurde. Liegt keine Bewilligung der Verfahrenshilfe vor, entsteht die Gebührenschuld für die Eingaben gemäß § 1 Abs 2 BuLVwG-EGebV im Zeitpunkt der Einbringung der Bescheidbeschwerde und wird mit diesem Zeitpunkt fällig. Kommt der Antragsteller trotz Aufforderung nicht dem Ersuchen um Nachweis der Bewilligung der Verfahrenshilfe nach, kann nicht von einer Gebührenbefreiung oder Refundierung ausgegangen werden. Ohne **Bewilligung der Verfahrenshilfe** besteht kein **Anspruch auf Befreiung von Gerichtsgebühren** und anderen bundesgesetzlich geregelten staatlichen Gebühren ([BFG 27.06.2025, RV/3100085/2025](#)).

## EU-Rechtsakte

- Am **24.07.2025** ist von der **Europäischen Kommission** die "[Erläuterung und Vorlage für die öffentliche Zusammenfassung von Schulungsinhalten für KI-Modelle mit allgemeinem Verwendungszweck](#)" veröffentlicht worden. Gemäß Art 53 Abs 1 lit d KI-VO haben **Anbieter von KI-Modellen mit allgemeinem Verwendungszweck** eine detaillierte Zusammenfassung der für das Training des KI-Modells mit allgemeinem Verwendungszweck verwendeten Inhalte zu erstellen und zu veröffentlichen. Dabei haben sie sich an die vom **Büro für Künstliche Intelligenz** – das bei der Kommission angesiedelt ist – bereitgestellte **Vorlage** zu halten. Diese Vorlage hat die Kommission nunmehr samt Erläuterungen bereitgestellt. KI-Modelle mit allgemeinem Verwendungszweck werden in Anwendungen wie ChatGPT, Microsoft Copilot und Google Gemini verwendet. Die Bestimmung des Art 53 Abs 1 lit d KI-VO gilt ab dem **02.08.2025**.

## Nationale Rechtsakte

- Am **23.07.2025** wurde das **Datenzugangsgesetz**, [BGBl I 2025/33](#), kundgemacht. Mit diesem Gesetz wird die [Verordnung \(EU\) 2022/868](#), besser bekannt als **Data Governance Act (DGA)**, in innerstaatliches Recht durchgeführt. Das DGA regelt insb die Weiterverwendung bestimmter Daten, die im Besitz öffentlicher Stellen sind. Einer Umsetzung ins innerstaatliche Recht bedarf es nicht, weil es eine EU-Verordnung ist. Im Datenzugangsgesetz wird der **Bundeskanzler** als zuständige Behörde für die

Registrierung von **datenaltruistischen Organisationen** sowie als **zentrale Informationsstelle** festgelegt. Weiters enthält das Gesetz datenschutzrechtliche Rollenzuweisungen, Strafbestimmungen und eine Gebührenbefreiung. Das Haftungsmodell für die **Strafbarkeit juristischer Personen** ist dem Haftungsmodell des Verbandsverantwortlichkeitsgesetzes nachgebildet.

- Am **24.07.2025** wurde das **Informationsfreiheits-Anpassungsgesetz**, [BGBl I 2025/50](#), kundgemacht. Mit dieser Sammelnovelle werden 138 Bundesgesetze, darunter die Verwaltungsverfahrensgesetze, dem neuen **Grundrecht auf Information** und dem **Informationsfreiheitsgesetz (IFG)** angepasst. Das neue Grundrecht auf Information bzw auf Zugang zu Informationen wird ab **01.09.2025** verfassungsgesetzlich gewährleistet.
- Am **23.07.2025** wurde ein "*Bundesgesetz, mit dem das **Bankwesengesetz** geändert wird*", [BGBl I 2025/37](#), kundgemacht. Mit dieser Novelle wird die Regelung des **Bankgeheimnisses** dem **Grundrecht auf Information** und dem **IFG** angepasst.
- Am **24.07.2025** wurde ein "*Bundesgesetz, mit dem das **Informationsordnungsgesetz** und das **Parlamentsmitarbeiterinnen- und Parlamentsmitarbeitergesetz** geändert werden*", [BGBl I 2025/42](#), kundgemacht. Das InfOG regelt den Umgang mit klassifizierten und nicht-öffentlichen Informationen durch den Nationalrat und den Bundesrat. Das ParlMG regelt die Beschäftigung parlamentarischer Mitarbeiter. Beide Gesetze wurden in Hinblick auf das neue **Grundrecht auf Information** angepasst. Abgerundet wird diese Gesetzesanpassung mit einer Änderung der Geschäftsordnung des Nationalrats, die durch ein "*Bundesgesetz, mit dem das **Geschäftsordnungsgesetz 1975** geändert wird*", [BGBl I 2025/32](#), erfolgt ist.
- Am **24.07.2025** wurde ein "*Bundesgesetz, mit dem das **Strafgesetzbuch** geändert wird*", [BGBl I 2025/45](#), kundgemacht. Aufgrund dieser Novelle des StGB wird **Cyberflashing**, das unaufgeforderte Übermitteln von Genitalbildern, gerichtlich strafbar. Ausgestaltet ist das Verbot von Cyberflashing als **Ermächtigungsdelikt**. Dh der Täter darf nur mit Ermächtigung des Opfers verfolgt und bestraft werden.
- Am **18.07.2025** wurde die "*Verordnung der Rundfunk und Telekom Regulierungs-GmbH, mit der die Nummernübertragungsverordnung 2022 geändert wird*", [BGBl II 2025/164](#), kundgemacht. Die Änderung betrifft die **Fortführung** des Vertrags mit dem abgebenden Anbieter eines **Mobil-Sprachkommunikationsdienstes**.

- Am **25.07.2025** wurde die "Verordnung der Bundesregierung, mit der die Verordnung über die Informationssicherheit (Informationssicherheitsverordnung; **InfoSiV**) geändert wird", [BGBl II 2025/169](#), kundgemacht. Mit dieser Novelle wird die InfoSiV dem **Grundrecht auf Information** und dem **IFG** angepasst.
- Am **25.07.2025** wurde die "Verordnung der Finanzmarktaufsichtsbehörde (FMA) über Meldestichtage, Meldeintervalle, Gliederung und Inhalte von Meldungen gemäß der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte betreffend Emittenten vermögenswertereferenzierter Token und Emittenten von E-Geld-Token (**MiCAR-Emittenten-Meldeverordnung; MiCAR-E-MV**)", [BGBl II 2025/170](#), kundgemacht. In der **MiCAR-E-MV** werden ua Meldeinhalte von Meldungen durch Emittenten **vermögenswertereferenzierter Token** und Emittenten von **E-Geld-Token** festgelegt.
- Am **21.07.2025** wurde das **Salzburger Informationsfreiheits-Anpassungsgesetz**, [LGBl 2025/76](#), kundgemacht. Mit dieser Sammelnovelle werden die **Salzburger Landesverfassung** und knapp 40 Salzburger Landesgesetze an das neue **Grundrecht auf Information** angepasst.
- Am **28.07.2025** wurde das **Oö. Informationsfreiheits-Anpassungsgesetz (Oö. IFAG)**, [LGBl 2025/64](#), kundgemacht. Mit dieser Sammelnovelle werden die **oberösterreichische Landesverfassung** und rund 50 oberösterreichische Landesgesetze an das neue **Grundrecht auf Information** angepasst.
- Am **23.07.2025** wurde das "Landesgesetz, mit dem das Oö. **TDB-Begleitregelungsgesetz (Oö. TDB-BrG)** erlassen und das Oö. **Auskunftspflicht-, Datenschutz- und Informationsweiterverwendungsgesetz (Oö. ADIG)** geändert wird", [LGBl 2025/59](#), kundgemacht. Mit diesem Gesetz wird die Etablierung einer **gebietskörperschaftenübergreifenden Transparenzdatenbank** in Oberösterreich umgesetzt.
- Am **23.07.2025** wurde ein "Landesgesetz, mit dem das Oö. **Archivgesetz** geändert wird (**Oö. Archivgesetz-Novelle 2025**)", [LGBl 2025/60](#), kundgemacht. Mit dieser Novelle wird die Archivierung der Dokumentation staatlichen Handelns in Oberösterreich **digitalisiert**. Dementsprechend enthält die Novelle auch datenschutzrechtliche Bestimmungen.

to the point

# Datenschutzmonitor. 31/2025 vom 06.08.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH SA 01.08.2025, C-422/24, *Storstockholms* (Bodycams, Informationspflicht)

EuGH SA 01.08.2025, C-371/24, *Comdribus* (Biometrie, Erforderlichkeit, erkennungsdienstliche Behandlung)

- **Rechtsprechung des VwGH**

VwGH 24.06.2025, Ra 2025/04/0148 (Videoüberwachung, berechtigtes Interesse)

- **Rechtsprechung des BVwG**

BVwG 03.06.2025, W211 2292541-1 (Initiativantrag, Beschwerdegegner, konkludente Einwilligung, gesetzliche Grundlage)

BVwG 09.04.2025, W108 2284624-2 (Exzess, Missbrauchsabsicht)

BVwG 28.05.2025, W137 2259971-1 (Auskunft, Data Breach, Personenbezug)

BVwG 10.06.2025, W274 2307868-1 (Auskunftserteilung im laufenden Verfahren, Feststellungskompetenz)

- **EU-Rechtsakte**

EK Pressemitteilung 28.07.2025, IP/25/1913 (Temu, DSA)

Praxisleitfaden für KI mit allgemeinem Verwendungszweck (Stellungnahme der EK)

DurchführungsVOs zur eIDAS-VO (europäische Brieftasche)

Entwürfe für DurchführungsVOs zur Cybersicherheit

## To the Point:

### Rechtsprechung des EuGH

EuGH SA 01.08.2025, C-422/24, *Storstockholms*

#### **Bodycams, Informationspflicht**

- Ein öffentlicher Verkehrsbetrieb in Stockholm setzt bei Fahrscheinkontrollen Bodycams ein, um Gewaltsituationen zu dokumentieren und die Identität von Schwarzfahrern festzustellen. Die schwedische Datenschutzbehörde verhängte ua wegen unzureichender Informationen über diese Datenerhebung an betroffene Fahrgäste gemäß Art 13 DSGVO eine Geldbuße iHv SEK 4 Mio (ca EUR 360.000). Der Verkehrsbetrieb erhob dagegen erfolglos Beschwerde an das Verwaltungsgericht Stockholm. Erst das Berufungsgericht gab dem Rechtsmittel statt und hob die Geldbuße mit der Begründung auf, dass beim Einsatz von Bodycams Art 14 DSGVO einschlägig sei. Denn Art 13 DSGVO verlange eine bewusste Handlung der Betroffenen, was im Fall von Videoaufzeichnungen nicht zutreffe. Die schwedische Datenschutzbehörde wandte sich daraufhin an das schwedische Höchstgericht. Dieses legte dem EuGH die Frage vor, ob bei der Datenerhebung durch Bodycams Art 13 (Datenerhebung *bei* der Betroffenen) oder Art 14 DSGVO (Datenerhebung *nicht* bei der Betroffenen) einschlägig ist.

Die Generalanwältin hat erwogen: Art 13 DSGVO ist dann anwendbar, wenn die personenbezogenen Daten unmittelbar von der Betroffenen selbst stammen. Art 14 greift hingegen, sobald die Daten aus irgendeiner anderen Quelle, etwa einem Dritten, einer öffentlich zugänglichen Quelle oder einer anderen Betroffenen, bezogen wurden. **Entscheidend** ist somit nicht die aktive Mitwirkung der Betroffenen an der Erhebung, sondern **allein der Ursprung der Daten**. Steht kein **"Vermittler"** zwischen der Betroffenen und dem Verantwortlichen, findet Art 13 DSGVO Anwendung, auch wenn die Betroffene die Datenerhebung weder initiiert noch bemerkt hat.

Dies entspricht den Leitlinien für Transparenz gemäß der Verordnung 2016/679 der Artikel-29-Gruppe (WP 260), wonach Art 13 DSGVO sowohl bei einer **bewussten Bereitstellung der Daten** als auch bei einer **durch reine Beobachtung erfolgten Erhebung**, etwa mittels Kameras oder anderer automatisierter Aufzeichnungsgeräte, gilt. Die Informationspflicht nach Art 13 DSGVO führt erst dazu, dass die Betroffene von der Verarbeitung **Kenntnis** erlangt. Diese Kenntnis ist also **Folge, nicht Voraussetzung der Anwendbarkeit** des Art 13 DSGVO. Bei

Bodycams wird eine Person allein durch ihre physische Anwesenheit zur Datenquelle. Die dadurch erfolgende unmittelbare Datenerhebung unterfällt daher Art 13 DSGVO.

EuGH SA 01.08.2025, C-371/24, *Comdribus*

#### **Biometrie, Erforderlichkeit, erkennungsdienstliche Behandlung**

- Ein Demonstrant wurde wegen der Teilnahme an einer nicht angemeldeten Demonstration festgehalten. Zwar gab er seine Personalien an, jedoch verweigerte er die Abnahme seiner Fingerabdrücke und das Anfertigen von Fotos. Gegen den Demonstranten wurde ein Strafverfahren wegen des Verdachts auf Straftaten im Zusammenhang mit der Demonstration und wegen der Weigerung, sich erkennungsdienstlichen Maßnahmen zu unterziehen, eingeleitet. Vom ersten Vorwurf wurde er freigesprochen, für die **Verweigerung der erkennungsdienstlichen Behandlung wurde er jedoch verurteilt**. Gegen dieses Urteil legten sowohl der Demonstrant als auch die Staatsanwaltschaft Rechtsmittel ein. Das vorlegende Gericht fragte den EuGH (i) ob die Richtlinie 2016/680 (DSRL-PJ) eine Erhebung biometrischer Daten bereits bei einem plausiblen Verdacht auf eine Straftat oder deren Versuch erlaubt; (ii) ob die zuständige Behörde im Einzelfall begründen muss, warum die Erhebung biometrischer Daten unbedingt erforderlich ist, und (iii) ob eine Bestrafung allein wegen der Weigerung zur Abgabe biometrischer Daten zulässig ist, auch wenn es zu keiner Verurteilung wegen der zugrunde liegenden Straftat kommt.

Der Generalanwalt hat erwogen: Zweck des Art 10 DSRL-PJ ist es, einen erhöhten Schutz für die Verarbeitung besonderer Kategorien personenbezogener Daten zu bieten. Darunter fallen **biometrische Daten** wie **Fingerabdrücke**. Eine Verarbeitung dieser Daten ist nur erlaubt, wenn dies **"unbedingt erforderlich"** ist. Die Anforderung der Erforderlichkeit ist erfüllt, wenn das Ziel der Datenverarbeitung nicht ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte der Betroffenen eingreifen. Bei der Bewertung der "unbedingten Erforderlichkeit" sind auch Faktoren wie Art und Schwere der Straftat, besondere Umstände der Straftat, Zusammenhang der Straftat mit anderen laufenden Verfahren, Vorstrafen und individuelles Profil der Betroffenen zu berücksichtigen. Bei der Schwere der Tat sind auch die Besonderheiten der Aufgaben der Polizeibehörden zu berücksichtigen. Das Kriterium der "unbedingten Erforderlichkeit" ist nicht schon



deshalb ausgeschlossen, weil eine Straftat nicht als "schwer" eingestuft wird.

**Nationale Rechtsvorschriften**, die die Erhebung biometrischer Daten bei jeder Person ermöglichen, gegen die plausible Gründe für den Verdacht des Versuchs oder der Begehung einer Straftat vorliegen, sind zulässig, sofern sie die zuständigen Behörden zur Prüfung der unbedingten Erforderlichkeit verpflichten.

Die Behörde hat ihre Entscheidung **angemessen zu begründen**, sodass ein Betroffener die Gründe nachvollziehen und wirksame Rechtsbehelfe ergreifen kann.

Eine **Strafe wegen der Verweigerung einer erkennungsdienstlichen Behandlung** ist auch dann **zulässig**, wenn die Straftat, die dieser Maßnahme zugrunde lag, nicht verfolgt oder verurteilt wird, sofern vor der Durchführung der Maßnahme die "unbedingte Erforderlichkeit" im Einzelfall geprüft und dokumentiert wurde.

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Gemäß Art 6 Abs 1 lit f DSGVO ist die Verarbeitung personenbezogener Daten zulässig, wenn ein **berechtigtes Interesse** besteht, die Verarbeitung zur Verwirklichung dieses Interesses erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der Betroffenen nicht überwiegen. Es muss einzelfallbezogen geprüft werden, ob eine Verarbeitung als gerechtfertigt angesehen werden kann. Die **Videoüberwachung** eines öffentlich zugänglichen Weges in **unmittelbarer Nähe einer privaten Liegenschaft** ist grundsätzlich berechtigt, wenn diese zum persönlichen Schutz sowie zum Schutz des Eigentums erfolgt. Die Datenverarbeitung muss jedoch erforderlich sein und auf das absolut Notwendige beschränkt werden. Wenn mildere Mittel – wie etwa das Anbringen einer **Alarmanlage**, eine **Verstärkung des Torschlosses** oder eine Kameraattrappe – zur Erreichung des Schutzzwecks möglich sind, sind vorrangig diese heranzuziehen. Im Falle einer Videoüberwachung muss auch diese weniger eingriffsintensiv gestaltet werden, indem der öffentlich zugängliche Weg nicht erfasst wird ([VwGH 24.06.2025, Ra 2025/04/0148](#)).

### Rechtsprechung des BVwG

BVwG 03.06.2025, W211 2292541-1

**Initiativantrag, Beschwerdegegner, konkludente Einwilligung, gesetzliche Grundlage**

- Nach der Behandlung eines Initiativantrags im Gemeinderat erhielt eine Unterstützerin eines Initiativantrags einen Verständigungsbrief des Bürgermeisters, in dem sie über das Ergebnis der Beschlussfassung informiert wurde, obwohl sie nicht die Zustellungsbevollmächtigte war. Die Unterstützerin erhob daraufhin Datenschutzbeschwerde gegen den Magistrat der Stadt bei der DSB. Diese stellte fest, dass der Bürgermeister die für die Datenverarbeitung verantwortliche Stelle war und die Unterstützerin im Recht auf Geheimhaltung verletzt hat, indem er ihre Adressdaten zur Übermittlung eines Schreibens verarbeitet hat. Der Bürgermeister erhob (erfolglose) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Eine amtswegige Berichtigung der Bezeichnung des Verantwortlichen als Beschwerdegegner hat je nach Ermittlungsergebnis dann zu erfolgen, wenn der vom Betroffenen gewählte Beschwerdegegner falsch ist. Der Verständigungsbrief enthält keine Hinweise auf den Magistrat, sondern weist ausschließlich den Namen, die Unterschrift und die Kontaktdaten des Bürgermeisters auf. Es ist offensichtlich, dass die Unterstützerin den Bürgermeister als Beschwerdegegner iSd § 24 Abs 2 Z 2 DSG bezeichnen wollte.

Die bloße Teilnahme als Unterstützerin an einer Bürgerinitiative kann nicht als **konkludente Einwilligung** für nicht absehbare Datenverarbeitungen durch den Bürgermeister gewertet werden.

Der Bürgermeister handelte als staatliche **Behörde** iSd § 1 Abs 2 DSG. Gemäß § 8 Abs 4 NÖ Stadtrechtsorganisationsgesetz (NÖ STROG) ist der Bürgermeister nur zur Verständigung der Zustellungsbevollmächtigten verpflichtet. Daraus ergibt sich keine Ermächtigung für den Bürgermeister, eine (schriftliche) Verständigung und eine entsprechende Verarbeitung der Daten zum Informationszweck über den Ausgang des Initiativantrags vorzunehmen. Die Datenverarbeitung war daher weder aufgrund einer den Bürgermeister treffenden rechtlichen (gesetzlichen) Verpflichtung bzw. Ermächtigung, noch einer von ihm wahrzunehmenden Aufgabe im öffentlichen Interesse gerechtfertigt.

Der Erlaubnistatbestand des Art 6 Abs 1 lit f DSGVO (berechtigte Interessen) ist auf die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Datenverarbeitungen nicht anwendbar. Die Datenverarbeitung war somit unzulässig.

Aus der weiteren Rechtsprechung des BVwG:

- Bei offenkundig unbegründeten oder **exzessiven Datenschutzbeschwerden** darf die DSB eine Gebühr verlangen oder sich weigern, tätig zu werden (Art 57 Abs 4

DSGVO). Die Aufsichtsbehörde trägt die **Beweislast** für den offenkundig unbegründeten oder exzessiven Charakter der Datenschutzbeschwerde. Der EuGH legt Art 57 Abs 4 DSGVO dahingehend aus, dass Anfragen nicht allein aufgrund ihrer Zahl als exzessiv eingestuft werden können. Die DSB muss unter Berücksichtigung der einzelfallbezogenen Umstände das Vorliegen einer Missbrauchsabsicht der anfragenden Person nachweisen. Eine **Missbrauchsabsicht** liegt vor, wenn Datenschutzbeschwerden eingereicht werden, ohne dass dies objektiv erforderlich ist, um die Rechte aus der DSGVO zu schützen. Da der Betroffene lediglich **Mutmaßungen ohne konkrete Verletzungen** angestellt hat, durfte die DSB die Behandlung der Datenschutzbeschwerden wegen exzessiver Ausübung des Beschwerderechts iSd Art 57 Abs 4 DSGVO ablehnen ([BVwG 09.04.2025, W108 2284624-2](#)).

- Das **Auskunftsrecht** ist auf **eigene Daten** beschränkt. Es kann nicht dazu genutzt werden, eine **umfassende Benachrichtigung** über einen Vorfall (zB **Data Breach**) zu erhalten. Der Begriff "**personenbezogene Daten**" ist weit zu verstehen. Informationen betreffend einen Data Breach, wie die Geschäftszahl des Ermittlungsverfahrens der Staatsanwaltschaft, Auskünfte hinsichtlich der Ermittlungsergebnisse sowie entsprechende Presseaussendungen sind jedoch keine personenbezogenen Daten, weil ihnen die **Identifizierbarkeitskomponente** – ähnlich wie in der Situation eines offenen WLANs – fehlt ([BVwG 28.05.2025, W137 2259971-1](#)).
- Das **Auskunftsrecht** ist ein Recht auf eine Leistung. Die **Feststellung** einer Verletzung in Rechten auf eine bestimmte Leistung kommt nicht mehr in Frage, wenn dem Leistungersuchen bereits entsprochen worden ist. Da das BVwG nach der Sach- und Rechtslage zum Zeitpunkt seiner Entscheidung erkennt, ist der Auskunftsanspruch auch dann als erfüllt anzusehen, wenn die Auskunft erst im **Verfahren vor dem BVwG** erteilt wird ([BVwG 10.06.2025, W274 2307868-1](#)).

## EU-Rechtsakte

- Am **28.07.2025** veröffentlichte die **Europäische Kommission (EK)** die **vorläufige Feststellung**, dass das chinesische Unternehmen **Temu** betreffend die ordnungsgemäße Bewertung der Risiken der Verbreitung **rechtswidriger Produkte** auf seinem Marktplatz gegen das Gesetz über digitale Dienste (**DSA**) verstößt. Die Untersuchung wird fortgesetzt und bezieht sich auch auf von Temu ergriffene **Risikominderungsmaßnahmen**, die **Verwendung suchterzeugender**

**Gestaltungsmerkmale**, die Transparenz seiner **Empfehlungssysteme** und seinen **Datenzugang für Forschende** ([EK Pressemitteilung 28.07.2025, IP/25/1913](#)). **Anm: Nähere Informationen zum DSA finden Sie in unserem Praxishandbuch DSA.**

- Am **01.08.2025** bestätigte die Europäische Kommission, dass der **Praxisleitfaden für KI mit allgemeinem Verwendungszweck** ein geeignetes freiwilliges Instrument für Anbieter von KI mit allgemeinem Verwendungszweck ist, um die Einhaltung der KI-VO 2024/1689 nachzuweisen, [Commission Opinion, C\(2025\) 5361 final](#). Der Praxisleitfaden wurde auf Unionsebene unter Einbeziehung eines großen Kreises an Stakeholdern ausgearbeitet und besteht aus den Kapiteln **Sicherheit und Gefahrenabwehr, Transparenz und Urheberrecht**. **Anm: Wir haben im Datenschutzmonitor 28/2025 vom 16.07.2025 berichtet. Der Begriff "Praxisleitfaden" wurde bei der finalen Überarbeitung in die deutsche Fassung der KI-VO aufgenommen. Auf der verlinkten Website wird hingegen noch der zuvor verwendete Begriff "Verhaltenskodex" verwendet. Nähere Informationen zu den Praxisleitfäden finden Sie hier: [Leissler/Böszörményi in Zankl, KI-VO \(2024\) Art 56 KI-VO \(Paywall\)](#).**
- Am **02.08.2025** sind die **Governance-Vorschriften der KI-VO** in Kraft getreten. **Nähere Informationen zur KI-VO finden Sie im oben zitierten Kommentar zur KI-VO sowie in unserem Handbuch Künstliche Intelligenz in der Praxis.**
- Am **30.07.2025** wurden die (i) "**Durchführungsverordnung (EU) 2025/1566 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards für die Überprüfung der Identität und der Attribute der Person, der das qualifizierte Zertifikat oder die qualifizierte elektronische Attributsbescheinigung ausgestellt werden soll**", [ABI L 2025/1566](#); (ii) "**Durchführungsverordnung (EU) 2025/1567 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Verwaltung von qualifizierten elektronischen Fernsignaturerstellungseinheiten und qualifizierten elektronischen Fernsiegelerstellungseinheiten**", [ABI L 2025/1567](#); (iii) "**Durchführungsverordnung (EU) 2025/1568 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Verfahrensmodalitäten für**

**gegenseitige Begutachtungen elektronischer Identifizierungssysteme** und für die Zusammenarbeit bei der Organisation solcher Begutachtungen innerhalb der **Kooperationsgruppe** und zur Aufhebung des Durchführungsbeschlusses (EU) 2015/296 der Kommission", [ABI L 2025/1568](#); (iv) "Durchführungsverordnung (EU) 2025/1569 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf **qualifizierte elektronische Attributsbescheinigungen** und von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen bereitgestellte elektronische Attributsbescheinigungen", [ABI L 2025/1569](#); (v) "Durchführungsverordnung (EU) 2025/1570 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die **Notifizierung von Informationen über zertifizierte qualifizierte elektronische Signaturerstellungseinheiten** und zertifizierte qualifizierte elektronische **Siegelerstellungseinheiten**", [ABI L 2025/1570](#); (vi) "Durchführungsverordnung (EU) 2025/1571 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die **Formate und Verfahren** für die jährlichen Berichte der **Aufsichtsstellen**", [ABI L 2025/1571](#); (vii) "Durchführungsverordnung (EU) 2025/1572 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf das **Format und die Verfahren** für die **Absichtsmitteilung** und die Überprüfung im Hinblick auf den Beginn der Erbringung qualifizierter Vertrauensdienste", [ABI L 2025/1572](#), kundgemacht. Mit diesen **sieben DurchführungsVOs** werden Anforderungen, Standards und Verfahren betreffend die **europäischen Brieffaschen** iSd [eIDAS](#) festgelegt.

- Am **01.08.2025** ist der Entwurf einer **DurchführungsVO** veröffentlicht worden, mit dem ein Mechanismus für die gegenseitige Begutachtung (**Peer-Review**) der nationalen Behörden für die **Cybersicherheitszertifizierung** gemäß dem [Rechtsakt zur Cybersicherheit \(VO \(EU\) 2019/881\)](#) eingeführt werden soll, [Ares\(2025\)6278765](#).
- Am **01.08.2025** ist der Entwurf einer **DurchführungsVO**, [Ares\(2025\)6278517](#), veröffentlicht worden, in dem der Liste der **Sachstandsdokumente** neue

Sachstandsdokumente für Cybersicherheitszertifizierungen hinzugefügt oder aktualisiert werden sollen. Sachstandsdokumente sind Dokumente, in welchen Evaluierungsmethoden, -techniken und -instrumente für die **Cyberzertifizierung** festgelegt werden (auf Englisch: **state-of-the-art documents**).

to the point

# Datenschutzmonitor. 32/2025 vom 13.08.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des VwGH**

VwGH 04.07.2025, Ra 2023/04/0220 (COVID, Gesundheitsdaten, Verwaltungsstrafverfahren)

- **Rechtsprechung des OGH**

OGH 30.07.2025, 23Ds4/24a (Rechtsanwalt, direkte Kontaktaufnahme)

OGH 23.07.2025, 3Ob58/25p (Smart Meter, Aussetzung)

- **Rechtsprechung des BVwG**

BVwG 28.05.2025, W108 2230691-1 (Automatisierte Entscheidungsfindung, Bonitätsscore, Auskunftsrecht, Geschäftsgeheimnis)

BVwG 20.06.2025, W256 2246580-1 (ÄrzteG, Informationspflicht, Datenübertragbarkeit)

BVwG 12.06.2025, W211 2291308-1 (Rollenverteilung, Informationspflicht, Schadenersatz)

BVwG 16.06.2025, W211 2310626-1 (Exekutionsverfahren, justizielle Tätigkeit)

BVwG 16.06.2025, W101 2259199-2 (Aussetzungsbescheid, Rechtsschutzinteresse)

- **Rechtsprechung der DSB**

DSB 24.03.2025, 2025-0.165.785 (Akteneinsicht, Parteistellung, Zulässigkeitsprüfung)

- **Nationale Rechtsakte**

Wiener Informationsfreiheitsanpassungsgesetz 2025

Steiermärkische Förderungstransparenzgesetz (Transparenzportal)

## To the Point:

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Die Erhebung und Übermittlung eines ärztlichen Attests ist eine **Verarbeitung besonderer Kategorien** personenbezogener Daten. Gemäß § 9 Abs 1 COVID-19-Maßnahmegesetz waren Organe des **öffentlichen Sicherheitsdienstes** befugt, Unterlagen zur Einhaltung von Betretungsverboten, Voraussetzungen und Auflagen einzusehen und **Beweismittel** zu sichern. Die Vorlage und mögliche Weiterleitung des Attests zur Befreiung der **Maskenpflicht** an die **Verwaltungsstrafbehörde** und an die **Ärztammer** war für den Betroffenen **vorhersehbar** und für die Einleitung eines Verwaltungsstrafverfahrens **erforderlich**. Die Weiterleitung an die **Ärztammer** diene zur Überprüfung der Echtheit der ärztlichen Bestätigung. Da das BVwG die Beweiswürdigung ausführlich und sorgfältig vorgenommen hat und der Revision keine über den Einzelfall hinausgehende Bedeutung zukommt, war diese zurückzuweisen ([VwGH 04.07.2025, Ra 2023/04/0220](#)).

### Rechtsprechung des OGH

Aus der Rechtsprechung des OGH:

- Dem an den **Rechtsanwalt** gerichteten Verbot der **direkten Kontaktaufnahme** mit der anwaltlich vertretenen Gegenseite nach **§ 19 RL-BA 2015** wird durch das in Art 15 DSGVO verankerte **Auskunftsrecht** des Betroffenen nicht derogiert ([OGH 30.07.2025, 23Ds4/24a](#)).
- Das Revisionsverfahren wird bis zur Entscheidung des EuGH in der [Rs C-468/24, Netz Niederösterreich](#), **unterbrochen**. In dieser Rs sind beim EuGH Vorlagefragen zu datenschutzrechtlichen Bedenken hinsichtlich des Austauschs einer Strommesseinrichtung gegen einen **Smart Meter** anhängig. Diese Fragen sind in diesem Revisionsverfahren präjudiziell, weshalb es zweckmäßig und geboten ist, bis zur Entscheidung des EuGH zuzuwarten ([OGH 23.07.2025, 3Ob58/25p](#)).

### Rechtsprechung des BVwG

BVwG 28.05.2025, W108 2230691-1

**Automatisierte Entscheidungsfindung, Bonitätsscore, Auskunftsrecht, Geschäftsgeheimnis**

- Nach einem Auskunftsersuchen gemäß Art 15 DSGVO stritt ein Betroffener mit einer Wirtschaftsauskunftei über die Vollständigkeit der erteilten Auskunft. Die Auskunft hatte drei Seiten mit überwiegend

allgemeinen Ausführungen zur Datenverarbeitung übersandt, behauptete jedoch, keine automatisierte Entscheidungsfindung iSd Art 22 DSGVO iZm der Bonitätsbewertung des Betroffenen durchzuführen. Da der Betroffene darin eine Verletzung seiner Rechte sah, legte er Datenschutzbeschwerde bei der DSB ein. Nach Ablauf der Entscheidungsfrist erhob er Säumnisbeschwerde an das BVwG. Im weiteren Verfahrensgang forderte das BVwG die Auskunftstei ausdrücklich auf, sämtliche vorhandene Informationen und Unterlagen zur automatisierten Verarbeitung der personenbezogenen Daten des Betroffenen vorzulegen sowie etwaige als Geschäftsgeheimnis eingestufte Informationen entsprechend zu kennzeichnen und das Geheimhaltungsinteresse konkret darzulegen. Trotz dieser gerichtlichen Aufforderung legte die Auskunftstei keine weiteren konkreten Unterlagen oder detaillierten Informationen vor. Das BVwG hat in der Sache entschieden und gab der Datenschutz- bzw Säumnisbeschwerde teilweise statt.

Das BVwG hat erwogen: Nach der Rechtsprechung des EuGH ist Art 22 Abs 1 DSGVO dahin auszulegen, dass eine **"automatisierte Entscheidung im Einzelfall"** vorliegt, wenn ein auf personenbezogene Daten gestützter **Wahrscheinlichkeitswert maßgeblich** bestimmt, ob ein Dritter ein Vertragsverhältnis mit der Betroffenen begründet, durchführt oder beendet. Dies traf für die von der Auskunftstei berechneten **Bonitätsscores** zu.

Der Anspruch auf Auskunft nach Art 15 Abs 1 lit h DSGVO verlangt, Betroffene so zu informieren, dass sie die Funktionsweise des **Scorings**, die zugrunde liegenden Daten, die **Gewichtung der Parameter** und die **möglichen Auswirkungen auf ihre Rechtsstellung** nachvollziehen können. Weder die bloße Übermittlung einer komplexen mathematischen Formel noch die detaillierte Beschreibung jedes Schritts genügt, wenn sie keine **präzise und verständliche Erläuterung** ist.

Die von der Auskunftstei übermittelten allgemeinen Hinweise ("statistische Werte" sowie pauschale Aufzählungen von Datenquellen und Kategorien) genügen diesen Transparenzanforderungen nicht. Insbesondere fehlen (i) eine Aufschlüsselung der **konkret herangezogenen personenbezogenen Daten** des Betroffenen als **Parameter/Eingangsvariablen**, (ii) deren tatsächlicher **Einfluss auf das Ergebnis (Gewichtung)**, (iii) Informationen zur **Funktionsweise des Algorithmus** sowie (iv) eine **verständliche Erläuterung**, weshalb der **konkrete Score** (Ratingwert 2,02; Ampelscore 2) zustande kam. Ebenso wurde keine **individualisierte Auskunft** zur Tragweite und den angestrebten

Auswirkungen des errechneten Scores erteilt. Der pauschale Verweis auf **Geschäftsgeheimnisse** rechtfertigt keine Verweigerung detaillierter Erläuterungen, solange der Verantwortliche diese nicht substantiiert darlegt und zumindest gegenüber Gericht bzw Aufsichtsbehörde offengelegt. Da die Auskunft weder die **involvierte Logik** hinreichend erläuterte noch die Tragweite und angestrebten Auswirkungen individualisiert beschrieb, hat sie das Auskunftsrecht des Betroffenen verletzt.

BVwG 20.06.2025, W256 2246580-1

### **ÄrzteG, Informationspflicht, Datenübertragbarkeit**

- Ein Vater verlangte von einem Kinderarzt die Übermittlung sämtlicher medizinischer Daten sowie Auskunft, an wen diese weitergegeben wurden für sich, seine Lebensgefährtin, seinen minderjährigen Sohn und seine minderjährige Tochter. Der Vater vermutete, dass durch eine verpflichtende Gefährdungsmeldung Daten ua an die Bezirkshauptmannschaft versendet wurden. Der Arzt übermittelte sämtliche medizinische Daten zum Sohn und erteilte Auskunft über die verarbeiteten Stammdaten der Familie, verneinte aber eine weitere Datenverarbeitung oder -weitergabe. Der Vater hielt die erteilte Auskunft für unvollständig.

Die DSB wies die Datenschutzbeschwerde wegen Verletzung im Recht auf Information, Auskunft, Datenübertragbarkeit und Geheimhaltung hinsichtlich des Vaters und der Lebensgefährtin ab und hinsichtlich des Sohnes und der Tochter zurück. Zur Tochter führte die DSB begründend aus, dass dem Vater die Vertretungsbefugnis fehle, weil er nicht mit deren Obsorge betraut war. Dagegen erhob der Vater (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Der Arzt verarbeitete zu der Familie keine weiteren medizinischen Daten/Unterlagen. Auch wurden solche Daten aufgrund einer an ihn gerichteten Gefährdungsmeldung nicht (schriftlich) weitergegeben. Eine Mangelhaftigkeit der Auskunft ist daher nicht ersichtlich.

Die Regelung des **§ 3b Abs 2 ÄrzteG** nimmt Datenverarbeitungen, welche im Zuge der ärztlichen Berufsausübung durchzuführen sind, von der **Informationspflicht** des Art 13 und 14 DSGVO aus. Eine Verletzung im Recht auf Information lag daher schon aus diesem Grund nicht vor.

Die Familie hat keinen **Antrag auf Datenübertragbarkeit** nach Art 20 DSGVO an den Arzt gerichtet, weshalb keine Verletzung im Recht auf Datenübertragbarkeit vorliegen konnte.

Eine (schriftliche) Korrespondenz zwischen dem Arzt und der Bezirkshauptmannschaft

fand iZm einer verpflichtenden Gefährdungsmeldung nicht statt. Die behauptete Verletzung im **Recht auf Geheimhaltung** ist daher nicht gegeben.

Die erfolgte Zurückweisung der Datenschutzbeschwerde hinsichtlich des Sohnes war nur ein **Vergreifen im Ausdruck**.

BVwG 12.06.2025, W211 2291308-1

### **Rollenverteilung, Informationspflicht, Schadenersatz**

- Eine gemeinnützige Organisation unterstützte arbeitsuchende Personen dabei, eine neue Perspektive am Arbeitsmarkt zu finden, und setzte hierfür arbeitsmarktpolitische Projekte von öffentlichen Auftraggebern um. Dafür schloss sie einen Förderungsvertrag sowie eine damit verbundene **Vereinbarung zur Auftragsverarbeitung** gemäß Art 28 DSGVO mit dem Auftraggeber ab. Ein Teilnehmer einer solchen arbeitsmarktpolitischen Maßnahme unterzeichnete eine Information gemäß Art 13 DSGVO. Anschließend warf er der gemeinnützigen Organisation vor, ihn nicht ordnungsgemäß auf sein Widerspruchsrecht nach Art 21 DSGVO und sein Widerrufsrecht nach Art 7 Abs 3 DSGVO hingewiesen zu haben. Er behauptete, listig getäuscht worden zu sein, um seine Unterschrift zu erlangen.

Die DSB wies die Datenschutzbeschwerde ab. Sie stellte fest, dass die gemeinnützige Organisation als Auftragsverarbeiter gemäß Art 4 Z 8 DSGVO zu qualifizieren sei, weil sie die Verarbeitung im Auftrag eines Verantwortlichen durchgeführt habe. Zudem fehle dem Teilnehmer im Hinblick auf Art 13 und Art 14 DSGVO die Beschwer. Daraufhin erhob der Teilnehmer (erfolglos) Bescheidbeschwerde an das BVwG und beantragte (ebenso erfolglos) Schadenersatz nach Art 82 DSGVO.

Das BVwG hat erwogen: Gemäß Art 4 Z 7 DSGVO ist "**Verantwortlicher**" die Person oder Stelle, die über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Trifft ein Akteur **tatsächlich** und **faktisch** die **Entscheidung** für die Aufnahme einer Datenverarbeitung, ist dieser als Verantwortlicher iSd DSGVO anzusehen. Die Rolle von **Auftragsverarbeitern** ergibt sich aus den **konkreten Tätigkeiten** in einem bestimmten Kontext. Die Art des Dienstes bestimmt, ob die Verarbeitungstätigkeit auf eine Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen hinausläuft.

Die **Pflicht zur Information** gemäß Art 13 und 14 DSGVO trifft den Verantwortlichen.

Die **gemeinnützige Organisation** ist hinsichtlich des Zwecks und der Mittel der Verarbeitung der personenbezogenen Daten an

die **Weisungen**, die sich ua aus dem Fördervertrag und aus dem Auftragsverarbeitungsvertrag ergeben, **gebunden**. Diese Regelungen lassen der gemeinnützigen Organisation keinen Raum, einen **hinreichenden Einfluss** auf die durchgeführten Datenverarbeitungen auszuüben. Folglich ist bzw war die gemeinnützige Organisation nicht Verantwortliche hinsichtlich der gerügten Datenverarbeitung.

Für den geltend gemachten **Schadenersatzanspruch** ist das BVwG **sachlich unzuständig**.

BVwG 16.06.2025, W211 2310626-1

### **Exekutionsverfahren, justizielle Tätigkeit**

- Im Rahmen eines Exekutionsverfahrens prüfte ein **Exekutionsrichter** die Einkommenssituation eines Schuldners mit einer Datenabfrage beim Dachverband der Sozialversicherungsträger. Der Schuldner brachte Datenschutzbeschwerde bei der DSB ein. Die DSB wies die Datenschutzbeschwerde zurück, weil die Abfrage im Rahmen der justiziellen Tätigkeit des Gerichts erfolgt sei. Der Begriff justizielle Tätigkeit sei weit auszulegen und umfasse auch Datenverarbeitungen im Rahmen von Exekutionsverfahren. Der Schuldner erhob (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die DSB ist gemäß Art 55 Abs 3 DSGVO **nicht** für die Aufsicht über die von den Gerichten im Rahmen ihrer **justiziellen Tätigkeit** vorgenommenen Verarbeitungen zuständig.

Der Begriff "justizielle Tätigkeit" ist in der DSGVO nicht näher definiert und ist autonom iSd Unionsrechts auszulegen. Eine justizielle Tätigkeit liegt vor, wenn ein Richter in Ausübung seines richterlichen Amtes tätig wird oder sonst in Besorgung der übertragenen Amtsgeschäfte weisungsfrei gestellt ist. Zu prüfen ist, ob durch die Kontrolle der DSB die **Unabhängigkeit** der Gerichte mittel- oder unmittelbar **beeinflusst** werden kann. Es kommt nicht darauf an, ob es sich verfahrensrechtlich um ein Streitiges oder außerstreitiges Verfahren handelt.

**Exekutionsverfahren** sind justizielle Tätigkeiten. Eine von einem Exekutionsrichter durchgeführte Datenabfrage in Ausübung des richterlichen Amtes, gestützt auf die Exekutionsordnung, ist davon umfasst. Der Schuldner kann gegen die Datenverarbeitung eine Beschwerde nach § 85 GOG an das im Instanzenzug übergeordnete Zivilgericht richten.

Aus der weiteren Rechtsprechung des BVwG:

- Ein **Aussetzungsbescheid** der DSB verliert seine Rechtswirksamkeit mit dem Eintritt des Zeitpunkts, bis zu welchem die

Aussetzung verfügt wurde. Nach diesem Zeitpunkt ist wegen nachträglichen Wegfalls des **Rechtsschutzinteresses** (der **Beschwerer**) das Beschwerdeverfahren **einzustellen** ([BVwG 16.06.2025, W101 2259199-2](#)).

### **Rechtsprechung der DSB**

DSB 24.03.2025, 2025-0.165.785

#### **Akteneinsicht, Parteistellung, Zulässigkeitsprüfung**

- In einem vorangegangenen Verfahren erhob ein Auskunftswerber Datenschutzbeschwerde gegen einen Rechtsanwalt und weitete anschließend die Datenschutzbeschwerde auf die nunmehrige Antragstellerin aus. Die DSB erkannte dies als neue, getrennt zu beurteilende Sache und leitete ein neues Beschwerdeverfahren ein, das später nur gegenüber dem Auskunftswerber mit Bescheid zurückgewiesen wurde. Die Antragstellerin erfuhr von diesem Verfahren nur indirekt. Weder wurde ihr der Zurückweisungsbescheid zugestellt, noch wurde sie anderweitig in das Verfahren einbezogen. Mehrere Anträge ihres Rechtsanwalts auf Akteneinsicht und Zustellung des Bescheids lehnte die DSB mit der Begründung ab, dass die Antragstellerin keine Verfahrenspartei sei. Daraufhin beantragte die Antragstellerin selbst die Zustellung des Zurückweisungsbescheids. Die DSB wies diesen Antrag ab.

Die DSB hat erwogen: Das Recht auf **Akteneinsicht** nach § 17 AVG setzt ein Verwaltungsverfahren voraus, in dem der Akteneinsichtswerber **Parteistellung** hat. Die Antragstellerin war zwar im Verwaltungsverfahren **Beteiligte**, weil sich die Tätigkeit der DSB auf die Antragstellerin bezogen hat, indem die DSB ihre grundsätzliche Zuständigkeit bejaht hat und die entsprechenden Vorwürfe zur Kenntnis genommen und aktenkundig gemacht hat.

**Partei** ist aber nur, wer einen **Rechtsanspruch** oder ein **rechtliches Interesse** hat. Maßgebend ist, dass die **Sachentscheidung** in die Rechtssphäre des Betroffenen **bestimmend eingreift** und eine **unmittelbare**, nicht bloß abgeleitete und mittelbare **Wirkung** entfaltet. Im Zweifel ist ein subjektives Recht dann zu vermuten, wenn nicht ausschließlich öffentliche Interessen, sondern zumindest auch das Interesse einer von der Allgemeinheit abgrenzbaren Person für die gesetzliche Festlegung der verpflichtenden Norm maßgebend war. Diese Voraussetzung ist erfüllt, wenn ein die bestehenden **subjektiven Rechte belastender Rechtsgestaltungs- oder Feststellungsbescheid** erlassen werden soll.

Die DSB prüft in der **Eingangsprüfung** die formelle und materielle Zulässigkeit der

Datenschutzbeschwerde. In diesem Verfahrens stadium besteht kein subjektives Recht auf Abweisung einer inhaltlich unberechtigten Datenschutzbeschwerde. Ein solches entsteht erst, wenn die Datenschutzbeschwerde nach erfolgter **Zulässigkeitsprüfung** der Beschwerdegegnerin zugestellt und ihr die Beschwerdevorwürfe vorgehalten werden. Die Parteistellung kann sich im Verlauf eines mehrstufigen Verwaltungsverfahrens ändern, wenn sich der Verfahrensgegenstand und die Rechtsschutzinteressen ändern.

Die § 24 Abs 1 und 2 DSG iVm § 13 Abs 3 AVG begründen lediglich eine **objektive Rechtspflicht der DSB**, eine den Form- und Inhaltskriterien nicht entsprechende Datenschutzbeschwerde von Amts wegen inhaltlich nicht zu behandeln. Ein subjektives Recht ist dabei lediglich insoweit berührt, als dem Beschwerdeführer das Recht zukommt, keiner willkürlichen oder sonst unbegründeten Nicht-Zulassung einer Datenschutzbeschwerde unterworfen zu werden.

**Mangels Parteistellung** der Antragstellerin kommt ihr kein Recht auf Zustellung des Zurückweisungsbescheids oder ein Recht auf Akteneinsicht gemäß § 17 Abs 1 AVG zu. Insbesondere fehlt es ihr an einem Rechtsschutzinteresse, weil sie durch die Zurückweisung der Datenschutzbeschwerde nicht beschwert oder in einem subjektiven Recht verletzt sein kann. **Beachte: Am 01.09.2025 tritt das neue Grundrecht auf Information bzw Informationszugang in Kraft. Das Informationsfreiheitsgesetz wird zum Recht auf Akteneinsicht subsidiär gelten, könnte künftig jedoch Zugriff auf Fremddaten ermöglichen, sofern diesem Zugriff keine Geheimhaltungspflicht gemäß § 6 IFG entgegensteht.**

### **Nationale Rechtsakte**

- Am **04.08.2025** wurde das **Steiermärkische Förderungstransparenzgesetz (StFTG 2025)**, [LGBI 2025/55](#), kundgemacht. Mit diesem Gesetz werden die Verpflichtungen des Landes Steiermark zur Etablierung einer gebietskörperschaften-übergreifenden Transparenzdatenbank (**Transparenzportal**) umgesetzt.
- Am **06.08.2025** wurde das **Wiener Informationsfreiheitsanpassungsgesetz 2025**, [LGBI 2025/39](#), kundgemacht. Mit dieser Sammelnovelle werden knapp 30 Wiener Landesgesetze an das neue **Grundrecht auf Information** angepasst.



to the point

# Datenschutzmonitor. 33/2025 vom 20.08.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung der Justiz**

OGH 05.08.2025, 12Os71/25w (Datenverarbeitung in Schädigungsabsicht, § 63 DSGVO, tatbestandliche Handlungseinheit)

OLG Wien 11.02.2025, 4R5/25x (Auskunft, Rechtsanwalt, Vollmacht)

OLG Linz 16.01.2025, 4R157/24x (Auskunft, datenschutzfremdes Ziel, Rechte von Dritten)

OLG Wien 26.02.2025, 11R202/24t (Hoheitsverwaltung, Datenverarbeitung, Unterlassung)

- **Rechtsprechung des BVwG**

BVwG 20.06.2025, W252 2290822-1 (Auskunft, Akteneinsicht, nationale Sicherheit, Exzess)

BVwG 23.06.2025, W211 2297059-1 (Insolvenzverfahren, strafrechtliche Verurteilung, Rechtsanspruch)

BVwG 26.05.2025, W101 2267859-1; 26.05.2025, W101 2280857-1 (Data Breach, COVID, Nachweis)

BVwG 28.05.2025, W137 2255428-1 (Suchmaschine, De-Indexierung, Person des öffentlichen Lebens)

BVwG 24.06.2025, W176 2291296-1 (Amtswissen, Datenherkunft, Dokumentation, Befangenheit)

BVwG 04.06.2025, W298 2301992-1 (Rückwirkung, öffentliches Interesse, Löschung)

BVwG 30.05.2025, W256 2246885-1 (Gesundheitsdatum, Rechtsanspruch, Erforderlichkeit)

BVwG 26.06.2025, W298 2291079-1 (Rollenverteilung, Rechtsnorm)

BVwG 23.06.2025, W211 2291530-1 (Rechenschaftspflicht, Auskunft, Protokollierung, Feststellung)

BVwG 25.06.2025, W254 2307864-1 (Auskunft, Feststellung, Sanierung)

BVwG 17.06.2025, W252 2280887-1; 17.06.2025, W252 2280766-1 (Missbrauchsabsicht, Unrichtigkeit des Rechtsstandpunkts, Obsorge)

BVwG 20.06.2025, W274 2224656-1 (Missbrauchsabsicht)

BVwG 24.06.2025, W292 2256548-1 ("Sache" des Verfahrens)

BVwG 02.06.2025, W176 2286423-1 (Präklusion, Verfahrensautonomie, Minderjährige)

BVwG 20.05.2025, W292 2273428-1 (COVID, Beschwerdegegner, Aussetzung)

BVwG 20.06.2025, W254 2310916-1 (Kohärenzverfahren, Fristhemmung)

BVwG 17.06.2025, W171 2309847-1 (Säumnisbeschwerde, kondemnatorische Entscheidung)

- **Rechtsprechung der LVwG**

LVwG NÖ 14.07.2025, LVwG-AV-508/001-2024 (KFZ, Zulassungsevidenz, Garagierergewerbe)

- **Rechtsprechung der DSB**

DSB 24.02.2025, 2025-0.045.624 (Medienprivileg, Bürgerjournalismus, berufliche Kontaktdaten)

DSB 19.05.2025, 2025-0.327.266 (Videoüberwachung, Behörde, Privatwirtschaftsverwaltung, berechtigtes Interesse)

## To the Point:

### Rechtsprechung der Justiz

Aus der Rechtsprechung der Justiz:

- Der Angeklagte fertigte während eines Videotelefonats ohne Zustimmung der Geschädigten Screenshots an, die deren Genitalien und Schamgegend zeigten. Anschließend veröffentlichte der Angeklagte diese Screenshots zweimal auf Facebook und schickte sie dreimal dem Bruder der Geschädigten. Damit verwirklichte der Angeklagte den Straftatbestand der **Datenverarbeitung in Schädigungsabsicht** nach **§ 63 DSG** in Form einer **tatbestandlichen Handlungseinheit** ([OGH 05.08.2025, 120s71/25w](#)). **Anm: Die tatbestandliche Handlungseinheit wurde früher als fortgesetztes Delikt bezeichnet. Im Verwaltungsstrafrecht werden (nunmehr) beide Begriffe synonym verwendet.**
- Beauftragt eine Betroffene einen **Rechtsanwalt** mit der Durchsetzung ihres Betroffenenrechts auf Auskunft, muss der Verantwortliche die **Vollmacht** und **Identität** der Betroffenen prüfen. Weitere Informationen zur Bestätigung der Identität dürfen nicht generell, sondern nur bei begründeten Zweifeln an der Identität verlangt werden. Eine **Ausweiskopie** ist ein geeigneter Identitätsnachweis. Der **Bevollmächtigungsvertrag** ist an keine speziellen Formerfordernisse geknüpft. Teilt der Verantwortliche lediglich mit, keine elektronischen Vollmachten zu akzeptieren, ohne Zweifel an der Echtheit der Unterschrift zu äußern, ist für den Betroffenen nicht ersichtlich, ob berechtigterweise weitere Nachweise zur Erfüllung des Auskunftersuchens verlangt werden. Da der Verantwortliche die allenfalls bestehenden Zweifel iSd Art 12 Abs 6 DSGVO nicht einzelfallbezogen dargelegt hat, wurde die Klageerhebung durch den Verantwortlichen veranlasst ([OLG Wien 11.02.2025, 4R5/25x](#)).
- Die Auskunftspflicht besteht auch dann, wenn der Auskunftswerber mit seinem **Auskunftersuchen** ein **datenschutzfremdes Ziel** verfolgt. Das festgestellte Motiv des Klägers, nach der Auskunftserteilung die Möglichkeit zu haben, den bei den **Online-Glücksspielen** erlittenen Verlust (infolge nichtiger Rechtsgeschäfte) gerichtlich geltend zu machen, ist nicht unlauter. Richtig ist, dass das Auskunftsrecht die Rechte und Freiheiten anderer Personen – wozu auch der **Verantwortliche zählt** – nicht beeinträchtigen soll. Dies darf jedoch nicht dazu führen, dass jegliche Auskunft verweigert wird ([OLG Linz 16.01.2025, 4R157/24x](#)).
- Die der Erfüllung **behördlicher Aufgaben** dienende **Datenverarbeitung** iSd DSGVO

(elektronischer Art) oder des DSG (auch analoger Natur) ist der **Hoheitsverwaltung** zuzuordnen. Die **Unterlassungsklage** zielt damit unzulässigerweise auf eine **Untersagung** (wenn auch rechtswidrigen) **hoheitlichen Handelns** ab. Rechtswidriges und schuldhaftes hoheitliches Handeln kann gemäß § 1 Abs 1 AHG einen **Amtshaftungsanspruch** begründen. Andere Ansprüche als Schadenersatz auf Zahlung oder Feststellung der Ersatzpflicht können nicht auf das AHG gestützt werden. Insb sind Wiederherstellungs- oder (vorbeugende) **Unterlassungsbegehren nicht möglich** ([OLG Wien 26.02.2025, 11R202/24t](#)).

### Rechtsprechung des BVwG

[BVwG 20.06.2025, W252 2290822-1](#)

#### **Auskunft, Akteneinsicht, nationale Sicherheit, Exzess**

- Ein ehemaliger Bediensteter des Bundesheeres beehrte von seiner Dienstbehörde Auskunft über die Verarbeitung seiner personenbezogenen Daten im Personalinformationssystem (**PERSIS**) und im sog "**kleinen Personalakt**", insb iZm Disziplinarverfahren und Mitarbeitergesprächen. Die Behörde erteilte teilweise Auskunft, verweigerte aber die Beauskunftung bestimmter Daten mit Verweis auf Akteneinsichtsrechte in Disziplinarverfahren und argumentierte, die DSGVO sei nicht anwendbar, weil die Datenverarbeitung der militärischen Landesverteidigung und damit der nationalen Sicherheit diene. Zudem wurde das Auskunftersuchen als exzessiv bezeichnet. Der ehemalige Bedienstete erhob Datenschutzbeschwerde. Die DSB gab dieser teilweise Folge und trug der Dienstbehörde auf, vollständige Auskunft zu erteilen. Dagegen erhob die Dienstbehörde (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Tätigkeiten, welche die **nationale Sicherheit** betreffen, worunter auch der **Verteidigungsbereich** fällt, sind vom **sachlichen Anwendungsbereich** der DSGVO ausgenommen. Diese Ausnahme ist jedoch eng auszulegen und betrifft nur Datenverarbeitungen, die unmittelbar der Wahrung der nationalen Sicherheit dienen. Die bloße Tatsache, dass das Bundesheer Aufgaben im Bereich der Landesverteidigung wahrnimmt, führt nicht dazu, dass sämtliche Personalverwaltungsdaten von der DSGVO ausgenommen sind.

Die Verarbeitung personenbezogener Daten im **Personalakt** und iZm **Disziplinarverfahren** fällt in den Anwendungsbereich der DSGVO. Die DSB kann auch Verantwortlichen des **öffentlichen Bereichs** Leistungsaufträge erteilen. Die Einschränkung des § 24 Abs 5 DSG auf Verantwortliche des privaten Bereichs hat aufgrund des

**Anwendungsvorrangs** des Art 58 Abs 2 lit c DSGVO, der eine solche Einschränkung nicht vorsieht, unangewendet zu bleiben.

Ein Verweis auf bestehende **Akteneinsichtsrechte** in Disziplinarverfahren entbindet die Behörde nicht von der Pflicht, ein Auskunftersuchen nach der DSGVO zu beantworten. Der Gegenstand einer Akteneinsicht kann je nach Lage des Einzelfalls mit dem Gegenstand einer Auskunft nach Art 15 DSGVO inhaltsgleich sein, doch ist das keinesfalls zwingend. Das datenschutzrechtliche Auskunftsrecht ist **eigenständig** und nicht subsidiär gegenüber dem Akteneinsichtsrecht.

Eine Vielzahl von Anträgen oder Datenschutzbeschwerden allein reicht nicht aus, um ein Auskunftersuchen als **exzessiv** iSd Art 57 Abs 4 DSGVO einzustufen. Vielmehr ist eine **Missbrauchsabsicht** der betroffenen Person nachzuweisen.

BVwG 23.06.2025, W211 2297059-1

### **Insolvenzverfahren, strafrechtliche Verurteilung, Rechtsanspruch**

- In einem **Insolvenzverfahren** legte ein Gläubiger dem Insolvenzgericht **strafrechtliche Verurteilungen** der Schuldnerin vor. Seiner Ansicht nach war die Angabe der Vermögensverhältnisse der Schuldnerin unzutreffend. Dies wollte er mit den vorgelegten Urteilen beweisen. Weiters wollte er die Annahme eines Zahlungsplans verhindern, um weiterhin Regress gegen die Schuldnerin führen zu können. Die Schuldnerin sah in der Veröffentlichung eine Verletzung ihres Rechts auf Geheimhaltung und brachte Datenschutzbeschwerde bei der DSB ein. Die DSB stellte eine Verletzung des Rechts auf Geheimhaltung fest. Der Gläubiger erhob (erfolgreich) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die Verarbeitung **strafrechtsbezogener Daten** gemäß Art 10 DSGVO darf nur unter **behördlicher Aufsicht** erfolgen oder wenn dies nach einer geeigneten **Rechtsvorschrift** vorgesehen ist. Die Verarbeitung von strafrechtlich relevanten Daten durch **Privatpersonen** ist in § 4 Abs 3 DSG geregelt. Eine Verarbeitung ist zulässig, wenn dies zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten gemäß Art 6 Abs 1 lit f DSGVO erforderlich ist.

Eine **Interessenabwägung** ist durchzuführen. Dabei muss die Verarbeitung *ex ante* als erforderlich beurteilt werden. An die **Erforderlichkeit** werden keine zu hohen Ansprüche gestellt. Eine **plausible Begründung** der Beweiserheblichkeit reicht. Das berechtigte Interesse, nicht-sensible Daten für die Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen** zu verarbeiten, kann aus einem

**Größenschluss** aus Art 9 Abs 2 lit f DSGVO abgeleitet werden.

Der Erhalt von **Regressmöglichkeiten** gegenüber einer Schuldnerin kann ein berechtigtes Interesse im Insolvenzverfahren sein. Falls der **Zahlungsplan** angenommen wird, kann nach Erfüllung kein Regress mehr aus Forderungen geführt werden. Diese Möglichkeit besteht nur bei einem Abschöpfungsverfahren.

Ein Insolvenzgericht hat bei der Bestätigung des Zahlungsplans aber nur die Kriterien nach der Insolvenzordnung (IO) zu beurteilen. Die Annahme eines Zahlungsplans liegt in der Entscheidung der Gläubiger. Das Gericht hat nicht auf das Interesse einzelner Gläubiger Rücksicht zu nehmen. Die Übermittlung der Urteile an das Insolvenzgericht war daher **überschießend** und nicht erforderlich.

BVwG 26.05.2025, W101 2267859-1; 26.05.2025, W101 2280857-1

### **Data Breach, COVID, Nachweis**

- Betroffene erfuhren durch Medienberichterstattung von einer angeblichen unrechtmäßigen Verarbeitung und Offenlegung ihrer **COVID-19-Testergebnisse** durch ein Corona-Testzentrum. Durch den Versand einer **Excel-Liste** per E-Mail wurden ihrer Auffassung nach Daten zu den Testergebnissen unrechtmäßig offengelegt. Daraufhin brachten sie Datenschutzbeschwerde bei der DSB ein. Die DSB gab den Datenschutzbeschwerden statt und stellte eine unrechtmäßige Datenverarbeitung fest. Nach Auffassung der DSB wurde die Excel-Liste unberechtigt offengelegt und ohne Rechtfertigungsgrund ungesichert in einem E-Mail-Postfach aufbewahrt. Dies allein könne den Zugang von unberechtigten Dritten zu Gesundheitsdaten begünstigen und bedeutet eine Verletzung im Recht auf Geheimhaltung. Dagegen erhob das Testzentrum (erfolgreich) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Jede betroffene Person hat einen Anspruch auf Geheimhaltung ihrer personenbezogenen Daten. Der Anknüpfungspunkt des Grundrechtsanspruchs ist das Vorliegen eines schutzwürdigen Interesses.

Im Verfahren konnte die ursprüngliche E-Mail, mit der die Excel-Liste angeblich versandt wurde, **nicht wiederhergestellt** werden. Eine unrechtmäßige Offenlegung konnte auch durch **Logfiles** nicht bestätigt werden. Wie die Excel-Liste an die Medien gelangte, blieb unklar. Kann **keine** unrechtmäßige Offenlegung oder Verarbeitung von Daten im Verfahren festgestellt werden, ist eine Sicherheitsverletzung iSd Art 32 Abs 1 DSGVO bzw die Verletzung der Grundsätze der Datensicherheit und der

Datenminimierung nicht erwiesen. In Ermangelung einer unrechtmäßigen Datenverarbeitung kann keine Verletzung des Rechts auf Geheimhaltung festgestellt werden.

Der bloße Umstand einer an die Medien gelangten Excel-Liste ist **kein ausreichender Nachweis** für eine unrechtmäßige Offenlegung aus dem Verantwortungsbereich des Testzentrums.

BVwG 28.05.2025, W137 2255428-1

### **Suchmaschine, De-Indexierung, Person des öffentlichen Lebens**

- Eine Unternehmerin stand aufgrund ihrer Heirat mit einem bekannten Industriellen sowie durch ihre Tätigkeit als Geschäftsführerin in der Öffentlichkeit. Sie brachte ein Löschersuchen bei einem Suchmaschinenbetreiber ein, in dessen **Suchmaschine** bei Eingabe ihres Namens mehrere URLs zu einer Website aufschienen, auf denen ein anonym Verfassers in drei Beiträgen personenbezogene Informationen über sie veröffentlichte. Die Beiträge enthielten ua persönliche Angriffe und einen Schenkungsvertrag zwischen der Unternehmerin und ihrer Großmutter. Der Suchmaschinenbetreiber kam dem Ersuchen nicht nach. Die DSB stellte eine Verletzung des Rechts auf Löschung fest und verpflichtete das Unternehmen zur Löschung der konkreten URLs. Sie hielt fest, dass der Ausnahmetatbestand des Art 17 Abs 3 lit a DSGVO nicht vorliege und die Beiträge diffamierende und unrichtige Aussagen enthielten, die auf die Schädigung der Unternehmerin abzielten. Dagegen erhob der Suchmaschinenbetreiber (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: **Werturteile** geben die **subjektive Meinung** des Erklärenden wieder und können personenbezogene Daten anderer Personen enthalten. Sie sind einem **Berichtigungsanspruch per se nicht zugänglich**. Während Tatsachen einem Beweis zugänglich sind, ob sie richtig oder falsch sind, ist dies bei Werturteilen nicht der Fall.

Zwei der veröffentlichten Artikel sind **Werturteile** eines unbekanntes Dritten, weil die dort geäußerten Ausführungen keiner objektiven Überprüfung zugänglich sind. Die **Sachinformationen** sind für sich genommen nicht "falsch", sondern sie werden vom Autor klar abwertend bzw negativ interpretiert.

Der dritte Artikel enthält hingegen nur die **objektive Kernaussage**, dass "die im Vertrag genannte Schenkung schon am nächsten Tag in voller Höhe zurückerstattet worden sei". Diese Aussage ist einer Überprüfung auf ihre Richtigkeit grundsätzlich zugänglich, weil kein Einschätzungsspielraum besteht. **Werturteile**, die konkludente

Tatsachenbehauptungen sind, dürfen **nicht schrankenlos geäußert** werden.

Im Hinblick auf **Personen des öffentlichen Lebens** ist nicht jeder Aspekt des Privatlebens in gleichem Ausmaß von Interesse für die Öffentlichkeit. An einer subjektiven Meinung über eine Person des öffentlichen Lebens, welche nicht auf einem ausreichenden Tatsachensubstrat gründet, besteht kein ausreichendes Interesse der Öffentlichkeit. Daher überwiegt das Geheimhaltungsinteresse der Unternehmerin.

Es liegt ein **Wertungsexzess** vor, welcher die **Grenzen zulässiger Kritik überschreitet**. Die Beiträge orientieren sich nicht hinreichend bzw nachvollziehbar an konkreten Fakten. Der Gegenstand der Berichterstattung zielt ausschließlich auf die Diffamierung der Unternehmerin ab.

Aus der weiteren Rechtsprechung des BVwG:

- Das **"Amtswissen"** als abstrakt vorhandenes Wissen kann nicht Gegenstand einer zu erteilenden Auskunft iSd Art 15 DSGVO sein, weil keine Verarbeitung personenbezogener Daten iSd Art 4 Z 2 DSGVO erfolgt. Hinsichtlich der Auskunftspflicht über die **Datenherkunft** spricht Art 15 Abs 1 lit g DSGVO ausdrücklich von **"verfügbaren" Informationen**. Eine Pflicht zur **Dokumentation** von Datenquellen besteht nicht. Ein subjektives Recht auf **Verfahrensverbinding** nach § 39 Abs 2 AVG gibt es nicht. Adressat der Bestimmung des § 7 AVG betreffend **Befangenheit** kann niemals ein **Organ** als bloße Summe von Zuständigkeiten sein, sondern nur ein Mensch, also der **Organwahrter**. Ein Befangenheitsgrund gemäß § 7 AVG kann sich nicht auf eine Behörde beziehen (BVwG 24.06.2025, W176 2291296-1).
- Die mit **rückwirkender Kraft** ausgestattete Gestaltungswirkung eines **aufhebenden Erkenntnisses** bedeutet auch, dass allen Rechtsakten und faktischen (Vollzugs-)Akten, die während der Geltung des später aufgehobenen Erkenntnisses auf dessen Grundlage gesetzt wurden, im Nachhinein die Rechtsgrundlage entzogen wird. Ein behördlicher Eingriff in das Grundrecht auf Datenschutz gemäß § 1 DSG wegen überwiegender berechtigter **öffentlicher Interessen** ist nur dann erlaubt, wenn er durch gesetzliche Grundlagen hinreichend determiniert ist. Datenverarbeitungen auf gesetzlicher Grundlage sind vom bedingenen Grundverfahren abhängig bzw teilen deren rechtliches Schicksal. Es ist weder für einen Betroffenen noch für einen verständigen Dritten absehbar, dass zwar die Speicherung der rechtsstaatlich zu Unrecht durchgeführten Verfahren gelöscht werden muss, nicht jedoch ein darauf beruhender

- Antrag ([BVwG 04.06.2025, W298 2301992-1](#)).
- Die Information über eine **Krankenhausbehandlung** ist als Angabe über die Inanspruchnahme/Nichtinanspruchnahme einer Gesundheitsdienstleistung zu qualifizieren und ist somit auch bei einer Negativauskunft ein **Gesundheitsdatum**. In einem **arbeitsgerichtlichen Entlassungsverfahren** darf dieses Gesundheitsdatum jedoch zur Überprüfung eines "vorgetäuschten" **Krankenstands** beim Krankenhaus abgefragt werden. Der Erlaubnistatbestand des Art 9 Abs 2 lit f DSGVO (Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen**) normiert für sensible Daten einen Sonderfall des allgemeinen Erlaubnistatbestands des berechtigten Interesses nach Art 6 Abs 1 lit f DSGVO. Da für die Geltendmachung oder Verteidigung von Rechtsansprüchen **keine Abwägung mit Betroffeneninteressen** vorgesehen ist, ist auf die **Erforderlichkeit** ein besonderes Augenmerk zu legen. Diese ist jedenfalls gegeben, wenn die Datenanfrage auf die **Wiederlegung eines Prozessvorbringens** gerichtet ist ([BVwG 30.05.2025, W256 2246885-1](#)).
  - Die **Rolle als Verantwortlicher** ist nach einer **funktionalen Sichtweise** festzulegen. Die Verantwortlichkeit wird anhand des tatsächlichen Einflusses zugewiesen. Sieht eine **Rechtsnorm** implizite rechtliche Verpflichtungen vor, ist als Verantwortlicher jene Person oder Stelle anzusehen, die diese rechtliche Verpflichtung trifft. **Rechtsanwälte, Hausverwaltungen und Sachverständige** sind regelmäßig selbst Verantwortliche ([BVwG 26.06.2025, W298 2291079-1](#)). **Anm: Ob Hausverwaltungen nur im Verhältnis zu Eigentümern oder auch zu Mietern gemeint sind, geht aus der Entscheidung nicht hervor. Verfahrensgegenstand war nicht die Rolle von Hausverwaltungen.**
  - Die **Rechenschaftspflicht** ist auf den ersten Blick sehr weitgehend, sie unterliegt jedoch **Verhältnismäßigkeitsabwägungen** entsprechend dem risikobasierten Ansatz. Eine **unbeschränkte Nachweispflicht** betreffend die Einhaltung jeder einzelnen datenschutzrechtlichen Pflicht würde mit grundlegenden **rechtsstaatlichen Prinzipien** in Konflikt geraten. Eine generelle **Protokollierung** jedes einzelnen Verarbeitungsvorgangs ist nicht gefordert und würde die Grundsätze der **Datenminimierung** und **Speicherbegrenzung** konterkarieren. Die Rechenschaftspflicht ist nur gegenüber der **zuständigen Aufsichtsbehörde** zu erfüllen. Die **Feststellung** einer in der Vergangenheit liegenden Auskunftspflichtverletzung kommt nicht in Betracht ([BVwG 23.06.2025, W211 2291530-1](#)).
  - Eine **Rechtsverletzung durch Nichterteilen der Auskunft** kann bis zum Ende des Verfahrens vor dem BVwG nachträglich beseitigt werden (**Sanierung**). Dem Auskunftswerber ist während des Verfahrens vor dem BVwG die Auskunft erteilt worden. Die **Feststellung** einer **in der Vergangenheit** liegenden Auskunftspflichtverletzung kommt nicht in Betracht. Das Beschwerdeverfahren ist mit Beschluss einzustellen ([BVwG 25.06.2025, W254 2307864-1](#)).
  - Eine **Missbrauchsabsicht** kann dadurch gekennzeichnet sein, dass dem Betroffenen die **Unrichtigkeit seines Rechtsstandpunkts** bewusst ist. Auf eine Missbrauchsabsicht deuten weiters **ausschweifende Vorbringen** und **übermäßige Wiederholungen** hin. Ist der primäre Zweck der Datenschutzbeschwerde, den Kontakt zum minderjährigen Sohn herzustellen, obwohl der Vater kein Sorgerecht hat und ein aufrechtes Kontaktverbot besteht, ist die Missbrauchsabsicht offensichtlich. Die **Obsorge- und Kontaktrechtsproblematik** ist ein sachfremdes Motiv, das unter dem Deckmantel des Datenschutzrechts nicht verfolgt werden darf ([BVwG 17.06.2025, W252 2280887-1](#); [17.06.2025, W252 2280766-1](#)).
  - Der Datenschutzbeschwerde liegen keine spezifischen Gründe zugrunde, die **eigenen datenschutzrechtlichen Interessen** des Betroffenen zu wahren. Eine Berechtigung, datenschutzrechtliche Betroffenenrechte seines **minderjährigen Sohnes** wahrzunehmen, kommt dem Vater nicht zu. Der Vater hat eine hohe Anzahl an Datenschutzbeschwerden bei der DSB und dem BVwG anhängig gemacht, die somit von einer **Missbrauchsabsicht** getragen werden ([BVwG 20.06.2025, W274 2224656-1](#)).
  - Den äußersten Rahmen für die Prüfbefugnis des BVwG bildet die **"Sache"** des Verfahrens. Die "Sache" des Verfahrens ist nur jene Angelegenheit, die den **Inhalt des Spruchs** bildet. Die Abgrenzung des Verfahrensgegenstands hat in **Relation zum angefochtenen Bescheid** und nicht anhand der Datenschutzbeschwerde zu erfolgen ([BVwG 24.06.2025, W292 2256548-1](#)).
  - Die DSGVO enthält keine Vorgaben betreffend die Fristen zur Geltendmachung eines Anspruchs nach Art 77 DSGVO. Gemäß dem **Grundsatz der Verfahrensautonomie** der Mitgliedstaaten ist es Sache der einzelnen Mitgliedstaaten, die Modalitäten für das **Verwaltungsverfahren** und das Gerichtsverfahren zu regeln. Die Ausübung der Befugnisse der DSB richtet sich nach dem mitgliedstaatlichen Recht. Die subjektive Präklusivfrist läuft binnen **eines Jahres** ab Kenntnis des beschwerenden Ereignisses ab. Die Kenntnis der Eltern kann **minderjährigen Geschädigten**, nicht aber

volljährigen Geschädigten, zugerechnet werden ([BVwG 02.06.2025, W176 2286423-1](#)).

- Zur Zumutbarkeit der **Bezeichnung des Beschwerdegegners** iZm **Impfernungsschreiben** sind zahlreiche Verfahren beim BVwG anhängig. Gleichzeitig ist diese Rechtsfrage auch Gegenstand eines Verfahrens vor dem VwGH. Das Beschwerdeverfahren wird daher gemäß § 34 Abs 3 VwGVG bis zur Entscheidung des VwGH **ausgesetzt** ([BVwG 20.05.2025, W292 2273428-1](#)).
- Bei grenzüberschreitenden Verarbeitungen ist ein sog **Kohärenzverfahren** durchzuführen. Dabei wird eine **federführende Aufsichtsbehörde** bestimmt, die für die Verfahrensführung zuständig ist. Während des Kohärenzverfahrens ist die sechsmonatige **Entscheidungsfrist** der DSB **gehemmt**. Die Durchführung des Kohärenzverfahrens liegt nicht im Ermessen der DSB. Daher wird das Kohärenzverfahren bei Vorliegen der gesetzlichen Voraussetzungen **ex lege** beim Einbringen der Datenschutzbeschwerde in Gang gesetzt ([BVwG 20.06.2025, W254 2310916-1](#)).
- Ist eine **Säumnisbeschwerde** berechtigt, kann das BVwG eine sog **kondemnatorische Entscheidung** treffen. Mit dieser Entscheidung wird die DSB unter Zugrundelegung der geäußerten Rechtsansicht des BVwG zum Erlassen des Bescheids binnen acht Wochen "verurteilt" ([BVwG 17.06.2025, W171 2309847-1](#)).

### Rechtsprechung der LVwG

Aus der Rechtsprechung der LVwG:

- Die Kraftfahrbehörde darf gemäß § 47 Abs 2a KFG den Namen und die Anschrift des Zulassungsbesitzers aus der **Zulassungsevidenz** bei Glaubhaftmachung eines **rechtlichen Interesses** an eine Privatperson herausgeben. Auskunft aus der Zulassungsevidenz kann auch **juristischen Personen** und sonstigen Unternehmen erteilt werden. Das rechtliche Interesse der Inhaberin eines **Garagierungsgewerbes** an der Geltendmachung einer **Vertragsstrafe** ist ausreichend ([LVwG NÖ 14.07.2025, LVwG-AV-508/001-2024](#)).

### Rechtsprechung der DSB

[DSB 24.02.2025, 2025-0.045.624](#)

#### **Medienprivileg, Bürgerjournalismus, berufliche Kontaktdaten**

- Auf einer Informations- und Kommunikationsplattform zum Thema Arbeitsmarkt in Österreich wurde das Profil einer Führungskraft für Personal und Finanzen eines staatlichen Fonds erstellt und veröffentlicht.

Weiters wurde eine von der Führungskraft an den Plattformbetreiber verfasste E-Mail veröffentlicht, die ein Lösungsersuchen sowie Vorwürfe enthielt. Die Führungskraft erhob Datenschutzbeschwerde. Aufgrund des Lösungsersuchens entfernte der Plattformbetreiber das Profil der Führungskraft von der Webseite. Die E-Mail samt beruflicher Kontaktdaten blieb aber auf der Webseite sichtbar. Die DSB wies die Datenschutzbeschwerde ab.

Die DSB hat erwogen: Das neue **Medienprivileg** des **§ 9 Abs 1a DSG** erlaubt dem Verantwortlichen, bestimmte sensible Daten gemäß Art 9 DSGVO und bestimmte strafrechtlich relevante Daten gemäß Art 10 DSGVO zur Wahrung **berechtigter Interessen** zu verarbeiten, soweit dies zur Ausübung der **Meinungsäußerungs- und Informationsfreiheit** erforderlich und verhältnismäßig ist. Im Sinne eines Umkehrschlusses erlaubt § 9 Abs 1a DSG auch die Verarbeitung nicht-sensibler personenbezogener Daten im Rahmen des **Bürgerjournalismus** aus berechtigten Interessen.

Der Plattformbetreiber hatte ein **berechtigtes Interesse** an der Veröffentlichung der E-Mail, weil diese die Vorgehensweise des Fonds dokumentiert sowie eine öffentliche Diskussion und die öffentliche Widerlegung der in der E-Mail erhobenen Vorwürfe ermöglicht. Die Veröffentlichung ist auch **erforderlich**, um den angestrebten Zweck zu erreichen. Ein bloßer Hinweis auf die Aufforderung zur Löschung von Beiträgen hätte nicht dieselbe Überzeugungswirkung bei den Lesern wie eine Veröffentlichung im Original.

Die **Abwägung** zwischen dem Grundrecht auf Datenschutz der Führungskraft und dem Recht auf Freiheit der Meinungsäußerung und der Informationsfreiheit des Plattformbetreibers geht zu Gunsten des Letzteren aus, weil lediglich der Inhalt einer Nachricht, die von öffentlichem Interesse ist, sowie die beruflichen Kontaktdaten der Führungskraft veröffentlicht wurden. **Berufliche Kontaktdaten** sind nicht besonders schutzwürdig, weil sie öffentlich leicht zugänglich sind.

Da das einzig erkennbare Motiv der Verarbeitung in der Verbreitung von Informationen (Vorgehensweise des Fonds und seiner Führungskräfte) lag, ist eine **journalistische Tätigkeit** iSd § 9 Abs 1a DSG gegeben, die auch gerechtfertigt ist.

Die Webseite ist als **Medium** iSd § 1 Abs 1 Z 1 MedienG zu qualifizieren, weil es ihr um die Verbreitung von Informationen an einen größeren Personenkreis im Wege der **Massenverbreitung** geht. Gemäß § 9 Abs 1a DSG ist das **Recht auf Löschung** auf personenbezogene Daten, die von einem Medium zu journalistischen Zwecken veröffentlicht wurden, **nicht anwendbar**.

**Videoüberwachung, Behörde, Privatwirtschaftsverwaltung, berechtigtes Interesse**

- Die DSB leitete aufgrund einer **anonymen Anzeige** ein amtswegiges Prüfverfahren gegen die Magistratsabteilung 6 (MA 6) ein, weil diese an verschiedenen Standorten eine umfassende Videoüberwachung vornahm. Insgesamt wurden an 19 Standorten 44 Kameras betrieben, welche die Warte- und Kassenbereiche überwachten. Die Kassenbereiche wurden sowohl von außen als Kundensicht als auch von innen aus Sicht der Mitarbeiter erfasst. Die Aufnahmen wurden **verschlüsselt** für **72 Stunden** auf Servern im geschützten Rechenzentrum der Stadt Wien gespeichert, wobei auf die Live-Bilder die MA 6 und die Wache Rathaus zugreifen konnten. Abseits von den Live-Bildern konnte nur die MA 1 im Auftrag der MA 6 auf die Aufnahmen zugreifen. Die Mitarbeiter der MA 6 wurden zwar über die Kameras informiert, ihre Einwilligung wurde jedoch nicht eingeholt.

Die MA 6 führte aus, dass die Überwachung dem **Personen- und Objektschutz** diene, weil an den Standorten große Geldmengen verwaltet würden und es in der Vergangenheit bereits zu Raubüberfällen und Bedrohungen gekommen sei. Die DSB ordnete an, dass sämtliche Kameras binnen acht Wochen so einzustellen sind, dass die Arbeitsplätze und regelmäßig genutzte interne Bereiche nicht mehr erfasst werden.

Die DSB hat erwogen: Die Videoüberwachung identifizierbarer Personen ist eine Verarbeitung personenbezogener Daten. Die MA 6 war zur selbständigen Entscheidung über die Durchführung einer Videoüberwachung an den Standorten und damit über den Zweck der Verarbeitung befugt. Auch wenn andere Magistratsabteilungen einen gewissen Einfluss auf die Mittel der Videoüberwachung ausgeübt haben, hatte die MA 6 ausreichend Kenntnis über die konkreten Aufnahmebereiche der Videokameras und ist damit **Verantwortliche** iSd Art 4 Z 7 DSGVO.

Die MA 6 darf die **Videoüberwachung** im Rahmen der **Privatwirtschaftsverwaltung** grundsätzlich auf ihre **berechtigten Interessen** stützen, wenn die Verarbeitung erforderlich ist und die Grundrechte und Grundfreiheiten der Betroffenen nicht überwiegen. Da es zuvor zu dokumentierten Raub- und Drohvorfällen gekommen ist, große Bargeldbestände verwaltet werden und eine hohe Kundenfrequenz besteht, liegt eine tatsächliche **Gefährdungslage** und damit ein **berechtigtes Interesse** vor. Die Videoüberwachung ist grundsätzlich auch geeignet, weil die

Einsichtnahmemöglichkeit der **Wache Rathaus** durch die rasche Gefahreinschätzungs- und Eingriffsmöglichkeit einen präventiven Schutz bieten kann und eine abschreckende Wirkung hat.

Die **Außenkameras**, die ausschließlich Warte- und Kassenbereiche außen erfassen, haben einen begrenzten Aufnahmebereich, eine kurze Speicherdauer, strenge Zugriffsregelungen und erfassen keine sensiblen Räume und sind erforderlich. Auch überwiegt das Interesse der MA 6, die körperliche Unversehrtheit ihrer Mitarbeiter und ihr Eigentum zu schützen, dem Interesse der Betroffenen. Die **Innenkameras**, die die Arbeitsplätze oder Bildschirme der Mitarbeiter dauerhaft filmen, sind jedoch nicht erforderlich, weil ein gleich wirksamer Schutz bereits durch die Außenkameras erreicht ist.

to the point

# Datenschutzmonitor. 34/2025 vom 27.08.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des VfGH**

VfGH 12.08.2025, DS1/2025 (Doppelgleisigkeit, Zuständigkeit, justizielle Tätigkeit, Web-ERV)

- **Rechtsprechung des VwGH**

VwGH 28.07.2025, Fr 2025/04/0002 (Zuständigkeit, DSGVO)

- **Rechtsprechung der Justiz**

OLG Linz 10.06.2025, 7Bs96/25d (Handyauswertung, Cloud-Speicher, HealthApp)

- **Rechtsprechung des BVwG**

BVwG 22.05.2025, W101 2295861-1 (Geldbuße, COVID, Gesundheitsdaten, Strafbemessung)

BVwG 02.06.2025, W292 2298457-1 (Geldbuße, Google-Rezension, berechtigte Interessen)

BVwG 17.06.2025, W252 2296540-1 (Videoüberwachung, Dienstverhältnis, Einwilligung)

BVwG 30.06.2025, W137 2295299-1 (Geheimhaltungsinteresse, Familienangehöriger, Personenbezug, Bescheidzustellung)

BVwG 09.07.2025, W274 2259250-1 (Auskunft, Rechtsschutzbedürfnis, Einstellung)

BVwG 05.06.2025, W211 2296350-1 (AuskunftspflichtG, vorhandene Informationen)

BVwG 27.05.2025, W603 2304292-1 (unerbetene Nachricht, Privatsphäre, Ermahnung)

BVwG 03.07.2025, W252 2312918-2 (Verfahrenshilfe, Dokumentenkopie)

BVwG 30.06.2025, W211 2307833-1 (Auskunft, Feststellung, Sanierung)

- **EU-Rechtsakte**

Berichtigung der Durchführungsverordnung (EU) 2025/1570 zur eIDAS-VO



## To the Point:

### Rechtsprechung des VfGH

VfGH 12.08.2025, DS1/2025

#### **Doppelgleisigkeit, Zuständigkeit, justizielle Tätigkeit, Web-ERV**

- Ein Rechtsanwalt erhob Datenschutzbeschwerde bei der DSB, weil die verpflichtende Nutzung des Web-basierten Elektronischen Rechtsverkehrs (Web-ERV) gegen Art 5 und 25 DSGVO verstoßen würde. Er behauptete, der Web-ERV funktioniere fehlerhaft, produziere irreführende Sendebestätigungen und biete keine ausreichenden Kontroll- und Korrekturmöglichkeiten. Dadurch sei eine von ihm an das BVwG gerichtete Revision fälschlicherweise beim VfGH eingebracht worden, was zu erheblichen Kosten und drohendem Rechtsverlust geführt habe. Die Datenschutzbeschwerde war wegen der verpflichtenden Verwendung des Web-ERV ua auch gegen den VfGH gerichtet. Die DSB übermittelte die Datenschutzbeschwerde zur Stellungnahme an den Präsidenten des VfGH. Dieser gab jedoch keine Stellungnahme ab, sondern der VfGH entschied in der Sache selbst und wies die Beschwerde ab.

Der VfGH hat erwogen: In Art 55 Abs 3 DSGVO trifft der Unionsgesetzgeber eine von der (unionsrechtlich zwingenden) **Doppelgleisigkeit** des Rechtsschutzes abweichende Sonderregelung. Die DSB ist gemäß Art 55 Abs 3 DSGVO nicht zuständig für Beschwerden gegen Datenverarbeitungen im Rahmen der **justiziellen Tätigkeit** von Gerichten. Über Beschwerden hinsichtlich der justiziellen Tätigkeit des VfGH entscheidet dieser selbst (§ 88b VfGG iVm §§ 84, 85 GOG).

Im Hinblick auf das **unionsrechtliche Effektivitätsgebot** ist der VfGH gehalten, ohne weitere Zwischenschritte (zB Stellungnahme des VfGH an die DSB) sofort in der Sache selbst zu entscheiden, ohne den Rechtsanwalt auf eine (prozessuale) Entscheidung der DSB zu verweisen.

Der EuGH geht von einem weiten Verständnis der justiziellen Tätigkeit aus. Die vom Rechtsanwalt behauptete Verletzung der Art 5 und 25 DSGVO aufgrund der verpflichtenden **Verwendung des Web-ERV** betrifft jedenfalls eine justizielle Tätigkeit, weil die Verwendung des Web-ERV für Eingaben an den VfGH grundsätzlich eine **Formvorschrift** ist.

**Technische Schwierigkeiten oder Bedienungsfehler** bei der Nutzung des Web-ERV begründen **keinen Verstoß** gegen Art 5 oder Art 25 DSGVO. Die behaupteten Mängel des Web-ERV betreffen keine datenschutzrechtlichen Grundsätze. Fälle unrichtiger Sendebestätigungen können allenfalls

zu einer **Wiedereinsetzung in den vorigen Stand** führen.

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Der VwGH erkennt nach Art 133 Abs 2a B-VG über Beschwerden einer Person, die durch den **VwGH** in Ausübung seiner **gerichtlichen Zuständigkeit** in ihren Rechten gemäß der DSGVO verletzt zu sein behauptet ([\(VwGH 28.07.2025, Fr 2025/04/0002\)](#)).

### Rechtsprechung der Justiz

Aus der Rechtsprechung der Justiz:

- Die **Beschlagnahme** von **Daten**, insb Standortdaten auf einem **Mobiltelefon** und der Zugriff auf Datenträger, einschließlich externer Datenträger (insb **Cloud-Speicherplätze**), ist zur Aufklärung eines Einbruchdiebstahls zulässig. Die staatsanwaltliche Anordnung sowie die gerichtliche Bewilligung dieser Anordnung unterliegen jedoch einer **erhöhten Begründungspflicht**. Die zu beschlagnahmenden **Datenkategorien** und **Dateninhalte** sind zu umschreiben. Bei der Beurteilung im Einzelfall ist der **Verhältnismäßigkeitsgrundsatz** anzuwenden. Die Auswertung von **Gesundheitsdaten** wie die Aufzeichnungen einer **HealthApp** (zB Wegstrecken, Schritte, etc) ist unverhältnismäßig. Die Beschwerde des **Rechtsschutzbeauftragten der Justiz** ist somit berechtigt ([\(OLG Linz 10.06.2025, 7Bs96/25d\)](#)).

### Rechtsprechung des BVwG

BVwG 22.05.2025, W101 2295861-1

#### **Geldbuße, COVID, Gesundheitsdaten, Strafbemessung**

- Ein PCR-Testlabor wurde während der Covid-19-Pandemie mittels Direktvergabe vom Land Tirol beauftragt, PCR-Tests durchzuführen. Später entzog das Land Tirol dem PCR-Testlabor den Auftrag und führte eine Ausschreibung durch. Den Zuschlag erhielt in der Folge ein anderes Unternehmen als Nachfolgerin des PCR-Testlabors. Während der Übergangsphase wurden die Testergebnisse des PCR-Testlabors in eine Software der Nachfolgerin eingetragen. Nachdem der ehemalige Geschäftsführer eine E-Mail mit rund 24.000 personenbezogenen PCR-Testdaten an einen Dritten versendete, leitete die DSB ein amtswegiges Prüfverfahren ein. Sie stellte zahlreiche DSGVO-Verstöße fest, darunter (i) die unrechtmäßige Verarbeitung von Gesundheitsdaten, (ii) unzureichende Datensicherheitsmaßnahmen nach Art 32 DSGVO, (iii) die unterbliebene Benachrichtigung der

Betroffenen gemäß Art 34 DSGVO sowie (iv) einen zeitweise fehlenden Auftragsverarbeitervertrag zwischen PCR-Testlabor und Nachfolgerin. Für diese Verstöße verhängte die DSB eine Geldstrafe iHv EUR 96.000. Darüber hinaus stellte die DSB fest, dass (v) die bestellte Datenschutzbeauftragte unqualifiziert gewesen und (vi) ihre Benennung verspätet gemeldet worden sei, wofür sie eine weitere Geldstrafe iHv EUR 4.000 verhängte. Das BVwG gab der Bescheidbeschwerde des PCR-Labors in Bezug auf die ersten drei Verstöße statt und behob diese Spruchpunkte des Straferkenntnisses der DSB. Die Bescheidbeschwerde zum fehlenden Auftragsverarbeitervertrag wurde abgewiesen und wegen dieser Tatverwirklichung wurde eine neue Strafe iHv EUR 4.000 verhängt. Die Strafe iZm der Datenschutzbeauftragten wurde abgewiesen und auf EUR 3.000 herabgesetzt.

Das BVwG hat erwogen: Das PCR-Testlabor hat die Gesundheitsdaten nicht unrechtmäßig verarbeitet. Es konnten auch keine Sicherheitsverletzungen erwiesen werden.

Voraussetzung für die **Benachrichtigungspflicht** nach Art 34 Abs 1 DSGVO ist das Vorliegen einer **Datenschutzverletzung**, die dem Verantwortlichen bekannt geworden ist. Da dem PCR-Testlabor weder eine unrechtmäßige Verarbeitung von Gesundheitsdaten noch eine Sicherheitsverletzung nach Art 32 Abs 1 DSGVO vorwerfbar ist, ist diese Tatbestandsvoraussetzung nicht erfüllt.

Bei der **Strafbemessung** ist nicht der Umsatz im letzten abgeschlossenen Geschäftsjahr vor Erlass des Straferkenntnisses zu berücksichtigen, sondern die im Entscheidungszeitpunkt des BVwG aktuelle Einkommens- und Vermögenslage. **Anm: Die Strafbemessung ist nicht mit der Festsetzung des Höchstmaßes der Geldbuße (Strafrahmens) zu verwechseln.**

BVwG 02.06.2025, W292 2298457-1

### **Geldbuße, Google-Rezension, berechnete Interessen**

- Eine Kundin stornierte eine Online-Bestellung bei einem Blumenhändler und verlangte die Rückzahlung des Kaufpreises. Nachdem der Blumenhändler dies verweigerte, veröffentlichte die Kundin eine negative Google-Rezension. In Beantwortung dieser Rezension nannte der Blumenhändler den vollständigen Vor- und Nachnamen der Kundin. Die DSB verhängte eine Geldstrafe iHv EUR 400. Gegen dieses Straferkenntnis erhob der Blumenhändler (erfolglos) Bescheidbeschwerde an das BVwG. Er behauptete, dass er in seiner Datenschutzerklärung auf seiner Webseite darüber informierte, dass personenbezogene Daten zum

Zweck der Reaktion auf Kundenrezensionen verwendet werden könnten.

Das BVwG hat erwogen: Gemäß Art 4 Z 11 DSGVO liegt eine Einwilligung nur vor, wenn sie freiwillig, in informierter Weise und unmissverständlich abgegeben wurde. Die Online-Bestellung der Kundin kann nicht als Einwilligung gewertet werden, dass der Blumenhändler bei einer späteren Google-Rezension den vollständigen Vor- und Nachnamen der Rezensentin offenlegen darf.

Behandelt ein Vertrag mehrere Aspekte, muss eine **Einwilligung klar hervorgehoben** sein, ein bloßer **Hinweis** in der Datenschutzinformation **genügt nicht**. Die Offenlegung des vollständigen Namens der Kundin kann damit nicht auf den Erlaubnisatbestand der Einwilligung iSd Art 6 Abs 1 lit a DSGVO gestützt werden. Auch ist nicht ersichtlich, in welchem Zusammenhang die Veröffentlichung des Vor- und Nachnamens der Kundin erforderlich gewesen sein sollte, um den Kaufvertrag zu erfüllen oder vorvertragliche Leistungen zu erbringen.

Der Blumenhändler hat zwar ein **berechtigtes Interesse** an der **Wahrung seiner geschäftlichen Reputation**. Die Offenlegung des Vor- und Nachnamens war aber nicht zur Wahrung eines ideellen oder wirtschaftlichen Interesses erforderlich. Es besteht jedoch ein anerkanntes **Interesse von Internetnutzern** dahingehend, ihre **Identität nicht offenzulegen**. Die Möglichkeit von **anonymen Meinungsäußerungen** darf **im Internet** nicht schlechthin unterbunden werden.

Der Inhalt der Rezension der Kundin war weder unsachlich noch ein Wertungsexzess. Da die Verarbeitung für die Kundin nicht vorhersehbar war, verstößt sie gegen den **Grundsatz nach Treu und Glauben**.

Die **vorsätzliche Veröffentlichung** kann nicht als geringfügiger Verstoß, der das Absehen von einer Geldbuße ermöglichen würde, qualifiziert werden.

BVwG 17.06.2025, W252 2296540-1

### **Videoüberwachung, Dienstverhältnis, Einwilligung**

- Ein Unternehmen betrieb in seinen Geschäftsräumlichkeiten eine auf den Hintereingang gerichtete Überwachungskamera, um sein Eigentum zu schützen. Die Kamera erfasste jedoch auch Arbeitsplätze, einen Ablagebereich und die Teeküche. Eine ehemalige Mitarbeiterin erachtete sich in ihrem Recht auf Geheimhaltung verletzt und erhob Datenschutzbeschwerde bei der DSB. Die DSB gab der Datenschutzbeschwerde teilweise statt und trug dem Unternehmen auf, den Aufnahmebereich zeitlich und örtlich einzuschränken. Dagegen erhob das Unternehmen (erfolglose)

Bescheidbeschwerde an das BVwG. Darin behauptete es, dass die Angestellte über die Videoüberwachung informiert wurde und ein Hinweisschild am Eingang angebracht sei. Da sich die Angestellte nicht gegen die Videoüberwachung aussprach, sei von einer konkludenten Zustimmung auszugehen.

Das BVwG hat erwogen: Die Aufnahmen der ehemaligen Mitarbeiterin, die eindeutig identifiziert werden kann, sind als **personenbezogene Daten** iSd Art 4 Z 1 DSGVO zu qualifizieren.

Die Einwilligung nach Art 4 Z 11 DSGVO verlangt eine **aktive Einwilligung**. **Stillschweigen** oder eine **konkludente Zustimmung genügt nicht**. Dass die ehemalige Mitarbeiterin nichts gegen die Kameras gesagt hat, ersetzt keine gültige Einwilligung.

Der **Schutz des Eigentums** ist ein **berechtigtes Interesse**. Die Erforderlichkeit verlangt, dass die Videoüberwachung auf das notwendige Maß beschränkt wird. Da der Eigentumsschutz während der Öffnungszeiten bereits **durch die Anwesenheit der Mitarbeiter gewährleistet** wurde, war die Überwachung während der Arbeitszeit und in Bereichen wie Arbeitsplätzen und Teeküche für die Überwachung des Hintereingangs nicht erforderlich.

Entspricht eine Verarbeitung nicht den Anforderungen der DSGVO, sind geeignete **Abhilfemaßnahmen** zu erlassen. Auch die übrigen Dienstnehmer des Unternehmens haben nicht aktiv in die Videoüberwachung eingewilligt. Die Freiwilligkeit einer Einwilligung im **Beschäftigungskontext** ist wegen des **Machtungleichgewichts** besonders schwer nachzuweisen. Die vom Unternehmen vorgelegten "DSGVO-Verträge" mit den Angestellten enthielten keine ausdrückliche Einwilligung zur Videoüberwachung und genügen somit nicht den Anforderungen der DSGVO. Die DSB ordnete zu Recht an, die Videoüberwachung **zeitlich auf die Zeit zwischen Betriebsschluss und Betriebsbeginn zu beschränken**.

BVwG 30.06.2025, W137 2295299-1

#### **Geheimhaltungsinteresse, Personenbezug, Familienangehöriger, Bescheidzustellung**

- Ein Sohn war gemeinsam mit seinem Vater mit identem Namen an derselben Adresse gemeldet. Ein an den Sohn adressierter Bescheid wurde aufgrund fehlender akademischer Titel im Adressfeld irrtümlich vom Vater geöffnet, wodurch diesem die im Bescheid enthaltenen personenbezogenen Daten des Sohnes zugänglich wurden. Der Sohn erhob daraufhin Datenschutzbeschwerde wegen Verletzung im Recht auf Geheimhaltung. Die DSB vertrat die Ansicht, dass der Inhalt des Bescheids aufgrund der Verknüpfung mit dem Namen des

Sohnes als Verarbeitung seiner personenbezogenen Daten zu werten sei. Die beschneiderlassende Behörde habe verabsäumt, ausreichende organisatorische Maßnahmen zu ergreifen, um unbefugten Zugang zu den personenbezogenen Daten zu verhindern. Dagegen erhob die Behörde (erfolgreich) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Der Bescheid stellt nicht schon in seinem gesamten Inhalt personenbezogene Daten des Beschwerdeführers dar. Nach dieser Logik wären auch personenbezogene Daten Dritter, die in einen Bescheid Eingang finden, personenbezogene Daten des Bescheidadressaten. Eine derartige Ausdehnung kann aber auch dem weiten Begriff von personenbezogenen Daten iSd Art 4 Z 1 DSGVO keinesfalls unterstellt werden. Tatsächlich verbleiben als **personenbezogene Daten** des Sohnes lediglich die **Wohnadresse** und der **Umstand des Grundstückseigentums**.

Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Geheimhaltungsinteresse daran besteht. Die Beurteilung der Schutzwürdigkeit der Interessenlage hat unter Berücksichtigung aller **konkreten Umstände des Einzelfalls** nach einem **objektiven Maßstab** zu erfolgen. Entscheidend ist, ob das zu beurteilende **Geheimhaltungsinteresse** bei der gegebenen Fallgestaltung für jedermann und generell schutzwürdig ist. Ein solches Interesse ist hinsichtlich der Wohnadresse einer Person **gegenüber Personen in der eigenen Hausgemeinschaft** jedenfalls zu **verneinen**. Denn jede Briefsendung, die der an selbiger Adresse wohnhafte Vater entgegennehmen darf, würde sonst bereits eine Verletzung eines berechtigten Interesses an der Geheimhaltung des personenbezogenen Datums "Wohnsitz/Meldeadresse" bedeuten. Auch hinsichtlich des Grundstückseigentums des Sohnes kann im konkreten Fall kein schutzwürdiges Interesse an der Geheimhaltung erkannt werden, weil der Vater dem Sohn das Grundstück selbst übereignet hat. **Anm: Das BVwG verneint erstmals, dass die Zuordnung von Informationen zu einer identifizierten Person zugleich den Personenbezug dieser Informationen begründet. Es weist auch erstmals darauf hin, dass Voraussetzung für eine Geheimhaltungspflichtverletzung ein Geheimhaltungsinteresse ist. Schließlich zeigt diese Entscheidung auch, dass das Versenden von Schriftstücken (zB Briefe) nur aufgrund von Name und Adresse vor (potenziellen) Fehlzustellungen nicht schützt.**

## Auskunft, Rechtsschutzbedürfnis, Einstellung

- Ein Betroffener beehrte iZm einem Datensicherheitsvorfall Auskunft beim Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz (**BMASGPK**). Da zunächst keine Auskunft erteilt wurde, erhob der Betroffene Datenschutzbeschwerde bei der DSB. Diese lehnte die Behandlung der Beschwerde mit Bescheid als exzessiv ab, weil der Betroffene bereits über 60 Datenschutzbeschwerden an die DSB erhoben hat. Das BVwG gab der Bescheidbeschwerde des Betroffenen im ersten Rechtsgang Folge, behob den Bescheid der DSB und trug ihr die Fortsetzung des Verfahrens auf. Die DSB erhob außerordentliche Revision an den VwGH, der das Erkenntnis des BVwG aufhob und diesem die neuerliche Entscheidung nach Einräumung von Parteihör auftrag. Im zweiten Verfahrensgang vor dem BVwG teilte die DSB mit, dass der BMASGPK inzwischen Auskunft erteilt hat. Die DSB stellte das Verfahren ein und brachte dies dem Betroffenen zur Kenntnis. Auch das BVwG stellte das Verfahren wegen Wegfalls des Rechtsschutzbedürfnisses des Betroffenen infolge zwischenzeitlich ergangener Datenauskunft ein.

Das BVwG hat erwogen: **Prozessvoraussetzung** für das Verfahren vor dem VwGH ist das **Rechtsschutzbedürfnis**. Fehlt dieses schon bei Einbringung einer Revision, ist diese unzulässig. Fällt die Voraussetzung erst nach der Einbringung der Revision weg, führt dies zur Verfahrenseinstellung. Diese Grundsätze können auf Verfahren vor dem BVwG übertragen werden. Da eine Auskunft erteilt wurde, ist das **Rechtsschutzinteresse** des Betroffenen **weggefallen**, sodass das Verfahren **einzustellen** war. **Anm: Während das Verfahren beim BVwG oder VwGH anhängig ist, ist die DSB unzuständig. Sie hätte das Verfahren nicht einstellen dürfen.**

### Aus der weiteren Rechtsprechung des BVwG:

- Auskünfte nach dem **AuskunftspflichtG** sind **Wissenserklärungen**. Ihr Inhalt ist auf Informationen beschränkt, die zum Zeitpunkt der Anfrage der Verwaltung **bekannt sind**. Umfasst ist nur **gesichertes Wissen** im tatsächlichen oder rechtlichen Bereich. Die Auskunftserteilung darf die übrigen **Aufgaben der Verwaltung nicht wesentlich beeinträchtigen**. Da die Behörde für die Auskunftserteilung eine Analyse von Datensätzen in mehreren Arbeitsschritten hätte vornehmen müssen, verfügte sie nicht über die begehrten Informationen, weshalb die Auskunft zu Recht verweigert wurde. Eine Prüfung, ob die Interessen Dritter beeinträchtigt werden könnten,

war nicht erforderlich ([BVwG 05.06.2025, W211 2296350-1](#)). **Anm: Diese Entscheidung wird auf das neue **Informationsfreiheitsgesetz (IFG)** voraussichtlich übertragen werden. Denn auch nach dem IFG sind nur verfügbare Informationen zu erteilen (§ 2 Abs 1 IFG).**

- Das Versenden **unerbetener E-Mail-Nachrichten** ist verboten (§ 174 TKG). Das durch die verletzte Norm geschützte Rechtsgut ist die **Privatsphäre** von natürlichen Personen. Der Gesetzgeber hat durch die mögliche **Höchststrafe** von **EUR 50.000** die hohe Wertigkeit des durch die verletzte Norm geschützten Rechtsguts zum Ausdruck gebracht. Durch die Zusendung der unerbetenen elektronischen Nachricht wird die Privatsphäre beeinträchtigt. Der Ausspruch einer **Ermahnung** gemäß § 45 Abs 1 VStG scheidet daher aus. Die öffentliche mündliche **Verhandlung** wurde **online** durchgeführt ([BVwG 27.05.2025, W603 2304292-1](#)).
- Erscheint die Rechtsverfolgung (oder Rechtsverteidigung) als "offenbar mutwillig" oder "aussichtslos", ist keine **Verfahrenshilfe** zu bewilligen. Die beabsichtigte Rechtsverfolgung erweist sich als aussichtslos. Im Verfahren haben sich keine Anhaltspunkte ergeben, wonach es unerlässlich wäre, eine **originalgetreue Reproduktion** von **Dokumenten** wie Einvernahme- und Sicherstellungsprotokolle, Bescheide und Bescheidentwürfe oder Korrespondenzen auszuführen. Dem Auskunftsanspruch des Verfahrenshilfewerbers wurde bereits in vollem Umfang entsprochen ([BVwG 03.07.2025, W252 2312918-2](#)).
- Der Auskunftswerberin wurde während des Verfahrens vor dem BVwG **Auskunft** erteilt. Wenn das Rechtsschutzbegehren auf die Erlangung einer bestimmten Leistung gerichtet ist, die **zum Entscheidungszeitpunkt als erfüllt** anzusehen ist, ist davon auszugehen, dass das **Rechtsschutzziel erreicht** wurde. Gegenstand des Verfahrens war ausschließlich die monierte Nichtreaktion des Unternehmens auf das Auskunftersuchen der Betroffenen. Die Frage einer etwaigen Verspätung der Auskunftserteilung ist im Verfahren über das Auskunftsbegehren selbst nicht zu klären. Ein **Anspruch auf Feststellung der Verspätung besteht nicht** ([BVwG 30.06.2025, W211 2307833-1](#)).

### EU-Rechtsakte

- Am **20.08.2025** wurde die "**Berichtigung der Durchführungsverordnung (EU) 2025/1570 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und**

*des Rates in Bezug auf die Notifizierung von Informationen über zertifizierte qualifizierte elektronische Signaturerstellungseinheiten und zertifizierte qualifizierte elektronische Siegelerstellungseinheiten", [ABl L 2025/90654](#), kundgemacht. Der Berichtigung kommt Relevanz zu, weil das Datum, an dem die berichtigte DurchführungsVO **in Geltung tritt**, vom 19.12.2025 auf den 19.11.2025 "vorverlegt" wurde.*

to the point

# Datenschutzmonitor. 35/2025 vom 03.09.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des VwGH**

VwGH 29.07.2025, Ro 2022/04/0017 (Rollenverteilung, ELAK, Anwendungsbereich)

VwGH 01.08.2025, Ro 2023/04/0030;  
01.08.2025, Ro 2023/04/0031 (Onlineshop, Einwilligung, Koppelungsverbot)

- **Rechtsprechung der Justiz**

OGH 13.08.2025, 6Ob15/25m (Vorabentscheidungsersuchen, automatisierte Entscheidungsfindung, Bonitätsprüfung, Zahlungsarten)

- **Rechtsprechung des BVwG**

BVwG 27.05.2025, W605 2270910-1 (Adressverlag, Kreditauskunftei, Zweckänderung, Abhilfebefugnis)

BVwG 30.06.2025, W137 2253891-1 (FMA, Behörde, Empfänger, Auskunft)

BVwG 01.07.2025, W256 2252595-1 (Rechtsanspruch, strafrechtliche Verurteilung, berechtigtes Interesse)

BVwG 20.06.2025, W291 2300813-1 (Geldbuße, Videoüberwachung, Rollenverteilung)

BVwG 01.07.2025, W176 2226261-1 (Exzess, Missbrauchsabsicht)

BVwG 03.07.2025, W211 2301099-1 (ORF-Beitrag, Inkasso, Rückstandsausweis)

- **Rechtsprechung des BFG**

BFG 02.07.2025, RV/7104521/2020 (Glücksspielabgabe, Wettgebühr, Inland)

BFG 08.07.2025, RV/4100275/2022;  
08.07.2025, RV/4100327/2023 (Abgabenerhebung, Gesundheitsdaten, außergewöhnliche Belastung)

- **EU-Rechtsakte**

Durchführungsverordnung (EU) 2025/1328 zur Gesamtenergieeffizienz von Gebäuden

- **Nationale Rechtsakte**

Daten-Governance-Benennungsverordnung

Fünfte Änderung der FinanzOnline-Verordnung 2006

Oö. Informationsfreiheits-Anpassungsverordnung-Agrar

Steiermärkisches Informationsfreiheitsanpassungsgesetz 2025

## To the Point:

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Verarbeitet ein **Referatsleiter** personenbezogene Daten im **Rahmen seiner dienstlichen Aufgaben**, etwa zur Führung eines dienstrechtlichen Verfahrens, ist die **Organisation Verantwortlicher**. Eine Verantwortlichenstellung kann auch in der Speicherung personenbezogener Daten bestehen, der eine Weiterverarbeitung durch Bedienstete zugrunde liegt. Wird ein **ärztliches Gutachten** mit personenbezogenen Daten im **elektronischen Akt (ELAK)** erfasst, ist der **Anwendungsbereich der DSGVO** eröffnet. Daran ändert es auch nichts, wenn **mehrere identische Ausfertigungen** eines ärztlichen Gutachtens übermittelt werden ([VwGH 29.07.2025, Ro 2022/04/0017](#)).
- Die **Hauptleistungspflichten** beim Bestellen in einem Onlineshop sind **Ware gegen Geld**. Diese Hauptleistungspflichten bleiben ident, unabhängig davon, ob die Bestellung über ein **Kunden-** oder ein **Gastkonto** aufgegeben wird. Der Mehraufwand, der mit dem Bestellen über ein Gastkonto verbunden ist, ist dem Betroffenen zumutbar. Die Möglichkeit, Bestellinformationen im Kundenkonto zu speichern, ist nur ein **zulässiger Anreiz**. Der Betreiber des Onlineshops verstößt nicht gegen das **Koppelungsverbot**, wenn die Registrierung im Onlineshop mit der Verarbeitung der Kundendaten zu **Werbe-, Marketing- oder Kundenbetreuungszwecken** verbunden ist, solange, die Möglichkeit besteht, die Bestellung als Gast aufzugeben, ohne in diese Datenverarbeitungstätigkeiten einwilligen zu müssen ([VwGH 01.08.2025, Ro 2023/04/0030](#); [01.08.2025, Ro 2023/04/0031](#)).

### Rechtsprechung der Justiz

[OGH 13.08.2025, 6Ob15/25m](#)

#### **Vorabentscheidungsersuchen, automatisierte Entscheidungsfindung, Bonitätsprüfung, Zahlungsarten**

- Ein Verbraucherschutzverein klagte gegen ein Versandhandelsunternehmen, das bei Auswahl unsicherer Zahlungsarten (Rechnung, Teilzahlung) eine **automatisierte Bonitätsprüfung** durchführte. Je nach Ergebnis wurden Kunden bestimmte Zahlungsarten verweigert und die Kunden wurden auf sichere Alternativen (Kreditkarte, PayPal) verwiesen. Die Entscheidung basierte entweder auf einer **negativen Rückmeldung** einer Auskunftsteil oder einem Bonitäts-Score. Der Verein begehrte, diese Praxis ohne ausdrückliche Einwilligung und ohne ausreichende Rechtsgewährung für

die Betroffenen gemäß Art 22 DSGVO zu unterlassen.

Der OGH beschloss, das Verfahren auszusetzen und dem EuGH mehrere Fragen zur **Vorabentscheidung** vorzulegen, die (i) die Reichweite des Begriffs der "rechtlichen Wirkung" oder "erheblichen Beeinträchtigung" bei automatisierten Entscheidungen nach Art 22 DSGVO sowie (ii) die Voraussetzungen der Erforderlichkeit solcher Entscheidungen für Vertragsabschlüsse betreffen.

Der OGH hat erwogen: Zunächst ist zu klären, ob die automatisierte Entscheidung, bestimmte **Zahlungsarten** zu verweigern, bereits eine "**rechtliche Wirkung**" entfaltet oder den Kunden "in ähnlicher Weise erheblich beeinträchtigt". Nach bisheriger Ansicht liegt keine erhebliche Beeinträchtigung vor, solange dem Kunden **zumutbare Zahlungsalternativen** verbleiben. Der EuGH hat jedoch im [Urteil vom 07.12.2023, C-634/21, SCHUFA Holding \(Scoring\)](#), ausgesprochen, dass die Ablehnung eines Kredits auf Basis eines Wahrscheinlichkeitswerts eine erhebliche Beeinträchtigung sein kann. Offen ist, ob dies auch für die bloße Einschränkung von Zahlungsarten gilt.

Sollte Art 22 Abs 1 DSGVO anzuwenden sein, ist weiter zu prüfen, ob die automatisierte Entscheidung für den Vertragsabschluss oder die Vertragserfüllung "**erforderlich**" ist (Art 22 Abs 2 lit a DSGVO). Ein sachlicher Zusammenhang zwischen Vertragszweck und Bonitätsprüfung ist grundsätzlich gegeben, weil die Auswahl der Zahlungsart das Risiko des Händlers betrifft. Fraglich ist jedoch, ob die konkret erhobenen Datenkategorien **objektiv geeignet** sein müssen, die Bonität einzuschätzen, und wer dies zu behaupten und zu beweisen hat.

Zudem ist zu klären, ob die Erforderlichkeit der automatisierten Entscheidung auch davon abhängt, ob eine **manuelle Prüfung** mit vertretbarem Aufwand möglich wäre, oder ob allein die Entscheidung als solche maßgeblich ist. Dabei könnten Faktoren wie die Anzahl der Bestellungen und die Erwartung schneller Entscheidungen im Online-Handel eine Rolle spielen.

### Rechtsprechung des BVwG

[BVwG 27.05.2025, W605 2270910-1](#)

#### **Adressverlag, Kreditauskunftei, Zweckänderung, Abhilfebefugnis**

- Ein **Adressverlag** erhob Daten eines Betroffenen zum Zweck der Ausübung seines Gewerbes gemäß § 151 GewO und übermittelte diese aufgrund einer vertraglichen Vereinbarung an eine **Kreditauskunftei**. Diese verarbeitete die ihr übermittelten Daten zum Zweck der Ausübung des Gewerbes

der Kreditauskunfteien gemäß § 152 GewO. Der Betroffene erhob gegen beide Unternehmen Datenschutzbeschwerde bei der DSB wegen Verletzung des **Zweckbindungsgrundsatzes** gemäß Art 5 Abs 2 lit b iVm Art 6 Abs 4 DSGVO und beantragte, dass ein **Verarbeitungsverbot** gegen die Kreditauskunftei verhängt werde.

Im **Parallelverfahren** gab die DSB der Datenschutzbeschwerde gegen den Adressverlag statt und stellte einen Verstoß gegen den Zweckbindungsgrundsatz gemäß Art 5 Abs 1 lit b DSGVO und eine unrechtmäßige Datenverarbeitung gemäß Art 6 Abs 1 iVm Abs 4 DSGVO fest.

Die DSB gab auch der Datenschutzbeschwerde gegen die Kreditauskunftei statt. Sie stellte fest, dass die Daten unrechtmäßig zu Bonitätsbeurteilungszwecken verarbeitet wurden. Hinsichtlich der behaupteten Verletzung des Grundsatzes der Zweckbindung wies die DSB die Datenschutzbeschwerde jedoch ab. Der Antrag auf Verhängung eines Datenverarbeitungsverbots wurde von der DSB zurückgewiesen. Der Betroffene und die Kreditauskunftei erhoben jeweils Bescheidbeschwerde an das BVwG. Dieses bestätigte die Rechtswidrigkeit der Verarbeitung und stellte auch einen Verstoß gegen den Zweckbindungsgrundsatz fest. Den Antrag auf Verhängung eines Verarbeitungsverbots wies das BVwG ab.

Das BVwG hat erwogen: Betroffene können eine **Datenschutzbeschwerde** auf jede DSGVO-Bestimmung stützen, sofern ihre Rechtsposition verletzt ist, sodass auch objektive Verstöße gegen die Grundsätze des Art 5 DSGVO nach Art 77 DSGVO oder § 24 Abs 1 DSg geltend gemacht werden können.

Adressverlage dürfen Marketingdaten **nur für Marketingzwecke** verwenden oder übermitteln. Daten von Adressverlagen dürfen daher nicht zur Prüfung eines Vertragsabschlusses oder der Bonität benutzt werden. Auch wenn das Kreditinstitut die Daten vom Adressverlag aufgrund dessen Gewerbeberechtigung gemäß § 151 GewO erworben hat, erfolgte deren (Weiter-)Verarbeitung zu Bonitätszwecken und zur Ausübung des Gewerbes der Kreditauskunftei. Dies stellt im Vergleich zur ursprünglichen Ermittlung für Marketingzwecke eine **Zweckänderung** dar.

Die Kriterien des Art 6 Abs 4 DSGVO stellen sicher, dass die **Weiterverarbeitung eng mit dem ursprünglichen Zweck verbunden** ist und den legitimen Erwartungen der Betroffenen entspricht. Jede Verarbeitung personenbezogener Daten muss daher **kumulativ** den in Art 5 DSGVO aufgestellten Grundsätzen und einem der in Art 6 DSGVO angeführten Erlaubnistatbestände genügen. Da bereits eine Verletzung des Art 5 DSGVO zu bejahen ist, kann eine Prüfung der

Rechtmäßigkeit gemäß Art 6 Abs 1 DSGVO dahingestellt bleiben, weil die Übermittlung jedenfalls im Ergebnis unrechtmäßig war.

Auch die **Kreditauskunftei** verstieß gegen den Zweckbindungsgrundsatz, indem sie Daten vom Adressverlag, die gesetzlich nur für Marketingzwecke erhoben und übermittelt werden dürfen, zur Ausübung des Gewerbes der Kreditauskunfteien verwendete. Der Zweckbindungsgrundsatz bindet auch den Verantwortlichen, der die Daten **weiterverarbeitet**, an die ursprüngliche Zweckfestsetzung. Es kommt nicht darauf an, ob und zu welchem Zeitpunkt die Kreditauskunftei Einfluss auf den Zweck der Datenerhebung durch den Adressverlag hatte. Entscheidend ist, dass die Kreditauskunftei die Daten von einem Adressverlag bezogen hat, für die der Gesetzgeber einen Zweck eindeutig definiert hat. Es war der Kreditauskunftei somit gar nicht möglich, für die vom Adressverlag erworbenen Daten einen **anderen**, vom Gesetz abweichenden **Zweck** zu definieren, sodass die Datenverarbeitung rechtswidrig war.

Verstößt eine Verarbeitung gegen die in Art 5 DSGVO festgelegten Grundsätze, können die Aufsichtsbehörden nach Art 57 und 58 DSGVO tätig werden. Ein **Verbot nach Art 58 Abs 2 lit f DSGVO** ist eine **besonders einschneidende Maßnahme**, die als **ultima ratio** in Betracht kommt, nachdem weniger eingriffsintensive Alternativen geprüft wurden. Eine Aufsichtsbehörde ist nicht verpflichtet, eine Abhilfemaßnahme zu ergreifen, wenn ein solches Einschreiten nicht geeignet, erforderlich oder verhältnismäßig ist, um der festgestellten Unzulänglichkeit abzuweichen und die umfassende Einhaltung dieser Verordnung zu gewährleisten.

BVwG 30.06.2025, W137 2253891-1

#### **FMA, Behörde, Empfänger, Auskunft**

- Die **Finanzmarktaufsicht (FMA)** führte wegen Verdachtsmomenten betreffend hoher Zahlungseingänge auf dem Privatkonto eines Geschäftsführers eine **Vor-Ort-Prüfung** bei einer Bank durch. Da der Geschäftsführer den Verdacht hegte, die Bank habe Unterlagen zu seinen Kontenbewegungen an die FMA weitergegeben, ersuchte er die Bank um Auskunft. Die Bank erteilte eine Auskunft, erwähnte die Datenübermittlung an die FMA jedoch nicht. Der Geschäftsführer hielt die Auskunft für unvollständig, insbesondere weil er von einer Kompetenzüberschreitung der FMA ausging. Er brachte Datenschutzbeschwerde bei der DSB ein. Die DSB wies diese ab. Dagegen erhob der Geschäftsführer (erfolglose) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Durch das Recht auf **Auskunft** soll eine Betroffene in die



Lage versetzt werden, sich der **Verarbeitung** ihrer personenbezogenen Daten **bewusst** zu werden und deren **Rechtmäßigkeit** überprüfen zu können. Die für die Betroffene bestimmte Auskunft hat präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache und vollständig zu sein.

Um vollständig zu sein, hat eine Auskunft auch die **Empfänger** und **Kategorien von Empfängern** auszuweisen. Von den Empfängern sind jedoch **Behörden** nach Art 4 Z 9 DSGVO ausgenommen, denen vom Verantwortlichen im Rahmen einer **rechtlichen Verpflichtung** für die Ausübung eines **offiziellen Auftrags** Daten offengelegt werden.

Ebenso **entfallen** für solche Datenübermittlungen die **Informationspflichten** des Verantwortlichen gemäß Art 13 und 14 DSGVO. Eine Erfassung im **Verzeichnis von Verarbeitungstätigkeiten** ist auch nicht erforderlich.

Die **FMA** ist eine zur Durchführung der Bankenaufsicht, der Versicherungsaufsicht, der Wertpapieraufsicht und der Pensionskassenaufsicht eingerichtete **Anstalt des öffentlichen Rechts** mit eigener Rechtspersönlichkeit und konkreter **Untersuchungsbefugnis**. Die FMA darf zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung jederzeit Vor-Ort-Prüfungen der verpflichteten Kredit- und Finanzinstitute durchführen. Sie fällt dann unter die **Ausnahme** des Art 4 Z 9 2 Satz DSGVO und ist **nicht Empfänger** iSd DSGVO. Die Bank muss Datenübermittlungen an die FMA daher nicht beauskunften.

Ob die FMA ihre Kompetenzen überschritten hat, ist **kein Gegenstand** des Verfahrens zur Prüfung der Vollständigkeit einer Auskunft. Ein Verantwortlicher muss keine juristischen Erwägungen anstellen, ob eine **Kompetenzüberschreitung** eines Nicht-Empfängers vorliegt, um diesen dann zu beauskunften.

BVwG 01.07.2025, W256 2252595-1

### **Rechtsanspruch, strafrechtliche Verurteilung, berechtigtes Interesse**

- Eine Tierhalterin übergab einer Frau eine Katze zur Betreuung. Später nahm die Tierhalterin die Katze der Katzenbetreuerin im Zuge eines Exekutionsverfahrens wieder ab. Im Zuge dieses Konflikts kam es zu weiteren Verfahren zwischen den beiden Frauen. Die Katzenbetreuerin wurde in einer Facebook-Gruppe mit Personen aktiv, die ebenfalls Schwierigkeiten mit der Tierhalterin hatten. Ein Gruppenmitglied leitete der Katzenbetreuerin ein nicht anonymisiertes strafgerichtliches Urteil weiter, mit dem die Tierhalterin wegen schwerer

Körperverletzung und teils versuchten Hausfriedensbruchs verurteilt worden war.

Später erhob die Tierhalterin Privatanklage wegen übler Nachrede (§ 111 StGB) gegen die Katzenbetreuerin. Zur Verteidigung in diesem Privatanklageverfahren leitete die Katzenbetreuerin das erhaltene Strafurteil per E-Mail an ihre Rechtsanwältin weiter. Die Rechtsanwältin der Katzenbetreuerin übermittelte das Urteil mittels Web-ERV an das Bezirksgericht, um es im Privatanklageverfahren als Beweismittel vorzulegen. Die Tierhalterin sah dadurch ihr Geheimhaltungsrecht verletzt.

Die DSB wies die Datenschutzbeschwerde ab. Daraufhin erhob die Tierhalterin (teilweise erfolgreich) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Gemäß **Art 10 DSGVO** dürfen **personenbezogene Daten** über **strafrechtliche Verurteilungen** und **Straftaten** nur unter behördlicher Aufsicht verarbeitet werden oder wenn dies durch Rechtsvorschriften erlaubt ist und geeignete Garantien für die Rechte und Freiheiten der Betroffenen vorgesehen sind. Nach **§ 4 Abs 3 DSG** ist die Verarbeitung solcher Daten zulässig, wenn eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung besteht (Z 1) oder wenn dies zur Erfüllung gesetzlicher Sorgfaltspflichten (zB in den Berufsregeln der Rechtsanwälte) oder zur Wahrung berechtigter Interessen erforderlich ist und die Interessen der Betroffenen gewahrt bleiben (Z 2).

Die **Rechtsverteidigung** eines Verantwortlichen in einem Strafverfahren ist ein **berechtigtes Interesse**. Die Datenverarbeitung diene diesem Interesse. **§ 111 Abs 3 StGB sieht Strafflosigkeit** vor, wenn der **Wahrheitsbeweis** oder der **Beweis des guten Glaubens** gelingt. Daher konnte die Vorlage des Strafurteils zur Rechtsverteidigung erforderlich sein. Eine **Anonymisierung** hätte den Bezug zur Tierhalterin verdeckt.

Das **Geheimhaltungsinteresse** bei strafrechtlichen Verurteilungen ist wegen des **Stigmatisierungspotenzials** hoch. Ebenso gewichtig ist das Interesse an einer **effektiven Rechtsverteidigung**. Die Tierhalterin musste damit rechnen, dass Daten zu ihrer Person verarbeitet werden, insbesondere durch Vorlage eines Urteils. Die Übermittlung an die Rechtsanwältin gewährleistete die Wahrung berechtigter Interessen. Die Katzenbetreuerin erhielt das Urteil jedoch, um sich über **schlechte Erfahrungen** mit der Tierhalterin auszutauschen. Solche Erfahrungen begründen kein berechtigtes Interesse an der Übermittlung oder Verarbeitung solcher Informationen.

### **Geldbuße, Videoüberwachung, Rollenverteilung**

- Die DSB leitete aufgrund einer Anzeige durch eine Marktgemeinde ein Strafverfahren gegen den Eigentümer eines Gebäudes ein, der eine Kamera an seinem Haus angebracht hatte, die auch den öffentlichen Raum überwachte. Der Eigentümer hat das Gebäude an eine GmbH vermietet, deren Geschäftsführer er selbst war. Die Kamera nahm Bild- und Tonaufnahmen auf, sobald sie eine Bewegung registrierte. Die Aufnahmen waren über eine App auf einem Firmenhandy abrufbar. Nicht festgestellt werden konnte, wie lange die Daten auf der App gespeichert wurden und ob diese gelöscht wurden. Die Videoüberwachung wurde lediglich mit einer Beschilderung an der Hausfront gekennzeichnet. Die DSB verhängte eine Geldstrafe iHv EUR 1.000, weil die Verarbeitung auf keinen Erlaubnistatbestand nach Art 6 Abs 1 DSGVO gestützt werden konnte und der Eigentümer seiner Informationspflicht nach Art 12 und 13 DSGVO nicht nachkam. Dagegen erhob der Eigentümer Bescheidbeschwerde an das BVwG und gab an, die Kamera zum Schutz des Gebäudes und einer E-Ladestation installiert zu haben, nachdem es in der Vergangenheit zu Beschädigungen und einem Einbruch gekommen sei. Das BVwG wies die Bescheidbeschwerde ab und schrieb dem Geschäftsführer die Zahlung von zusätzlichen EUR 200 als **Beitrag zu den Verfahrenskosten** vor.

Das BVwG hat erwogen: Der Betrieb der **Videokamera** ist zweifelsfrei eine Verarbeitung personenbezogener Daten. Verantwortlicher ist, wer über die Zwecke und Mittel der Datenverarbeitung entscheidet. Maßgeblich dafür ist die faktische Entscheidungsgewalt, nicht die formale Eigentümerstellung oder die tatsächliche Durchführung der Überwachung. Der Eigentümer nahm aus Eigeninteresse Einfluss auf die Datenverarbeitung und bestimmte damit die Zwecke und Mittel der Überwachung und ist daher Verantwortlicher.

Eine Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn ein Erlaubnistatbestand des Art 6 Abs 1 DSGVO erfüllt ist, wobei für diese Videoüberwachung nur die Wahrung berechtigter Interessen in Betracht kommt. Der **Schutz des Eigentums** ist grundsätzlich ein **berechtigtes Interesse**. Die Videoüberwachung ist aber auf das **absolut notwendige Maß** zu beschränken. Die Kamera erfasste auch den öffentlichen Raum und überschreitet damit das erforderliche Maß. Der Schutz wäre auch bei einem geringeren Aufnahmebereich der Videokamera gewährleistet gewesen. Die Datenverarbeitung war daher nicht erforderlich und somit rechtswidrig.

Gemäß Art 12 und 13 DSGVO muss für Betroffene erkennbar sein, dass personenbezogene Daten verarbeitet werden, welche Daten verarbeitet werden, für welche Zwecke sie verarbeitet werden und durch wen sie verarbeitet werden. Diese **Informationen** müssen präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache erteilt werden. Erfolgt diese Information nicht, kann der Betroffene seine Betroffenenrechte nach Art 15 ff DSGVO nicht geltend machen.

Bei Videokameras kann etwa in einem ersten Schritt durch eine **Beschilderung** auf die Datenverarbeitung hingewiesen werden. Notwendige weitere Informationen sind in einem **zweiten Schritt** mit anderen Mitteln zur Verfügung zu stellen. Ein bloßes Piktogramm ohne weitere Angaben zum Verantwortlichen, zur Speicherdauer und zum Zweck genügt nicht. Der Eigentümer hat damit gegen den Transparenzgrundsatz und gegen die Informationspflichten verstoßen. Der Eigentümer handelte **fahrlässig**. Er hätte **erkennen müssen**, dass die Verarbeitung nicht im Einklang mit der DSGVO stand. Die Geldstrafe ist daher angemessen und verhältnismäßig.

### **Exzess, Missbrauchsabsicht**

- Der Betroffene verlangte Auskunft von einem Psychotherapeuten darüber, welche seiner personenbezogenen Daten verarbeitet werden. Nachdem der Psychotherapeut in seiner E-Mail ausführte, keine Daten mehr zu seiner Person vorliegend zu haben, brachte der Betroffene eine Datenschutzbeschwerde bei der DSB ein. Die DSB wies die Datenschutzbeschwerde wegen Exzess gemäß Art 57 Abs 4 DSGVO ab, weil der Betroffene 86 weitere Datenschutzbeschwerden eingebracht habe, in denen er jeweils verschiedenen Verantwortlichen eine unrichtige Verarbeitung seiner Daten und der Daten seines Sohnes vorwarf. Dagegen richtete der Betroffene eine erfolgreiche Bescheidbeschwerde an das BVwG. Im Erkenntnis führte das BVwG aus, dass der Betroffene in seiner Datenschutzbeschwerde nicht die unrichtige Verarbeitung seiner Daten, sondern die Verletzung seines Auskunftsrechts geltend mache, weshalb kein Fall des Art 57 Abs 4 DSGVO vorliege. Infolge der von der DSB erhobenen Amtsrevision hob der VwGH – nach der Entscheidung des EuGH in der Sache [C-416/23, Österreichische Datenschutzbehörde \(Demandes excessives\)](#) – das Erkenntnis des BVwG aufgrund **sekundärer Feststellungsmängel** zur Missbrauchsabsicht auf. Das Verfahren wurde im zweiten Rechtsgang vor dem BVwG fortgesetzt.

Das BVwG hat erwogen: Bei offenkundig unbegründeten oder exzessiven Datenschutzbeschwerden darf die DSB eine Gebühr verlangen oder sich weigern, tätig zu werden (Art 57 Abs 4 DSGVO). Die Aufsichtsbehörde trägt die **Beweislast**. Datenschutzbeschwerden dürfen nicht allein aufgrund **ihrer Zahl** als exzessiv eingestuft werden. Die DSB muss das Vorliegen einer Missbrauchsabsicht des Betroffenen nachweisen. Eine Missbrauchsabsicht liegt vor, wenn Datenschutzbeschwerden eingereicht werden, ohne dass dies objektiv erforderlich ist, um die Rechte aus der DSGVO zu schützen.

Die DSB muss alle relevanten Umstände jedes **Einzelfalls** berücksichtigen. Eine übermäßige Inanspruchnahme der DSB durch zahlreiche Datenschutzbeschwerden kann ein Indiz für Exzess sein, wenn die Datenschutzbeschwerden nicht objektiv durch Erwägungen gerechtfertigt sind, die sich auf den Schutz der Rechte beziehen.

Da die DSB die Behandlung der Datenschutzbeschwerde aufgrund von Art 57 Abs 4 DSGVO abgelehnt hat, behandelte sie die Datenschutzbeschwerde inhaltlich nicht. "Sache" des Verfahrens vor dem BVwG ist daher nur die Frage der **Rechtmäßigkeit** der Ablehnung der inhaltlichen Behandlung. Der Betroffene legte glaubwürdig dar, mit seiner Datenschutzbeschwerde das Ziel verfolgt zu haben, eine Auskunft über die Verarbeitung seiner Daten zu erhalten. Die Datenschutzbeschwerde bezog sich konkret auf den Psychotherapeuten. Der Psychotherapeut hat vor dem Auskunftersuchen personenbezogene Daten des Betroffenen verarbeitet. Es liegen keine Anhaltspunkte vor, dass der Betroffene **andere Zwecke** als den Schutz seiner Rechte aus der DSGVO verfolgte. Der Bescheidbeschwerde war daher erneut Folge zu geben und der DSB war aufzutragen, das Verfahren unter Abstandnahme von der Ablehnung der Datenschutzbeschwerde wegen Exzessivität fortzusetzen.

Aus der weiteren Rechtsprechung des BVwG:

- Die **ORF-Beitrags Service GmbH (OBS)** ist berechtigt, **Rückstandsausweise** auszustellen. Ein Rückstandsausweis ist ein **Exekutionstitel**. Die OBS darf zur **Eintreibung des ORF-Beitrags** die Information, dass ein Rückstandsausweis ausgestellt wurde, an ein **Inkassobüro** übermitteln ([BVwG 03.07.2025, W211 2301099-1](#)).

### Rechtsprechung des BFG

Aus der Rechtsprechung des BFG:

- Gemäß § 57 Abs 2 GSpG ist eine **Glücksspielabgabe** für **Online-Glücksspiel** zu entrichten, an dem die Teilnahme vom

Inland aus erfolgt. Das Tatbestandsmerkmal "**Teilnahme vom Inland aus**" kann aus eigener Wahrnehmung des Glücksspielanbieters ohne entsprechende Ermittlungen nicht erhoben werden. Die Teilnahme vom Inland aus ist daher anhand von Indizien wie "**inländische Registrierungsadresse**", "**inländische IP-Adresse**" oder "**Wohnsitzadresse**" zu beurteilen. Die Kumulation der – gleichwertigen – Indizien der Registrierungsadresse und der IP-Adresse wird nicht gefordert. Sowohl die Festsetzung der **Wettgebühr** als auch der **Glücksspielabgabe** kann auch alleine auf das Indiz "Wohnsitzadresse" gestützt werden ([BFG 02.07.2025, RV/7104521/2020](#)).

- Die Verarbeitung personenbezogener Daten durch die Abgabenbehörde und durch das BFG ist für **Zwecke der Abgabenerhebung** gemäß **§ 48d Abs 1 BAO** zulässig. **Besondere Kategorien personenbezogener Daten** dürfen für die Abgabenerhebung verarbeitet werden, wenn ein **erhebliches öffentliches Interesse** vorliegt (**§ 48d Abs 2 BAO**). Die Verarbeitung von **Gesundheitsdaten** ist rechtmäßig. Zudem unterliegen die Bediensteten des Finanzamts wie auch des Finanzgerichts der **abgabenrechtlichen Geheimhaltungspflicht**. Ein Rechtsanspruch auf den Abzug **außergewöhnlicher Belastungen** setzt den **Nachweis** dieser außergewöhnlichen Belastung durch die Vorlage entsprechender Unterlagen voraus. Eine bloße Glaubhaftmachung genügt nicht ([BFG 08.07.2025, RV/4100275/2022](#); [08.07.2025, RV/4100327/2023](#)).

### EU-Rechtsakte

- Am **29.08.2025** wurde die "**Durchführungsverordnung (EU) 2025/1328 der Kommission vom 30. Juni 2025 zur Durchführung der Richtlinie (EU) 2024/1275 des Europäischen Parlaments und des Rates durch die Erstellung gemeinsamer Vorlagen für die Übermittlung von Informationen aus den nationalen Datenbanken über die Gesamtennergieeffizienz von Gebäuden an die Beobachtungsstelle für den EU-Gebäudebestand**", [ABI L 2025/1328](#), kundgemacht. In dieser Durchführungsverordnung werden **gemeinsame Vorlagen** für die **Übermittlung von Informationen** aus den **nationalen Datenbanken** für die **Gesamtennergieeffizienz von Gebäuden** an die Beobachtungsstelle für den EU-Gebäudebestand festgelegt. Die zu übermittelnden Informationen sind zu anonymisieren, sodass **keine personenbezogenen Daten** übermittelt werden. **Anhang II** der Durchführungsverordnung enthält Formeln für die **Anonymisierung**.

## Nationale Rechtsakte

- Am **01.09.2025** sind das neue **Grundrecht auf Informationszugang** sowie das **Informationsfreiheitsgesetz (IFG)** in Kraft getreten. Ebenso am **01.09.2025** ist die **Verfügbarkeit des Informationsregisters** durch Verordnung des Bundeskanzlers kundgemacht worden, [BGBl II 2025/52](#). Die Informationen von allgemeinem Interesse sind sohin spätestens ab dem **01.12.2025** auf [www.data.gv.at](http://www.data.gv.at) bereitzustellen.
- Am **26.08.2025** wurde die **Daten-Governance-Benennungsverordnung (DGBenV)**, [BGBl II 2025/186](#), kundgemacht. Mit dieser Verordnung wird die **Bundesanstalt Statistik Austria** als **zuständige Stelle** für den Zugang zur Weiterverwendung von geschützten Daten in bestimmten Datenkategorien gemäß **§ 5 Abs 1 DZG** festgelegt.
- Am **29.08.2025** wurde die fünfzehnte Änderung der **FinanzOnline-Verordnung**, [BGBl II 2025/190](#), kundgemacht. Mit dieser Verordnung werden Teilnehmer, die zur Einreichung der **Umsatzsteuererklärung** verpflichtet sind, auch zur **elektronischen Zustellung verpflichtet**.
- Am **25.08.2025** wurde die **Oö. Informationsfreiheits-Anpassungsverordnung-Agrar**, [LGBI 2025/68](#), kundgemacht. Mit dieser Verordnung wird festgelegt, dass die Namen von Berichtigungsantragstellern und Einspruchswerbern **geheim zu halten** sind.
- Am **27.08.2025** wurde das **Steiermärkische Informationsfreiheitsanpassungsgesetz 2025**, [LGBI 2025/68](#), kundgemacht. Mit diesem Sammelgesetz wurden knapp **30 steiermärkische Gesetze** dem neuen **Grundrecht auf Informationszugang** angepasst.

# Datenschutzmonitor. 36/2025 vom 10.09.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH 04.09.2025, C-413/23 P, *EDSB/SRB* (Personenbezug, Pseudonymisierung, Empfänger, Einwilligung)

EuGH 04.09.2025, C-655/23, *Quirin Privatbank* (Unterlassungsanspruch, immaterieller Schaden, Ausgleichsfunktion)

EuGH SA 04.09.2025, C-414/24, *Datenschutzbehörde (Articulation des recours)* (Doppelgleichheit, Aufsichtsbehörde, Gericht)

EuGH SA 04.09.2025, C-199/24, *Legal Newsdesk Sweden* (Medienfreiheit, Meinungsfreiheit, Strafurteil)

EuGH SA 04.09.2025, C-312/24, *Darashev* (Personalakt, Dateisystem, strafrechtliche Ermittlungen, DSRL-PJ)

EuG 03.09.2025, T-553/23, *Latombe* (EU-US Data Privacy Framework, DPRC, US-Nachrichtendienste)

- **Rechtsprechung des VwGH**

VwGH 01.08.2025, Ra 2023/04/0058 (lebenswichtige Interessen)

VwGH 06.08.2025, Ra 2025/04/0163 (Einwilligung, Widerruf)

VwGH 06.08.2025, Ra 2024/04/0309 (berechtigte Interessen, Einzelfallprüfung)

- **Rechtsprechung der Justiz**

OGH 13.08.2025, 6Ob173/24w (Handelsregister, Offenlegungspflicht, juristische Person)

OLG Wien 28.07.2025, 30Bs196/25f (Beschlagnahme, Datenträger, Daten)

- **Rechtsprechung des BVwG**

BVwG 09.07.2025, W298 2309078-1 (berechtigtes Interesse, Warnliste der Kreditinstitute, Kleinkreditevidenz)

- **Rechtsprechung der DSB**

DSB 12.06.2025, 2024-0.490.294 (Homeoffice, Zutrittssystem, Betriebsrat)

DSB 07.08.2025, 2025-0.626.844 (Auskunft, Fernzugriff, Format, Erleichterungsgebot, Marktortprinzip)

- **Nationale Rechtsvorschriften**

Inkrafttreten des Grundrechts auf Informationszugang und Verfügbarkeit des Informationsregisters

Vorarlberg: Gesetz über begleitende Regelungen zur Informationsfreiheit und landesspezifische Regelungen zum Datenschutz

Vorarlberg: Verfassungsgesetz über eine Änderung der Landesverfassung (Parlamentarisches Datenschutzkomitee)

## To the Point:

### Rechtsprechung des EuGH

EuGH 04.09.2025, C-413/23 P, EDSB/SRB

#### **Personenbezug, Pseudonymisierung, Empfänger, Einwilligung**

- Im Rahmen des Abwicklungsverfahrens einer Bank veröffentlichte der **Einheitliche Abwicklungsausschuss (SRB)** – die für die Abwicklung insolvenzbedrohter Finanzinstitute zuständige Behörde der Europäischen Bankenunion – eine vorläufige Entscheidung über die Gewährung einer Entschädigung für betroffene Aktionäre oder Gläubiger. Er leitete ein Anhörungsverfahren ein, bei dem Betroffene eine Stellungnahme zur vorläufigen Entscheidung einreichen konnten. Die Stellungnahmen wurden vom SRB aggregiert, gefiltert und kategorisiert und dann an Deloitte zur Auswertung übermittelt. Die Inhalte der Stellungnahmen waren von den Identifikationsdaten der Betroffenen getrennt und mit einem alphanumerischen Code gekennzeichnet, sodass nur der SRB die Daten verknüpfen konnte.

Fünf Bankkunden brachten Beschwerden beim EDSB ein, weil der SRB nicht darüber informiert hatte, dass ihre Daten an Deloitte weitergegeben werden. Der EDSB beschloss, dass die an Deloitte übermittelten Daten **pseudonymisierte Daten** waren und stellte einen Verstoß gegen die Informationspflicht fest.

Der SRB erhob Klage an das **EuG**. Dieses hob den Beschluss des EDSB auf, weil dieser Inhalt, Zweck oder Auswirkungen der an Deloitte übermittelten Informationen nicht geprüft habe. Mangels einer solchen Prüfung dürfe der EDSB nicht davon ausgehen, dass sich die an Deloitte übermittelten Informationen auf eine natürliche Person beziehen. Gegen diese Entscheidung richtet sich das Rechtsmittel des EDSB.

Der EuGH hat erwogen: **Personenbezogen** ist eine **Information** über eine identifizierte oder identifizierbare natürliche Person, wenn sie aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer identifizierbaren Person verknüpft ist. **Persönliche Meinungen** oder **Sichtweisen** sind als **Ausdruck der Gedanken** einer Person zwangsläufig eng mit dieser Person verknüpft und somit personenbezogene Daten.

Die Anwendung der DSGVO setzt eine Prüfung voraus, ob die in Rede stehende Person identifiziert oder identifizierbar ist. **Pseudonymisierung** kann sich auf die Personenbezogenheit von Daten auswirken. Technische und organisatorische Maßnahmen können bewirken, dass personenbezogene Daten für einen Verantwortlichen, der nicht in der Lage ist, diese Maßnahmen

aufzuheben, **nicht personenbezogen** sind. Sie können aber wieder zu personenbezogenen Daten werden, wenn der Verantwortliche sie anderen Personen überlässt, die über Mittel zur Identifizierung der Betroffenen verfügen. Der Begriff "**personenbezogene Daten**" ist weit auszulegen, er ist jedoch **nicht unbegrenzt**. Der Betroffene muss **identifiziert** oder **identifizierbar** sein.

Die Information über **potenzielle Empfänger** personenbezogener Daten ist zum Zeitpunkt des Erhebens der Daten beim Betroffenen zu erteilen. Beruht die Datenverarbeitung auf einer **Einwilligung**, hängt die Gültigkeit dieser Einwilligung davon ab, ob dem Betroffenen zuvor die Information über alle Umstände der Datenverarbeitung erteilt wurde.

Die Pflicht zur Information über potenzielle Empfänger zielt darauf ab, dem Betroffenen zu ermöglichen, in **voller Kenntnis der Sachlage zu entscheiden**, ob er seine Daten zur Verfügung stellt oder dies verweigert. Die Informationspflicht besteht im **Rechtsverhältnis** zwischen dem Betroffenen und dem Verantwortlichen. Die **Identifizierbarkeit des Betroffenen** ist daher aus der **Sicht des Verantwortlichen** zu beurteilen. **Anm: Zu begrüßen ist die Klarstellung des EuGH, dass für den Personenbezug die Identifizierbarkeit der Person eine zwingende Tatbestandsvoraussetzung ist. Die Zusammenfassung der Schlussanträge des Generalanwalts kann im Schönerr Datenschutzmonitor 6/2025 vom 12.02.2025 nachgelesen werden.**

EuGH 04.09.2025, C-655/23, Quirin Privatbank

#### **Unterlassungsanspruch, immaterieller Schaden, Ausgleichsfunktion**

- Eine Bank hatte in einem Bewerbungsverfahren versehentlich personenbezogene Daten eines Bewerbers an einen Dritten weitergeleitet. Der Bewerber verlangte daraufhin von der Bank, eine Wiederholung der unrechtmäßigen Offenlegung zu unterlassen, und begehrte Ersatz für einen immateriellen Schaden, der sich insbesondere in negativen Gefühlen wie Sorge und Ärger äußerte.

Das vorliegende Gericht wollte ua wissen, ob (i) negative Gefühle als immaterieller Schaden gelten, (ii) die DSGVO einen Unterlassungsanspruch vorsieht und (iii) der Grad des Verschuldens bei der Bemessung des Schadenersatzes zu berücksichtigen ist.

Der EuGH hat erwogen: Die DSGVO sieht keinen unmittelbaren unionsrechtlichen **Unterlassungsanspruch** künftiger unrechtmäßiger Datenverarbeitung vor, wenn die Betroffene keine Löschung ihrer Daten verlangt. Den **Mitgliedstaaten** steht es jedoch frei, einen solchen präventiven

Unterlassungsanspruch nach nationalem Recht vorzusehen.

Der Begriff des "**immateriellen Schadens**" in Art 82 Abs 1 DSGVO ist weit auszulegen. Er umfasst auch **negative Gefühle** wie **Sorge** oder **Ärger**, die durch eine unbefugte Offenlegung personenbezogener Daten an Dritte ausgelöst werden, etwa durch den Verlust der Kontrolle über die Daten, deren mögliche missbräuchliche Verwendung oder eine Rufschädigung. Voraussetzung ist, dass die Betroffene nachweist, dass diese Gefühle und ihre negativen Folgen tatsächlich auf den DSGVO-Verstoß zurückzuführen sind. Eine Erheblichkeitschwelle ("**Bagatellgrenze**") für den Schaden besteht nicht.

Bei der Bemessung des Schadenersatzes ist der **Grad des Verschuldens** des Verantwortlichen nicht zu berücksichtigen. Ebenso irrelevant sind Haltung oder Beweggründe des Verantwortlichen. Der Schadenersatz nach Art 82 DSGVO dient ausschließlich dem **vollständigen Ausgleich** des konkret entstandenen Schadens und hat keine Straf- oder Abschreckungsfunktion. Eine etwaige Unterlassungsanordnung kann nicht anspruchsmindernd auf den Schadenersatz angerechnet werden.

EuGH SA 04.09.2025, C-414/24, *Datenschutzbehörde (Articulation des recours)*

### **Doppelgleisigkeit, Aufsichtsbehörde, Gericht**

- Ein Arzt brachte 2017 vor Inkrafttreten der DSGVO bei Gericht eine Klage auf Löschung seiner personenbezogenen Daten und Unterlassung einer erneuten Verarbeitung gegen den Betreiber einer Ärztebewertungsplattform ein. Nach Inkrafttreten der DSGVO stellte der Arzt während des weiterhin laufenden Zivilverfahrens ein erfolgloses Löschungsersuchen an den Betreiber. Daraufhin brachte der Arzt eine Datenschutzbeschwerde bei der DSB ein. Die DSB wies die Datenschutzbeschwerde wegen des schon anhängigen zivilgerichtlichen Verfahrens zurück. Dagegen brachte der Arzt Beschwerde an das BVwG ein. Das BVwG bejahte grundsätzlich die Entscheidungskompetenz der DSB, wies die Datenschutzbeschwerde jedoch wegen Fristversäumnis (Präklusion) gemäß § 24 Abs 4 DSG zurück. Daraufhin wandten sich der Arzt und die DSB an den VwGH. Der VwGH legte dem EuGH die Frage zur Vorabentscheidung vor, ob die DSB eine Datenschutzbeschwerde nach Art 77 DSGVO zurückweisen darf, wenn bereits ein Gerichtsverfahren nach Art 79 DSGVO zum selben Sachverhalt anhängig ist.

Der Generalanwalt hat erwogen: Jede Betroffene hat gemäß Art 77 Abs 1 DSGVO ein Recht auf eine **Beschwerde** an eine

**Aufsichtsbehörde**, unabhängig davon, ob es andere verwaltungsrechtliche oder gerichtliche Rechtsbehelfe gibt. Zusätzlich hat jede Betroffene nach Art 79 DSGVO ein **Recht** auf einen **wirksamen gerichtlichen Rechtsbehelf**. Betroffenen stehen gegen Verstöße der DSGVO mehrere nebeneinander bestehende Rechtsbehelfe zu. Das **Ziel** ist, jeder Person, die sich in ihren Rechten nach der DSGVO verletzt sieht, einen **wirksamen Rechtsbehelf** zu garantieren. Es obliegt den Mitgliedstaaten, im Rahmen ihrer **Verfahrensautonomie** Instrumente einzuführen, die einander widersprechende Entscheidungen in Bezug auf dieselbe Verarbeitung verhindern. Diese Instrumente müssen dem Grundsatz der **Effektivität** entsprechen und die Ausübung der Rechte nicht praktisch unmöglich machen oder übermäßig erschweren.

Auch wenn schon ein **gerichtlicher Rechtsbehelf** in Anspruch genommen wurde, ist unklar, ob tatsächlich eine Entscheidung in der Sache ergeht. Der Rechtsbehelf könnte aus verfahrensrechtlichen Gründen zurückgewiesen werden.

Grundsätzlich kann eine Betroffene zwar auch nach **Zurückweisung der Klage** erneut eine Beschwerde bei der Aufsichtsbehörde einlegen, diese kann aber unmöglich sein, wenn das nationale Recht bestimmte Fristen für die Geltendmachung vorsieht. In solchen Fällen hätten die Betroffenen **keinen wirksamen** Rechtsschutz.

Dies widerspricht auch der **behördlichen Sorgfaltspflicht**, wonach eine Beschwerde bei der Behörde mit aller gebotenen Sorgfalt bearbeitet werden soll. Im Rahmen der Beschwerdeprüfung hat die Behörde eine bereits ergangene Entscheidung zu beachten, mit der das Verfahren schon rechtskräftig abgeschlossen wurde. Falls bereits ein weiteres Verfahren anhängig ist, sollte sie ihre Prüfung aussetzen.

Eine Aufsichtsbehörde darf eine Beschwerde trotz bereits erhobenen gerichtlichen Rechtsbehelfs **nicht** zurückweisen, solange das gerichtliche Verfahren noch **nicht rechtskräftig** abgeschlossen und noch anfechtbar ist.

EuGH SA 04.09.2025, C-199/24, *Legal Newsdesk Sweden*

### **Medienfreiheit, Meinungsfreiheit, Strafurteil**

- Eine Datenbankbetreiberin stellte über eine Plattform personenbezogene Daten von Personen bereit, die in ein Zivil- oder Strafverfahren vor Gerichten verwickelt waren. Dafür erhielt die Plattform von der zuständigen Medienbehörde ein Publikationszertifikat, das verfassungsrechtlichen Schutz gewährt.

Obwohl die Daten des Betroffenen bereits aus dem öffentlichen Strafregister gelöscht waren, blieben sie auf der Plattform abrufbar. Seinem Löschbegehren wurde erst verzögert nach einer routinemäßigen Überprüfung nachgekommen. Daraufhin klagte der Betroffene auf Schadenersatz. Die Datenbankbetreiberin berief sich auf das Publikationszertifikat und argumentierte, die DSGVO finde keine Anwendung, weil der Datenschutz durch nationale Mediengesetze geregelt sei. Das vorlegende Gericht legte dem EuGH mehrere Fragen zur **Meinungs- und Medienfreiheit** vor.

Der Generalanwalt hat erwogen: Die Bestimmung des Art 85 Abs 1 DSGVO verpflichtet die Mitgliedstaaten, durch Gesetz einen Ausgleich zwischen dem Recht auf Datenschutz und dem **Recht auf Meinungs- und Informationsfreiheit** herzustellen. Gemäß Art 85 Abs 2 DSGVO dürfen Mitgliedstaaten für bestimmte Zwecke Ausnahmen für bestimmte Kapitel von der DSGVO vorsehen. Wäre dies auch über Abs 1 dieser Bestimmung möglich, würde dies den vom EU-Parlament abgelehnten Ansatz einer umfassenden Öffnung zugunsten der **Meinungsfreiheit** nachträglich einführen. Nach Art 85 Abs 1 DSGVO können die Mitgliedstaaten daher nicht pauschal ganze Kapitel der DSGVO für unanwendbar erklären, sondern allenfalls in engen Grenzen bestimmte Rechte einschränken.

Weder Art 85 Abs 1 noch Abs 2 DSGVO erlauben es, die Rechte der Betroffenen nach Kapitel VIII (**Rechtsbehelfe, Haftung** und Sanktionen) einzuschränken. Eine nationale Regelung, die Betroffenen lediglich Strafanzeige oder Klage wegen Verleumdung ermöglicht, widerspricht der DSGVO und ist daher unzulässig.

**Journalistische Zwecke** liegen vor, wenn sie zum Zweck haben, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten. Die **entgeltliche Bereitstellung** von **Strafurteilen** im Internet ohne Bearbeitung oder redaktionelle Tätigkeiten ist keine Verarbeitung zu journalistischen Zwecken.

EuGH SA 04.09.2025, C-312/24, *Darashev*

### **Personalakt, Dateisystem, strafrechtliche Ermittlungen, DSRL-PJ**

- Ein Innenminister speicherte in Personalakten Informationen über strafrechtliche Ermittlungen gegen seine Bediensteten. Ein Polizeibeamter wurde wegen Raubes beschuldigt und festgenommen, nach 24 Stunden jedoch wieder freigelassen. Das Verfahren wurde eingestellt. Nachdem der Polizeibeamte sich erfolglos an mehreren Auswahlverfahren für Beförderungen beteiligte, klagte er den Innenminister, weil dieser trotz Einstellung seines

Ermittlungsverfahrens weiterhin Daten über den Status des Polizeibeamten als Verdächtigen in seiner Personalakte speicherte. Er beantragte die Löschung dieser Daten und machte geltend, dass ihm wegen dieser Speicherung eine Beförderung verweigert wurde.

Das vorlegende Gericht fragte den EuGH im Wesentlichen, ob (i) die Speicherung von Daten über den Status eines Bediensteten als Verdächtiger in einem Strafverfahren in dessen Personalakte der DSGVO unterliegt, wenn diese Daten zuvor von einer zuständigen Organisationseinheit der Behörde im Sinne der RL 2016/680 (**DSRL-PJ**) erhoben wurden, und (ii) die Speicherung von Daten über eingestellte Strafverfahren in der Personalakte eines Polizeibeamten allein wegen der Art seiner dienstlichen Aufgaben als rechtmäßig gelten kann, sofern das nationale Recht die Behörde hierzu verpflichtet.

Der Generalanwalt hat erwogen: Die Speicherung von Daten über den Status als Verdächtiger in einer Personalakte ist eine Verarbeitung personenbezogener Daten. Bei der Personalakte handelt es sich um eine strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist und somit ein **Dateisystem** ist.

Die DSGVO gilt jedoch für die Speicherung personenbezogener Daten in Personalakten nicht, wenn die Speicherung zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten erfolgt. Denn unter dieser Voraussetzung gelangt die **DSRL-PJ** zur Anwendung, die die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zwecke der Strafverfolgung regelt. Sowohl nach der DSGVO als auch nach der DSRL-PJ ist der **Zweckbindungsgrundsatz** zu beachten. Der Minister wurde im Ermittlungsverfahren als zuständige Behörde iSd Art 3 Abs 7 der DSRL-PJ tätig. Da er jedoch keine Angaben zu den Zwecken der weiteren Verarbeitung der personenbezogenen Daten des Polizeibeamten machte und die Speicherung der Daten nicht zu den in Art 1 Abs 1 der DSRL-PJ genannten Zwecken erfolgte, ist die DSGVO anzuwenden.

Gemäß Art 6 Abs 3 DSGVO kann die **Rechtsgrundlage** für die Verarbeitung personenbezogener Daten durch Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, festgelegt werden. Für die rechtmäßige Speicherung von Daten über **eingestellte Ermittlungen** in der Personalakte eines Polizeibeamten muss eine klare und präzise Rechtsgrundlage im nationalen Recht bestehen, die für den Rechtsunterworfenen vorhersehbar ist. Die Rechtsgrundlage muss ein im **öffentlichen Interesse** liegendes Ziel



verfolgen und in einem angemessenen Verhältnis zu dem verfolgten Zweck stehen. Die Speicherung allein aufgrund der besonderen Aufgaben eines Polizeibeamten genügt nicht, um die Rechtmäßigkeit der Verarbeitung zu begründen. Die Speicherung der Daten über eingestellte Ermittlungen ohne anschließendes **Disziplinarverfahren** erfüllt nicht die Anforderungen an ein im öffentlichen Interesse liegendes Ziel. Zudem wird dadurch der Grundsatz der **Unschuldsvermutung** iSd Art 48 GRC verletzt, weil der Polizeibeamte weiterhin als verdächtig behandelt wird.

EuG 03.09.2025, T-553/23, *Latombe*

### **EU-US Data Privacy Framework, DPRC, US-Nachrichtendienste**

- Ein Betroffener erhob eine **Nichtigkeitsklage** gemäß Art 263 AEUV gegen den **Angemessenheitsbeschluss** 2023/1795 der Kommission über das Datenschutzniveau in den **USA**. Das EuG wies die Klage gegen den Angemessenheitsbeschluss, der die unionsrechtliche Grundlage des sog **EU-US Data Privacy Framework** bildet, ab.

Das EuG hat erwogen: Der EuGH hat zwei frühere Angemessenheitsbeschlüsse der Kommission betreffend die USA aufgehoben. Die USA erließen jedoch ein **Präsidentialdekret**, mit dem die Schutzmaßnahmen gegen die Tätigkeit der **US-Nachrichtendienste** verschärft und ein **Data Protection Review Court (DPRC)** geschaffen wurden.

Das DPRC ist ein **unabhängiges** und **unparteiisches Gericht**. Zur Beurteilung der Unabhängigkeit und Unparteilichkeit ist es nicht ausreichend, allein die formale Natur der Normen zu prüfen, mit denen ein Gericht eingerichtet und dessen Funktionsweise festgelegt wird. Vielmehr muss auch geprüft werden, ob diese Normen ausreichende Garantien bieten, um die Unabhängigkeit und Unparteilichkeit des Gerichts gegenüber den anderen Gewalten, insbesondere der Exekutive, zu gewährleisten. Das DPRC erfüllt diese Voraussetzungen. Die Kommission hat den **Angemessenheitsbeschluss** fortlaufend zu überwachen und kann diesen bei Änderungen des Rechtsrahmens in den USA abändern oder aufheben.

Die Sammelerhebung (**bulk interception**) personenbezogener Daten durch die US-Nachrichtendienste bedarf keiner **vorherigen Genehmigung** durch eine unabhängige Behörde. Es genügt die **nachträgliche gerichtliche Überprüfung**, der die **Signalaufklärung** der US-Nachrichtendienste unterliegt.

### **Rechtsprechung des VwGH**

Aus der Rechtsprechung des VwGH:

- Eine Beschränkung des Anspruchs auf Geheimhaltung durch einen behördlichen Eingriff bedarf dann einer gesetzlichen Grundlage, wenn ein Betroffener weder seine Zustimmung zur Verwendung seiner personenbezogenen Daten erteilt hat noch die Verwendung in seinem **lebenswichtigen Interesse** ist. Bei anderer Betrachtung könnten selbst lebenswichtige Interessen eines Betroffenen keinen Eingriff rechtfertigen, wenn keine ausdrückliche gesetzliche Grundlage vorhanden wäre. Dies würde zu einer undenkbaren Prävalierung der datenschutzrechtlichen Geheimhaltungsinteressen im Verhältnis zu lebenswichtigen Interessen führen. Der Ausnahmetatbestand der Zustimmung kann aber keine anderen Konsequenzen nach sich ziehen als jener der lebenswichtigen Interessen ([VwGH 01.08.2025, Ra 2023/04/0058](#)).
- Der **Widerruf einer Einwilligung** muss gemäß Art 7 Abs 3 DSGVO so einfach sein wie die Erteilung der Einwilligung zu einer Datenverarbeitung. Ob dieser rechtlich klaren Anordnung entsprochen wird, ist anhand der für den **Einzelfall** maßgeblichen Umstände zu prüfen. Eine im Einzelfall vorgenommene rechtliche Beurteilung kann nur dann die Zulässigkeit einer Revision begründen, wenn dies wegen einer **krassen Fehlbeurteilung** der einzelfallbezogenen Umstände durch das BVwG aus Gründen der Rechtssicherheit geboten ist ([VwGH 06.08.2025, Ra 2025/04/0163](#)).
- Bei der Beurteilung, ob eine bestimmte Datenverarbeitung im Lichte des Art 6 Abs 1 lit f DSGVO als gerechtfertigt angesehen werden kann, handelt es sich um eine **einzelfallbezogene Interessenabwägung**. Diese erfordert eine Beurteilung im Einzelfall unter Heranziehung sämtlicher maßgeblicher Umstände. Eine grundsätzliche Rechtsfrage iSd Art 133 Abs 4 B-VG liegt nur dann vor, wenn diese Einschätzung in einer die **Rechtssicherheit beeinträchtigenden** unvertretbaren Weise, also krass fehlerhaft, vorgenommen wurde. Ein Verweis auf eine "**provizierte Datenschutzverletzung**" begründet keine Rechtsfrage des Unionsrechts. Es ist Sache des nationalen Gerichts, zu beurteilen, ob die Voraussetzungen iSd Art 6 Abs 1 lit f DSGVO im Hinblick auf die Verarbeitung personenbezogener Daten erfüllt sind ([VwGH 06.08.2025, Ra 2024/04/0309](#)).

### **Rechtsprechung der Justiz**

Aus der Rechtsprechung der Justiz:

- Hinsichtlich der **Offenlegungspflichten** nach **§§ 277 ff UGB** bestehen unter

Bedachtnahme auf § 1 DSGVO und Art 8 GRCh keine Bedenken. Die DSGVO enthält Bestimmungen zum Schutz personenbezogener Daten natürlicher Personen, schützt aber nicht die Daten **juristische Personen**. Für die Offenlegung personenbezogener Daten natürlicher Personen in einem öffentlich zugänglichen **Handelsregister** kommen regelmäßig die Rechtfertigungsgründe des Art 6 Abs 1 lit c (rechtliche Verpflichtung) und/oder lit e (Aufgabe im öffentlichen Interesse) DSGVO in Betracht ([OGH 13.08.2025, 6Ob173/24w](#)).

- Die **Beschlagnahme** von **Datenträgern** und **Daten** darf nicht durchgeführt werden, um dadurch erst einen **(Anfangs-)Verdacht** zu begründen. Eine **pauschale Anordnung** ohne Konkretisierung der Datenarten oder bloß auf Grundlage eines unzureichend begründeten Tatverdachts ist **unzulässig** ([OLG Wien 28.07.2025, 30Bs196/25f](#)).

### **Rechtsprechung des BVwG**

Aus der Rechtsprechung des BVwG:

- Eine Bank hat ein **berechtigtes Interesse** an der Meldung eines **Zahlungsausfalls** an den Kreditschutzverband 1870 (**KSV 1870**). Die Meldung darf auch in die **Warnliste der österreichischen Kreditinstitute** und in die **Kleinkreditevidenz (KKE)** eingetragen werden. Die Verarbeitung von historischen Zahlungsinformationen ist geeignet, um das zukünftige Zahlungsverhalten eines Schuldners zu analysieren und damit eine Risikominimierung zu gewährleisten. Die Verarbeitung von Daten über die Erteilung einer Restschuldbefreiung ist zwar ein schwerer Eingriff in das Grundrecht auf Datenschutz. Sie ist aber berechtigt, wenn der Kunde seine Verpflichtungen über einen längeren Zeitraum nicht erfüllt und die Bank die restliche Forderung im Rechtsweg einfordern muss ([BVwG 09.07.2025, W298 2309078-1](#)).

### **Rechtsprechung der DSB**

DSB 12.06.2025, 2024-0.490.294

#### **Homeoffice, Zutrittssystem, Betriebsrat**

- Ein Arbeitgeber verwendete personenbezogene Daten aus einem elektronischen Zutrittssystem, um zu prüfen, ob ein Arbeitnehmer gegen die für ihn geltenden **Homeofficebestimmungen** verstieß. Der Arbeitgeber leitete die Daten über die Homeofficetage auch an das Finanzamt (**FA**) weiter. Der Betriebsrat (**BR**) wurde von der Datenverarbeitung informiert. In der Betriebsvereinbarung (**BV**) über die Nutzung des Zutrittssystems war die Verwendung des Systems zum Zweck der Anwesenheitsprüfung ausgeschlossen. Der Arbeitnehmer sah

in der nicht BV-konformen Nutzung des Systems und in der Weiterleitung seiner Daten an das FA eine Verletzung der Vertraulichkeit und brachte eine erfolglose Datenschutzbeschwerde bei der DSB ein.

Die DSB hat erwogen: Bei der Auslegung einer Datenschutzbeschwerde an die DSB ist nicht nur deren Wortlaut, sondern auch der **Wille** der Partei beachtlich. Der Verfahrensgegenstand wird durch das Parteivorbringen beschränkt. Für die Ermittlung der Rechtsqualität einer Beschwerde ist der **tatsächliche Inhalt**, insbesondere das **erkennbare Ziel**, entscheidend.

An dem Auswerten von Daten aus einem Zutrittssystem kann für den Zweck der Anwesenheitskontrolle ein **berechtigtes Interesse** nach Art 6 Abs 1 lit f DSGVO bestehen. Ein Arbeitgeber hat ein berechtigtes Interesse daran, Verdachtsfälle falscher Angaben zu Anwesenheiten unter Missachtung von **Homeoffice-Regelungen** aufzuklären. Die Auswertung von Daten eines Zutrittssystems kann zur anlassbezogenen Nachkontrolle erforderlich sein.

Das Interesse des Arbeitgebers an der Aufklärung eines Verdachts von falschen Angaben, um etwaige Verstöße gegen die Dienstpflicht aufzuklären, überwiegt entgegenstehende Geheimhaltungsinteressen der Arbeitnehmer. Bei der Überprüfung eines konkreten Verdachts handelt es sich um eine **ad-hoc-Kontrolle** und keine wiederkehrende oder länger währende Maßnahme. Diese ad-hoc-Kontrolle ist vertrags- und datenschutzrechtlich zwar beschränkt, aber **BR-zustimmungsfrei**.

Nach **§ 84 Abs 3 EStG** muss der Arbeitgeber die Anzahl der Homeoffice-Tage an das FA melden. Die Datenübermittlung erfolgte somit zum Erfüllen einer rechtlichen Verpflichtung gemäß Art 6 Abs 1 lit c DSGVO.

DSB 07.08.2025, 2025-0.626.844

#### **Auskunft, Fernzugriff, Format, Erleichterungsgebot, Marktortprinzip**

- Der Nutzer eines Streamingdienstes mit Sitz in den USA stellte im Jahr 2018 einen Antrag auf Auskunft an den Streamingbetreiber. Der Streamingbetreiber antwortete, dass bestimmte Informationen möglicherweise über sichere Online-Tools verfügbar sind und verwies auf das Nutzerkonto sowie auf die Datenschutzerklärung. Weiters stellte der Streamingbetreiber mehrere Dateien in den Formaten OPML oder JSON zum Download bereit. Eine personalisierte Auskunft zu Verarbeitungszwecken wurde nicht erteilt. Die DSB leitete das Verfahren an die irische Datenschutzbehörde als federführende Aufsichtsbehörde weiter und setzte das Verfahren aus. Die irische Aufsichtsbehörde erklärte sich für unzuständig und leitete die Datenschutzbeschwerde an die DSB

zurück. In weiterer Folge gab die DSB der Datenschutzbeschwerde statt.

Die DSB hat erwogen: Gemäß **Art 3 Abs 2 lit a DSGVO** findet die DSGVO Anwendung, wenn nicht in der Union niedergelassene Verantwortliche Daten von Betroffenen in der EU iZm angebotenen Waren oder Dienstleistungen verarbeiten ("**Marktortprinzip**"). Der Begriff "**Dienstleistung**" ist weit auszulegen. Erforderlich ist lediglich eine hinreichend erkennbare Absicht eines nicht im EWR niedergelassenen Verantwortlichen oder Auftragsverarbeiters, in der Union befindlichen Personen eine Dienstleistung anzubieten. Der Streamingbetreiber beabsichtigt, österreichische Nutzer zu erreichen. Da die Niederlassung in Irland nicht als Verantwortliche zu betrachten war, ist die DSB für die Datenschutzbeschwerde zuständig.

Der Streamingbetreiber erfüllte das Auskunftersuchen teilweise, indem er Dateien in den **Formaten JSON** und **OPML** bereitstellte. Diese Formate sind jedoch weder leicht zugänglich noch verständlich und widersprechen daher dem **Transparenzgebot** nach Art 12 Abs 1 DSGVO. Die Auskunftspflicht umfasst eine verständliche Aufbereitung, nicht nur eine technische Bereitstellung. Ein Portal, bei dem Betroffene selbst Daten zusammensuchen und fehlende Informationen beim Kundensupport anfragen müssen, widerspricht dem **Erleichterungsgebot** des Art 12 Abs 2 DSGVO. Von einem Betroffenen kann nicht verlangt werden, selbst die fehlenden Informationen zu identifizieren, weil dieser noch keine Kenntnis darüber haben kann, welche Daten verarbeitet werden.

Die **Datenschutzerklärung** ist *eine ex ante* Information zur Erfüllung der Informationspflichten nach Art 13 und 14 DSGVO, aber **keine personalisierte Information**. Sie enthält allgemeine Angaben, die nicht ohne Weiteres auf eine Einzelperson zutreffen. Eine vollständige Auskunft kann daher nicht mit dem bloßen Verweis auf eine allgemeine Erklärung erfolgen. Indem der Streamingbetreiber lediglich allgemein und ohne weitere Klarstellung auf die von ihm verfolgten Zwecke verwies, hat er den Streamingnutzer in seinem **Recht nach Art 15 Abs 1 lit a DSGVO verletzt**. Er konnte nicht bestimmen, welche Daten von ihm zu welchem Zweck wie lange verarbeitet werden.

### Nationale Rechtsakte

- Am **01.09.2025** sind das neue **Grundrecht auf Informationszugang** sowie das **Informationsfreiheitsgesetz (IFG)** in Kraft getreten. Ebenso am **01.09.2025** ist die **Verfügbarkeit des Informationsregisters** durch Verordnung des

Bundeskanzlers kundgemacht worden, [BGBl II 2025/52](#). Die Informationen von allgemeinem Interesse sind sohin spätestens ab dem **01.12.2025** auf [www.data.gv.at](http://www.data.gv.at) bereitzustellen.

- Am **04.09.2025** wurde das **vorarlbergerische Gesetz** über begleitende Regelungen zur **Informationsfreiheit** und landesspezifische Regelungen zum **Datenschutz** – Sammelnovelle, [LGBI 2025/44](#), kundgemacht. Mit dieser Sammelnovelle wurden **vorarlbergerische Gesetze** dem neuen **Grundrecht auf Informationszugang** angepasst. Ua sind das Landesverwaltungsgerichtsgesetz und das "*Gesetz über landesspezifische Regelungen zum Datenschutz*" novelliert worden.
- Am **04.09.2025** wurde das **vorarlbergerische Verfassungsgesetz** über eine Änderung der **Landesverfassung**, [LGBI 2025/43](#), kundgemacht. Mit diesem Landesverfassungsgesetz wurde das **Parlamentarische Datenschutzkomitee (PDK)** für die **Datenschutz-Aufsicht** über die Verarbeitung personenbezogener Daten durch den Landtag, den Landesvolksanwalt und den Landes-Rechnungshof von Vorarlberg für zuständig erklärt. **Anm: Das PDK ist seit Anfang des Jahres 2025 auf Bundesebene für die Datenschutz-Aufsicht der Legislativorgane zuständig. Die Länder können dem PDK für die Aufsicht über ihre Legislativorgane die Zuständigkeit einräumen. Sonst ist die DSB zuständig. Das PDK ist über die Website <https://pdk.gv.at> erreichbar. Bis dato ist ein Bescheid des PDK zur Verletzung des Rechts auf Geheimhaltung iZm dem BVT-Untersuchungsausschuss veröffentlicht ([PDK 25.06.2025, 2025-0.268.011](#)). Künftig werden im Schönherr Datenschutzmonitor auch die Bescheide des PDK erfasst werden.**

to the point

# Datenschutzmonitor. 37/2025 vom 17.09.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 09.09.2025, 24729/17, *Iloveva/Bulgaria* (Hassrede, Ermittlungspflicht, Facebook-Account)

EGMR 11.09.2025, 26519/16, *Yakymchuk/Ukraine* (geheime Videoüberwachung, Gerichtsbeschluss)

EGMR 11.09.2025, 28473/22, *Charki/France* (Medien, Telefonüberwachung)

- **Rechtsprechung des EuGH / EuG**

EuG 10.09.2025, T-58/24, *TikTok*; 10.09.2025, T-55/24, *Meta Platforms* (DSA, Online-Plattformen, Aufsichtsgebühr)

EuGH 11.09.2025, C-115/24, *Österreichische Zahnärztekammer* (Telemedizin, Herkunftslandprinzip)

- **Rechtsprechung der Justiz**

OGH 26.08.2025, 9ObA83/24g (Führungsgorgan, Dritte, sensible Daten, Rechtsverteidigung)

OGH 13.08.2025, 6Ob121/25z (Datenschutz, Schadenersatz, Bewertungsanspruch)

OLG Wien 16.07.2025, 2R62/25i (Auskunft, Fristverlängerung, Kostentragung)

- **Rechtsprechung des BVwG**

BVwG 01.09.2025, W256 2235360-1 (Profiling, Art 22 DSGVO, menschliche Entscheidung)

BVwG 14.07.2025, W274 2309030-1 (Medienprivileg, Löschung, Namensanonymität)

BVwG 22.07.2025, W211 2309849-1 (internationaler Schutz, Rückkehrentscheidung, biometrische Daten)

BVwG 14.07.2025, W274 2309622-1 (Gesundheitsdaten, Erlaubnistatbestand)

BVwG 16.07.2025, W211 2302514-1 (Ediktsdatei, Insolvenz, öffentliche Daten)

BVwG 09.07.2025, W274 2244313-1 (Missbrauchsabsicht, feindselige Motivation, Gebühr)

BVwG 17.07.2025, W137 2300883-1 (AuskunftspflichtG, Akteneinsicht)

BVwG 10.07.2025, W137 2306286-2 (AuskunftspflichtG, Richtlinien)

BVwG 23.05.2025, W164 2279298-1 (AMS, Bewerbung, Datenschutz)

BVwG 22.07.2025, W211 2267466-3 (Wiederaufnahme, Obsorge, *nova reperta*)

- **Rechtsprechung der LVwG**

LVwG Vorarlberg 07.08.2025, LVwG-352-1/2025-R22; 28.08.2025, LVwG-352-3/2025-R (Amtsverschwiegenheit, public watchdog, Interessenabwägung)

- **Rechtsprechung der DSB**

DSB 05.09.2025, 2025-0.271.604 (Kreditauskunftei, Zweckänderung, Informationspflicht)

- **EU-Rechtsakte**

Anwendbarkeit der Datenverordnung (Data Act)

EDPS, Guidelines 3/2025 on the interplay between the DSA and the GDPR (2025)

Berichtigung des Data Acts

## To the Point:

### Rechtsprechung des EGMR

Aus der Rechtsprechung des EGMR:

- Vertragsstaaten des EMRK haben eine **positive Pflicht**, von **Morddrohungen** und **schwerwiegender Hassrede** (serious hate speech) durch strafrechtliche Bestimmungen abzuschrecken und diese Bestimmungen effektiv anzuwenden. Die **effektive Anwendung** bedeutet, dass **ermittelt** wird und dabei geeignete Maßnahmen ergriffen werden. Eine Verpflichtung auf Erfolg besteht nicht. Werden entsprechende Hassnachrichten mit Accounts über Facebook verbreitet, dürfen Informationen über diese **Accounts von Facebook** angefordert werden (einschließlich Name, Adresse, Beruf, E-Mail-Adresse und Telefonnummer). Die Betreiber von **Websites**, über die Hassnachrichten verbreitet werden, dürfen einvernommen und die IP-Adressen der Websites dürfen ermittelt werden ([EGMR 09.09.2025, 24729/17, Ilareva/Bulgaria](#)).
- Basiert eine **geheime Videoüberwachung** auf einem **Gerichtsbeschluss**, ist der überwachten Person **Zugang** zu diesem Gerichtsbeschluss zu gewähren, sofern keine überzeugenden Argumente für die Geheimhaltung des Gerichtsbeschlusses sprechen. Die **Klassifizierung** des Gerichtsbeschlusses als geheim reicht für sich genommen nicht aus ([EGMR 11.09.2025, 26519/16, Yakymchuk/Ukraine](#)).
- Die **mediale Veröffentlichung** der Niederschrift von **abgehörten Telefongesprächen** iZm Korruptionsermittlungen kann zulässig sein ([EGMR 11.09.2025, 28473/22, Charki/France](#)).

### Rechtsprechung des EuGH / EuG

[EuG 10.09.2025, T-58/24, Tiktok](#); [10.09.2025, T-55/24, Meta Platforms](#)

- Die Kommission setzte im Jahr 2023 **jährliche Aufsichtsgebühren** für **sehr große Online-Plattformen (SGP)** und sehr große **Online-Suchmaschinen** fest (Art 43 Abs 1-3 DSA). Die Kommission erließ zunächst die DelegierteVO 2023/1127, in der sie detaillierte Methoden und Verfahren hinsichtlich der zu erhebenden Aufsichtsgebühren vorsah. Adressaten waren nach Art 33 Abs 4 DSA ua Meta und TikTok. Die endgültige Höhe der jeweils anwendbaren Gebühr legte die Kommission mit Durchführungsbeschlüssen fest. Die Berechnung beruhte auf Art 5 der DelegiertenVO sowie auf Daten von Drittanbietern. Die durchschnittliche monatliche Zahl aktiver Nutzer wurde jedoch anhand einer **gemeinsamen Methodik** für alle SGP bestimmt, die den jeweiligen Beschlüssen als

Anhang beigelegt waren. Meta Platforms Ireland und TikTok Technology Ltd erhoben erfolgreiche **Nichtigkeitsklagen** nach Art 263 AEUV an das EuG.

Das EuG hat erwogen: Für Art 43 DSA ist nicht die absolute Nutzerzahl jedes Dienstes entscheidend, sondern ihr relativer Wert im Verhältnis zu anderen benannten Diensten. Die Kommission hatte berechnete Zweifel an der Kohärenz der von den Anbietern verwendeten Methoden, zumal ihr nicht alle Daten vorlagen. Sie war daher im Interesse der Transparenz und Gleichbehandlung berechtigt, eine **gemeinsame Methodik** anzuwenden, weil die Aufsichtskosten im Verhältnis zur durchschnittlichen Nutzerzahl aufzuteilen sind.

Die DelegierteVO sieht **keine Rangordnung** zwischen den drei **Informationsquellen** – (i) vom Anbieter gemäß Art 24 Abs 2 DSA gemeldete Daten, (ii) gemäß Art 24 Abs 3 DSA angeforderte Informationen und (iii) andere der Kommission vorliegende Informationen – vor. Die Kommission war daher nicht verpflichtet, einer dieser Quellen den Vorzug zu geben.

Aus der Systematik und den Zielen des DSA folgt, dass der Begriff "**durchschnittliche Nutzerzahl**" einheitlich und kohärent zu verstehen ist. Nach Art 43 Abs 4 DSA muss die Kommission **delegierte Rechtsakte** erlassen, in denen die detaillierte Methodik und Verfahren zur Festlegung der jährlichen Aufsichtsgebühren geregelt werden. Diese Gebühren müssen nach Art 43 Abs 5 lit b DSA im Verhältnis zur durchschnittlichen Nutzerzahl stehen.

Gemäß Art 43 DSA besteht ein **Zusammenhang** zwischen der **Methodik zur Festlegung der jährlichen Aufsichtsgebühren**, die nur durch einen delegierten Rechtsakt bestimmt werden dürfen, und den Nutzerzahlen der benannten Dienste. Folglich ist die Methodik zur Berechnung der durchschnittlichen Nutzerzahl der Festlegung der Aufsichtsgebühr inhärent und als ein wesentlicher und unverzichtbarer Bestandteil dieser Festlegung anzusehen. Die Kommission ist daher verpflichtet, zumindest hinreichend detaillierte Bestandteile der Methodik im delegierten Rechtsakt festzulegen. Die gemeinsame Methodik wäre nicht in den **Durchführungsbeschlüssen**, sondern bereits in der DelegiertenVO festzulegen gewesen. Da sich die Kommission in der DelegiertenVO darauf beschränkt hat, drei Informationsquellen anzugeben, hat sie gegen **Art 43 Abs 3 bis 5 sowie Art 87 DSA** verstoßen.

Aus der Rechtsprechung des EuGH:

- Unter den Begriff der **Telemedizin** fallen nur Gesundheitsdienstleistungen, die im **Fernabsatz** und somit ohne gleichzeitige

physische Anwesenheit des Patienten am selben Ort ausschließlich mit Hilfe von Informations- und Kommunikationstechnologien erbracht werden. Telemedizinische Leistungen sind nach den **Rechtsvorschriften des Mitgliedstaats** zu erbringen, in dem der Dienstleister ansässig ist ([EuGH 11.09.2025, C-115/24, Österreichische Zahnärztekammer](#)).

### **Rechtsprechung der Justiz**

Aus der Rechtsprechung der Justiz:

- Personen, die einem **Führungsorgan** eines Verantwortlichen angehören, sind **keine unbefugten Dritte**. Sie dürfen einen Schriftsatz erhalten, um Kenntnis vom Sachverhalt zu erhalten. Die im Schriftsatz enthaltenen **sensiblen Daten** waren erforderlich für die **Rechtsverteidigung** iSd Art 9 Abs 2 lit f DSGVO ([OGH 26.08.2025, 9ObA83/24g](#)).
- Wird der Schutz oder die Durchsetzung eines **Datenschutzrechts** verfolgt, ist **kein Bewertungsausspruch** iSd § 502 ZPO hinsichtlich der Zulässigkeit der Revision vorzunehmen. Die Revision ist jedenfalls zulässig. Wird hingegen ein Anspruch auf **Schadenersatz** geltend gemacht und besteht der Entscheidungsgegenstand ausschließlich im **Geldbetrag** als Ausgleich für einen bereits erfolgten Eingriff, ist kein Bewertungsausspruch erforderlich, weil der Entscheidungsgegenstand in einem Geldbetrag besteht. Die Zulässigkeit der Revision hängt von der Höhe des Geldbetrags ab ([OGH 13.08.2025, 6Ob121/25z](#)).
- Informiert der Verantwortliche den Auskunftswerber, die **Fristverlängerung** auf drei Monate iSd Art 12 Abs 3 Satz 3 DSGVO in Anspruch nehmen zu wollen, bringt er zum Ausdruck, dass er innerhalb von einem Monat nicht erfüllen wird. Nur wenn diese Mitteilung so konkret ist, dass sie dem Auskunftswerber die Beurteilung erlaubt, ob die Fristverlängerung gerechtfertigt ist, kann davon ausgegangen werden, dass die **Klage iSd § 45 ZPO nicht veranlasst** wurde. Sonst hat der Verantwortliche die **Kosten des Verfahrens** zu tragen. Die Mitteilung, dass über **4.000 Auskunftersuchen** eingegangen sind, ist nicht hinreichend aussagekräftig. Die Auskunft ist überdies nicht in jedem Fall innerhalb eines Monats, sondern **unverzüglich** zu erteilen ([OLG Wien 16.07.2025, 2R62/25i](#)).

### **Rechtsprechung des BVwG**

BVwG 01.09.2025, W256 2235360-1

#### **Profiling, Art 22 DSGVO, menschliche Entscheidung**

- Das Arbeitsmarktservice (**AMS**) setzte das "**Arbeitsmarktchancen Assistenz-System**" (**AMAS**) ein, um mittels Algorithmus die Arbeitsmarktchancen von Arbeitssuchenden zu berechnen. Die Datenschutzbehörde leitete 2020 ein amtswegiges Prüfverfahren ein und untersagte diese Datenverarbeitung mangels geeigneter Rechtsgrundlage sowie wegen unzulässiger automatisierter Einzelentscheidung gemäß Art 22 DSGVO. Das AMS erhob dagegen Beschwerde an das BVwG, das den Bescheid zunächst aufhob und die Datenverarbeitung als rechtmäßig beurteilte. Nach Amtsrevision der DSB hob jedoch der VwGH das Erkenntnis des BVwG auf und forderte eine neuerliche Prüfung, insb zur Frage, ob das AMAS-Ergebnis eine maßgebliche Rolle für die Entscheidung spiele und damit eine automatisierte Einzelentscheidung vorliege.

In einem ergänzenden Ermittlungsverfahren legte das AMS weitere Unterlagen vor und erläuterte die Einbindung der AMS-Berater. Demnach hat AMAS personenbezogene Daten (ua Alter, Geschlecht, Ausbildung, Gesundheit) automatisiert verarbeitet und daraus eine Prognose für die Arbeitsmarktintegration erstellt. Die AMS-Berater sollten diesen Wert als Unterstützung im Beratungsgespräch nutzen, konnten ihn aber jederzeit anpassen oder korrigieren. Das BVwG hob den Bescheid der DSB erneut auf.

Das BVwG hat erwogen: Die Frage der Rechtmäßigkeit einer Verarbeitung nach den Bestimmungen des Art 6 und Art 9 DSGVO ist von der Frage des Verbots **automatisierter Entscheidungen** gemäß Art 22 DSGVO zu trennen. Die Verarbeitung der Daten durch das AMS ist durch § 25 AMStG iVm §§ 29 bis 31 AMStG ausreichend gesetzlich gedeckt und dient einem **erheblichen öffentlichen Interesse** (Art 6 Abs 1 lit e, Art 9 Abs 2 lit g DSGVO). Die Einbindung des Algorithmus als "zweite Meinung" ist **kein ausschließlich automatisiertes Profiling** iSd Art 22 Abs 1 DSGVO, weil die menschliche Entscheidung der Berater maßgeblich bleibt. Interne Richtlinien, Schulungen und Kontrollmechanismen stellen sicher, dass die Berater nicht bloß formell, sondern inhaltlich entscheiden und von der automatisierten Empfehlung abweichen können und uU müssen. Die bloße Nutzung eines **algorithmischen Assistenzsystems** begründet keine unzulässige automatisierte Einzelentscheidung, solange die **Letztentscheidung** und **Verantwortung** bei einer **natürlichen Person** liegen.

Das von der DSB verhängte Verarbeitungs-  
verbot war daher aufzuheben.

BVwG 14.07.2025, W274 2309030-1

### **Medienprivileg, Löschung, Namensanonymität**

- Der ehemalige Franchisenehmer einer Fast-foodkette verlangte von einem Medienunternehmen, seinen Namen aus einem 2011 erschienenen Online-Artikel über die Eröffnung eines Lokals zu löschen. Da das Medienunternehmen die Löschung ablehnte, erhob er Datenschutzbeschwerde bei der DSB und behauptete, die Verbindung mit der inzwischen insolventen Marke schade seiner beruflichen Entwicklung und verletze seine Persönlichkeitsrechte. Die DSB wies die Datenschutzbeschwerde ab. Daraufhin erhob der Unternehmer (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Das **neue Medienprivileg** unterscheidet zwischen "**institutionellem Journalismus**" und "**Bürgerjournalismus**" und umfasst eine sehr detaillierte Abwägung zwischen den Grundrechten auf Informationsfreiheit und Datenschutz. Für **journalistische Veröffentlichungen** in Medien iSd MedienG sind die Rechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung **grundsätzlich ausgeschlossen**. Betroffene können jedoch eine eingeschränkte Überprüfung durch die DSB beantragen.

Da die Voraussetzung der Veröffentlichung in einem Medium gemäß § 1 Abs 1 Z 1 MedienG vorliegt, ist die **Ausnahme vom Recht auf Löschung** *in concreto* gegeben. Aufgrund dieser generellen Ausnahme ist es unerheblich, ob der Artikel noch journalistische Relevanz hat, eine abgeschlossene unternehmerische Tätigkeit betrifft oder die Karriere des Betroffenen als Marketingexperte nachteilig beeinflussen könnte.

Das **Recht auf Namensanonymität** schützt die Person davor, dass ihr Name von Dritten in ihrer Persönlichkeit beeinträchtigenden Zusammenhängen genannt wird, wozu sie selbst keinen sachlichen Anlass gegeben hat und damit ihre Identität in eben diesem Zusammenhang einem nicht unmittelbar informierten größeren Personenkreis gegenüber preisgegeben wird. Da der Unternehmer selbst an der Entstehung des Artikels mitgewirkt hat, indem er dem Artikelverfasser seinen Namen sowie Informationen über das Unternehmen geliefert hat, hat er selbst einen sachlichen Anlass zur erfolgten Namensnennung gegeben. Ein Anspruch auf Löschung kann daher auch nicht aus § 16 ABGB abgeleitet werden. Die DSB hat die Datenschutzbeschwerde daher zu Recht abgewiesen.

BVwG 22.07.2025, W211 2309849-1

### **Internationaler Schutz, Rückkehrentscheidung, biometrische Daten**

- Ein Schutzsuchender beantragte internationalen Schutz in Österreich. Nachdem das **Bundesamt für Fremdenwesen und Asyl (BFA)** seinen Antrag abwies, erließ es eine **Rückkehrentscheidung** und ein **einjähriges Einreiseverbot** und trug diese Entscheidung einschließlich **biometrischer Daten** gemäß Art 3 VO (EU) 2018/1860 (**VO-SIS-Rückkehr**) im **Schengener Informationssystem (SIS)** ein. Der Schutzsuchende beantragte daraufhin die Löschung dieser **Ausschreibung**, weil ihm die portugiesische Behörde für den Fall der Löschung einen Aufenthaltstitel zugesagt haben soll. Da das BFA dem Lösungsersuchen nicht nachkam, erhob der Schutzsuchende Datenschutzbeschwerde bei der DSB. Gegen den abweisenden Bescheid der DSB erhob er (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die Mitgliedstaaten der EU müssen nach Art 3 Abs 1 VO-SIS-Rückkehr Rückkehrentscheidungen im SIS ausschreiben, um die Durchsetzung dieser Entscheidungen zu gewährleisten. Eine **Löschung** der entsprechenden Ausschreibung im SIS erfolgt nach Art 14 VO-SIS-Rückkehr nur, wenn die Rückkehrentscheidung aufgehoben oder für nichtig erklärt wird oder der betroffene Drittstaatsangehörige nachweisen kann, das Hoheitsgebiet der Mitgliedstaaten verlassen zu haben. Keine dieser Voraussetzungen liegt vor.

Dem Schutzsuchenden steht grundsätzlich ein **Recht auf Löschung** gemäß Art 17 DSGVO zu. Dieses Recht besteht gemäß Art 17 Abs 3 DSGVO jedoch nicht, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich ist. Die Verarbeitung der personenbezogenen Daten des Schutzsuchenden im SIS erfolgte rechtmäßig auf Grundlage von **Art 6 Abs 1 lit c und e DSGVO** iVm Art 3 VO-SIS-Rückkehr, weil das BFA verpflichtet war, die Rückkehrentscheidung im SIS auszuschreiben.

Nach Art 9 Abs 1 DSGVO ist die Verarbeitung von **sensiblen Daten** grundsätzlich untersagt. Die Verarbeitung der **biometrischen Daten** des Schutzsuchenden in Form von **Fingerabdrücken** war jedoch gemäß Art 9 Abs 2 lit g DSGVO zulässig, weil diese auf die VO-SIS-Rückkehr gestützt werden konnte, deren Zweck die Durchsetzung von Rückkehrentscheidungen gegen illegal aufhältige Drittstaatsangehörige ist. Die Verarbeitung von Fingerabdrücken ist zur Identifizierung der betroffenen Drittstaatsangehörigen im Schengenraum erforderlich und verhältnismäßig. Vor diesem Hintergrund

erfolgte die Datenverarbeitung durch das BFA rechtmäßig.

#### Aus der weiteren Rechtsprechung des BVwG:

- Werden **Gesundheitsdaten** und damit **sensible Daten** iSd Art 9 Abs 1 DSGVO verarbeitet, bedarf es zur Rechtfertigung der Verarbeitung neben dem allgemeinen **Erlaubnistatbestand** des Art 6 Abs 1 DSGVO auch einer besonderen Ausnahme iSd Art 9 Abs 2 DSGVO. Das bloße Überwiegen des berechtigten Interesses des Verantwortlichen gegenüber dem Geheimhaltungsinteresse des Betroffenen genügt nicht. Da der Verantwortliche die personenbezogenen Daten des Betroffenen an eine Behörde weitergeleitet hat, ohne dass eine Ausnahme des Art 9 Abs 2 DSGVO vorlag, war die Übermittlung unzulässig. Es spielt keine Rolle, ob die Daten nur einer Behörde und nicht einer breiten Öffentlichkeit zugänglich gemacht werden, weil jede Verarbeitung ohne eine **Ausnahmeregelung** nach Art 9 Abs 2 DSGVO unzulässig ist ([BVwG 14.07.2025, W274 2309622-1](#)).
- In der **Ediktsdatei** veröffentlichte Daten über eine **Insolvenz** sind **öffentlich zugängliche** (verfügbare) **Daten**. Sind Gegenstände aus der Insolvenzmasse bereits herausgekauft worden, darf der Käufer bei der **anschließenden Versteigerung** dieser Gegenstände den Namen des Insolvenzschuldners trotz der Veröffentlichung in der Ediktsdatei dennoch nicht verwenden ([BVwG 16.07.2025, W211 2302514-1](#)).
- Die Einholung medizinischer Gutachten in Gerichtsverfahren dient der Objektivierung des Gesundheitszustands von Parteien. Werden datenschutzrechtliche Betroffenenrechte aus **feindseliger Motivation** gegen den **Sachverständigen** eingesetzt, um das gutachterliche Ergebnis in Zweifel zu ziehen, liegt **Missbrauchsabsicht** vor. Hat der Betroffene vor dem BVwG zahlreiche kostspielige Verfahren geführt, war die Ablehnung der Datenschutzbehörde durch die DSB im Verhältnis zur **Einhebung der Gebühr** geeignet, um dieser Missbrauchsabsicht zu begegnen ([BVwG 09.07.2025, W274 2244313-1](#)).
- Das Auskunftsrecht nach dem **AuskunftspflichtG** ist nicht geeignet, um eine **Akten-einsicht** in einem Verfahren durchzusetzen, in dem der Auskunftswerber keine **Parteistellung** hat ([BVwG 17.07.2025, W137 2300883-1](#)). **Anm: Das AuskunftspflichtG ist am 01.09.2025 außer Kraft getreten und ist durch das Informationsfreiheitsgesetz (IFG) ersetzt worden. Das Recht auf Informationszugang nach dem IFG ist zwar subsidiär zum Recht auf Akteneinsicht (§ 16 IFG). Kommt dem Informationswerber kein Recht auf Akteneinsicht zu, könnte**

die Beurteilung, ob die Information zu erteilen ist, jedoch anders als nach dem AuskunftspflichtG ausfallen.

- Nach dem **AuskunftspflichtG** besteht kein Anspruch auf Ausfolgung der **Richtlinien** für den Unterstützungsfonds der Versicherungsträger ([BVwG 10.07.2025, W137 2306286-2](#)). **Anm: Auch für die Herausgabe solcher Richtlinien könnte sich die Rechtslage unter dem IFG geändert haben.**
- Wird das **Bewerbungsgespräch** abgebrochen, weil der Bewerber seine **Einwilligung** in die im Bewerbungsbogen abgedruckten Passagen nicht geben und die **Datenschutzerklärung** des potenziellen künftigen Dienstgebers einsehen möchte, ist die Ablehnung des Bewerbers der Sphäre des Dienstgebers zuzurechnen. Dem Bewerber ist vom **AMS** keine **Vereitelungshandlung** zur Last zu legen ([BVwG 23.05.2025, W164 2279298-1](#)).
- Kommt dem **Wiederaufnahmewerber** mangels **Obsorge** keine Vertretungsbefugnis für den minderjährigen Sohn zu, fehlt ihm die Legitimation zur Erhebung eines Wiederaufnahmeantrags. Die neu vorgelegten Screenshots sind auch keine neu hervorgekommenen Beweismittel (**nova reperta**), die voraussichtlich eine anders lautende Entscheidung herbeigeführt hätten ([BVwG 22.07.2025, W211 2267466-3](#)).

#### **Rechtsprechung der LVwG:**

[LVwG Vorarlberg 07.08.2025, LVwG-352-1/2025-R22; 28.08.2025, LVwG-352-3/2025-R](#)

#### **Amtsverschwiegenheit, public watchdog, Interessenabwägung**

- Ein Journalist beehrte vom **Amt der Vorarlberger Landesregierung** Auskunft über die Empfänger und die Höhe von ausbezahlten Covid-19-Wirtschaftsförderungen, inklusive Namen und PLZ der Förderempfänger, sowie von Sonderförderungen an Tourismus- und Busunternehmen. Weiters beehrte er die Herausgabe einer Liste aller natürlichen und juristischen Personen, von denen Fördermittel zurückgefordert wurden. In Beantwortung erhielt er anonymisierte Tabellen. Die Namen der Förderempfänger beauskunftete die Landesregierung nicht. Sie berief sich auf gesetzliche Verschwiegenheitspflichten und den Datenschutz. Da der Journalist auch die Offenlegung der tatsächlichen Förderempfänger erreichen wollte, brachte er gegen die abweisenden Bescheide zwei Bescheidbeschwerden an das LVwG Vorarlberg ein. Einer der Bescheidbeschwerden wurde teilweise Folge gegeben.

Das LVwG Vorarlberg hat erwogen: Eine Auskunft nach dem Vorarlberger Auskunftsg dar nur erteilt werden, wenn **keine**



gesetzliche Verschwiegenheitspflicht entgegensteht. Darunter fallen **Verschwiegenheitspflichten** aus Art 20 Abs 3 B-VG (**Amtsverschwiegenheit**) und auch das Recht auf **Geheimhaltung** aus dem DSGVO. Förderwerber haben grundsätzlich ein Interesse am Schutz ihrer Daten.

Nach Art 20 Abs 3 B-VG sind Landesorgane zur Verschwiegenheit über ihnen ausschließlich aus ihrer amtlichen Tätigkeit bekannt gewordene Tatsachen verpflichtet, deren Geheimhaltung im überwiegenden Interesse der Parteien geboten ist. Der **Parteienbegriff** ist dabei weit zu verstehen und umfasst alle Personen, die aus irgendeinem Anlass mit der Behörde in Kontakt kommen, somit auch vom Auskunftswerber verschiedene **Dritte**, die vom Auskunftsverlangen betroffen sind. Dem Geheimhaltungsinteresse der Förderempfänger steht das **öffentliche Interesse** an einem breiten **Diskurs** über die Vergabe und Abwicklung von Förderungen gegenüber.

Bevor eine Auskunft erteilt werden darf, ist eine **Interessenabwägung** durchzuführen. Das **Recht auf Freiheit der Meinungsäußerung** nach Art 10 EMRK erfasst dabei auch ein Recht auf **Zugang zu Information**. Kriterien für die Interessenabwägung nach Art 10 EMRK sind (i) das Ziel und der Zweck des Informationsansuchens, (ii) die tatsächliche Notwendigkeit des Informationsbegehrens für die Ausübung der Meinungsfreiheit, (iii) der Charakter der begehrten Informationen, (iv) die Rolle des Zugangswerbers und (v) die Existenz verfügbarer Informationen.

Die Bekanntgabe von Namen und PLZ der Förderempfänger liegt im Interesse eines Journalisten in seiner Funktion als "**Public Watchdog**". Bei der Bewertung des Geheimhaltungsinteresses der Förderempfänger ist zwischen Förderungen zu **unterscheiden**, die auf den **Umsatz** des Förderempfängers abstellen und solchen, für die dies **kein Kriterium** ist. Erst bei einer Förderhöhe ab EUR 5.000 **überwiegt** das Interesse am **öffentlichen Diskurs** über die gewährte Förderung, **unter** dieser **Wertgrenze** hingegen überwiegt das **Geheimhaltungsinteresse** des Förderwerbers. Die Offenlegung des Namens des jeweiligen Förderempfängers ist dann ein **unverhältnismäßiger** Eingriff in das Recht auf Schutz personenbezogener Daten. Bei Unternehmen, die den Veröffentlichungspflichten des UGB unterliegen, tritt das Geheimhaltungsinteresse hinter dem Interesse an Offenlegung zurück.

Das **Geheimhaltungsinteresse** natürlicher Personen, die kleine Förderbeträge erhielten, ist **höher** zu werten als das Interesse des Journalisten an der **Transparenz** der Mittelvergabe zur Ermöglichung eines öffentlichen Diskurses.

Unabhängig von der Rechtsform des Förderempfängers tritt bei Förderungen, die **umsatzunabhängig** gewährt werden, das Geheimhaltungsinteresse hinter dem Interesse an Transparenz der Mittelvergabe und einer demokratischen Diskussion zurück. Aus dem Umstand der gewährten Förderung lässt sich zwar eine **wirtschaftliche Beeinträchtigung** in einem bestimmten Zeitraum ableiten, jedoch **kein** Rückschluss auf den Umsatz ziehen. **Anm: Das Amtsgeheimnis wurde in der Zwischenzeit aufgehoben und durch das Grundrecht auf Informationszugang ersetzt. Da das LVwG Vorarlberg das Informationsinteresse des Journalisten als public watchdog gewichtete, führt die neue Rechtslage jedoch nicht zwingend zu einem anderen Ergebnis.**

### **Rechtsprechung der DSB**

DSB 05.09.2025, 2025-0.271.604

#### **Kreditauskunftei, Zweckänderung, Informationspflicht**

- Ein Betroffener stellte bei einer **Kreditauskunftei** ein Auskunftsersuchen und erfuhr dabei erstmals von der Verarbeitung seines Namens, seines Geburtsdatums und seiner historischen Adressen. Diese Daten wurden ursprünglich von einem **Adressverlag** zu **Marketingzwecken** erhoben und im Rahmen einer Vereinbarung an die Kreditauskunftei weitergegeben. Dort wurden sie für **Identitätsprüfungen** und die Berechnung von **Bonitätswerten** genutzt. Da der Betroffene über die Datenerhebung oder Zweckänderung nicht informiert wurde und auch keine Einwilligung erteilt hatte, erhob er Datenschutzbeschwerde bei der DSB.

Die DSB hat erwogen: Jede Verarbeitung personenbezogener Daten muss den in Art 5 DSGVO aufgestellten Grundsätzen sowie einem in Art 6 DSGVO angeführten Erlaubnistatbestand entsprechen. Der Verantwortliche trägt die **Beweislast** für die Einhaltung der Grundsätze. Der **Grundsatz der Zweckbindung** verlangt, dass personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden. Die Zwecke müssen **spätestens zum Zeitpunkt der Erhebung** feststehen, klar angegeben sein und die Rechtmäßigkeit der Verarbeitung gewährleisten.

Das Recht der Adressverlage und Direktmarketingunternehmen, Daten Dritter zu verwenden bzw zu übermitteln, ist **auf Marketingdaten beschränkt**. Jede Datenverwendung über diesen Zweck hinaus ist nicht umfasst. Daher dürfen Daten von Adressverlagen und Direktmarketingunternehmen nicht etwa zur Prüfung eines Vertragsschlusses oder der Bonität benutzt werden.

Die Kriterien des Art 6 Abs 4 DSGVO iVm ErwGr 50 DSGVO spiegeln die Notwendigkeit einer konkreten, kohärenten und ausreichend engen Verbindung zwischen dem Zweck der Datenerhebung und deren **Weiterverarbeitung** wider. Der Zweckbindungsgrundsatz **bindet** bei einer Weiterverarbeitung der Daten durch einen **anderen Verantwortlichen** auch diesen **an die ursprüngliche Zweckfestsetzung**.

Die Informationspflicht ist Voraussetzung dafür, dass die Betroffene ihre Rechte auf Auskunft, Berichtigung oder Löschung ausüben kann. Dafür müssen die Informationen für die Betroffene leicht zugänglich sein. Werden personenbezogene Daten nicht bei der Betroffenen erhoben und besteht auch sonst keine Verbindung zum Verantwortlichen, kann nicht davon ausgegangen werden, dass die **bloße Abrufbarkeit einer Datenschutzerklärung auf einer Website** ohne aktive, ausdrückliche Verständigung der Betroffenen von dieser Form der Bereitstellung genügt.

### **EU-Rechtsakte**

- Seit dem **12.09.2025** ist die **[Datenverordnung \(Data Act\) 2023/2854](#)** unmittelbar anwendbar. Geregelt wird darin insb der Zugang zu Daten, die bei der Nutzung von intelligenten Geräten erzeugt werden (**Internet of Things**).
- Am **12.09.2025** veröffentlichte der **Europäische Datenschutzausschuss (EDSA)** den Entwurf der **[Guidelines 3/2025 on the interplay between the DSA and the GDPR](#)**. Stellungnahmen können bis zum 31.10.2025 eingereicht werden. Die Leitlinien des EDSA befassen sich ua mit sog **Dark Patterns, Transparenz, Empfehlungssystemen** und dem **Schutz von Minderjährigen**.
- Am **09.09.2025** ist die Datenverordnung (**Data Act**) **berichtigt** worden, **[ABI L 2025/90691](#)**. Die Berichtigungen sind größtenteils redaktioneller Art.

to the point

# Datenschutzmonitor.

## 38/2025 vom 24.09.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH SA 18.09.2025, C-526/24, *Brillen Rottler* (Auskunftsrecht, Missbrauchsabsicht, Schadenersatz)

EuGH SA 18.09.2025, C-514/24, *Magyar Telekom* ("Nulltarif", GEREK-Leitlinien, Vorabentscheidungsersuchen)

EuGH SA 18.09.2025, C-188/24, *WebGroup Czech* (E-Commerce-RL, Herkunftslandprinzip)

- **Rechtsprechung des VfGH**

VfGH 25.06.2025, G71/2025 (Gesetzesbeschwerde, Nachrichtenüberwachung)

- **Rechtsprechung des VwGH**

VwGH 20.08.2025, Ra 2024/04/0321 (Ersatz der Beschwerdekosten, Revision)

VwGH 20.08.2025, Ra 2023/04/0260 (Zurückverweisung, Bindungswirkung)

VwGH 20.08.2025, Ra 2025/04/0049 (Parteienbezeichnung, Verantwortlichaustausch)

VwGH 21.08.2025, Ra 2025/04/0143; 21.08.2025, Ra 2025/04/0147 (Missbrauchsabsicht, Exzess)

- **Rechtsprechung des BVwG**

BVwG 29.07.2025, W211 2310137-1 (Auskunftsrecht, Negativauskunft, private Notizen)

BVwG 29.07.2025, W211 2294217-1 (Verjährung, Vorfrage, Antragsänderung)

BVwG 24.07.2025, W605 2256082-1 (Gesundheitsdaten, Vergleich, Erforderlichkeit, Beweis-erheblichkeit)

BVwG 28.07.2025, W211 2301653-1 (Videoüberwachung, berechnigte Interessen)

BVwG 23.07.2025, W298 2315584-1 (ORF-Beitrag)

- **EU-Rechtsakte**

Delegierte Verordnung (EU) 2025/1125

Durchführungsverordnung (EU) 2025/1126

Omnibusvorschriften für den Digitalbereich

## To the Point:

### Rechtsprechung des EuGH

EuGH SA 18.09.2025, C-526/24, *Brillen Rottler*

#### Auskunftsrecht, Missbrauchsabsicht, Schadenersatz

- Ein Betroffener meldete sich für den Newsletter eines Optikers an und erteilte seine Einwilligung zur Verarbeitung seiner Daten. Ungefähr zwei Wochen später richtete er ein Auskunftersuchen an den Optiker, der die Auskunft wegen Missbrauchsverdachts verweigerte.

Der Generalanwalt hat erwogen: Die Möglichkeit, einen Antrag als exzessiv abzulehnen, ist eine **Ausnahme**, die eng auszulegen ist. Um ein exzessives Auskunftersuchen abzulehnen, muss der Verantwortliche nachweisen, dass der Betroffene eine **Missbrauchsabsicht** verfolgt. Dazu sollte sich der Verantwortliche auf den Gegenstand des Auskunftersuchens, den zeitlichen Abstand zwischen der Einwilligung und dem Auskunftersuchen sowie die Tätigkeit, in deren Rahmen die Daten verarbeitet werden, stützen.

Es ist nicht ausgeschlossen, dass ein **erstes Auskunftersuchen exzessiv** ist. Aufgrund der grundlegenden Bedeutung des Auskunftsrechts, das es dem Betroffenen ermöglichen soll, seine übrigen DSGVO-Rechte auszuüben, müssen die Anforderungen hierfür jedoch hoch sein.

Den Betroffenen trifft zwar keine Begründungspflicht, die von ihm verfolgte Absicht muss aber nicht immer unberücksichtigt bleiben. Legitim ist ein Auskunftersuchen dann, wenn der Betroffene überprüfen will, ob der Verantwortliche seine Daten in zulässiger Weise verarbeitet. Außerdem ist das Auskunftsrecht erforderlich, um gegebenenfalls ein Recht auf Schadenersatz ausüben zu können.

**Missbrauchsabsicht** kann hingegen vorliegen, wenn der Betroffene die Absicht hat, den Verantwortlichen zur Ablehnung des Auskunftersuchens zu veranlassen, um von ihm die sofortige Zahlung einer Entschädigung zu verlangen, gegebenenfalls mit der Drohung, eine Schadenersatzklage zu erheben.

Allein der Umstand, dass der Betroffene öffentlich zugänglichen Informationen zufolge mehrfach Schadenersatzansprüche wegen Datenschutzverstößen geltend gemacht hat, reicht jedoch nicht aus, um eine Missbrauchsabsicht zu belegen. Art 82 DSGVO gewährt gerade das Recht, bei einem Verstoß gegen die DSGVO **Schadenersatz** zu verlangen, sodass die Wahrnehmung dieses Rechts nicht von vornherein als missbräuchlich angesehen werden kann.

Ein **schadensbegründendes Ereignis** kann bei jedem Verstoß gegen die DSGVO vorliegen, nicht nur bei einer unrechtmäßigen Datenverarbeitung. Art 82 Abs 1 DSGVO ist daher dahin auszulegen, dass auch Schäden ersatzfähig sind, die **nicht unmittelbar durch eine Verarbeitung personenbezogener Daten verursacht** wurden.

EuGH SA 18.09.2025, C-514/24, *Magyar Telekom*

#### "Nulltarif", GEREK-Leitlinien, Vorabentscheidungsersuchen

- Der EuGH hat in Urteilen aus den Jahren 2020 und 2021 klargestellt, dass sog. **"Nulltarif"-Klauseln** in Verträgen über **Internetzugangsdienste** mit der **VO (EU) 2015/2120** und dem darin normierten **Recht auf Zugang zum offenen Internet** unvereinbar sind. Eine nationale Aufsichtsbehörde forderte daraufhin **Telekommunikationsanbieter** auf, diese "Nulltarif"-Klauseln aus ihren Teilnehmerverträgen zu streichen. Fraglich ist, ob aufgrund der entsprechenden Änderung der Teilnehmerverträge den Nutzern gemäß Art 105 Abs 4 RL (EU) 2018/1972 (**europäischer Kodex für die elektronische Kommunikation; EKEK**) ein **Kündigungsrecht** ohne zusätzliche Kosten zukommt.

Der Generalanwalt hat erwogen: Die **"Nulltarif"-Klauseln** verstoßen unstreitig gegen Art 3 Abs 3 der VO (EU) 2015/2120 (**Gewährleistung des Zugangs zum offenen Internet**). Dies wurde vom EuGH allerdings erst nach Abschluss der verfahrensgegenständlichen Verträge klargestellt. Zum Zeitpunkt der Vertragsabschlüsse war die Ansicht vorherrschend, dass Optionen zum "Nulltarif" nicht generell ausgeschlossen sind. Dies wurde auch vom **Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK)** in seinen **Leitlinien** übernommen.

Bei der **zeitlichen Geltung** der **Vorabentscheidungsurteile** des EuGH ist auf den **Zeitpunkt des Inkrafttretens** des auslegenden Rechtsakts abzustellen. Die Vorabentscheidungsurteile sind **deklaratorischer Natur** und ändern nicht die Vorschriften, sondern legen sie nur aus. Die "Nulltarif"-Klauseln waren sohin seit Inkrafttreten der VO (EU) 2015/2120 mit dem Unionsrecht unvereinbar. Die **GEREK-Leitlinien** sind **nicht rechtsverbindlich**.

Den Telekomanbietern wurde die Änderung der Verträge durch keine Änderung des Unionsrechts vorgeschrieben, was gegen ein **kostenloses Kündigungsrecht** gesprochen hätte. Allerdings gelangt die gesamte Vorschrift des **Art 105 Abs 4 EKEK** zum (kostenlosen) Kündigungsrecht nicht zur

Anwendung, weil die Vertragsbedingungen nicht aus Eigeninitiative der Anbieter, sondern aufgrund der Aufforderung der nationalen Behörde erfolgten.

Die **Verantwortung** für die Aufnahme der "Nulltarif"-Klauseln in die Teilnehmerverträge liegt bei den **Anbietern**. Das kostenlose Kündigungsrecht kommt den Nutzern aufgrund anderer Rechtsgrundlagen zu. Dies aufgrund einer **verschuldensunabhängigen Haftung**, die durch den Umstand, dass die Klauseln den **GEREK-Leitlinien entsprachen, gemildert**, aber nicht aufgehoben wird. Nicht auszuschließen ist, dass die Nutzer andere Kosten als jene der Kündigung zu tragen haben.

Aus der weiteren Rechtsprechung des EuGH:

- Der in Art 2 lit h der [E-Commerce RL 2000/31/EG](#) definierte "**koordinierte Bereich**" ist weit zu verstehen. Er umfasst alle Anforderungen, die sich auf den Zugang zu und die Ausübung von **Diensten der Informationsgesellschaft** beziehen – unabhängig davon, ob sie aus dem Strafrecht stammen oder allgemeiner Natur sind. Entscheidend ist, dass sie sich auf das **Online-Angebot** beziehen. Die Pflicht zur **Altersverifikation** fällt in den koordinierten Bereich. Grundsätzlich darf daher nur das **Herkunftsland** Anforderungen an die Diensteanbieter stellen. Der Schutz der Menschenwürde und des **Kindeswohls** ist zwar ein hohes Gut, rechtfertigt aber keine generelle Abweichung von den Vorgaben der E-Commerce-Richtlinie. Abweichungen sind nur im Einzelfall zulässig. **Allgemeine, abstrakte Verpflichtungen** sind **unionsrechtswidrig** ([EuGH SA 18.09.2025, C-188/24, WebGroup Czech Republic und NKL Associates](#)).

### Rechtsprechung des VfGH

Aus der Rechtsprechung des VfGH:

- Eine **Gesetzesbeschwerde** ist nur dann zulässig, wenn eine Person **unmittelbar** und aktuell durch ein **verfassungswidriges Gesetz** in ihren Rechten verletzt wird und das Gesetz **ohne** gerichtliche **Entscheidung** oder **Bescheid** für sie wirksam wurde. Das Begehren auf Aufhebung mehrerer Bestimmungen der StPO (§§ 134 Z 3, 135 Abs 3, 140) zur Nachrichtenüberwachung sowie des EU-JZG (§§ 55a, 55d), welche die Zusammenarbeit bei strafrechtlichen Ermittlungen und den Austausch von Ermittlungsergebnissen zwischen EU-Mitgliedstaaten regeln, kann **nicht allein** mit **pauschalen Behauptungen** einer Rechtsverletzung begründet werden. Die bloße Überwachung von Chatverläufen und die Weiterleitung von Ermittlungsergebnissen an die Staatsanwaltschaft, die

daraufhin Untersuchungshaft beantragt, reichen zur Begründung einer unmittelbaren und aktuellen Betroffenheit nicht aus ([VfGH 25.06.2025, G71/2025 ua](#)).

### Rechtsprechung des VwGH

VwGH 20.08.2025, Ra 2024/04/0321

#### **Ersatz der Beschwerdekosten, Revision**

- Eine Arbeitnehmerin begehrte die Feststellung einer Verletzung ihres Grundrechts auf Datenschutz, weil das BVwG eine von ihr eingebrachte außerordentliche Revision irrtümlich an ihren Arbeitgeber, einen Gemeindeverband, übermittelte. Die Revision enthielt sensible Gesundheitsdaten. Der Gemeindeverband war im zugrundeliegenden Verfahren nicht Verfahrenspartei, hatte jedoch aus anderen Verfahren bereits Kenntnis von Teilen der übermittelten Informationen. Das BVwG stellte eine Verletzung des Rechts auf Geheimhaltung fest und sprach der Arbeitnehmerin den Ersatz der Beschwerdekosten in Höhe der Eingabegebühr zu. Weitere Anträge, insbesondere auf Schadenersatz und weitergehende Maßnahmen, wurden abgewiesen. Gegen dieses Erkenntnis erhob die Arbeitnehmerin ao Revision, die der VwGH ab- bzw zurückwies.

Der VwGH hat erwogen: Liegen **trennbare Absprüche** vor, ist die Zulässigkeit einer gegen diese erhobenen Revision jeweils getrennt zu prüfen.

Die Bestimmungen des § 85 GOG und § 78 AußStrG sind im Verfahren nach **Art 130 Abs 2a B-VG** anzuwenden. Die Übermittlung der Revision an einen nicht am Verfahren beteiligten Dritten ist eine datenschutzrechtliche Verarbeitung, der es an einer Rechtsgrundlage fehlt.

Der **Kostenersatz** beschränkt sich auf die notwendigen Beschwerdekosten, soweit diese ordnungsgemäß verzeichnet wurden. Ein weitergehender Ersatz, etwa für Vertretungskosten oder Schadenersatz, ist gemäß § 78 AußStrG nicht vorgesehen. Die Erteilung von Aufträgen an andere Gerichte kommt nur bei Erforderlichkeit in Betracht. Diese liegt nicht vor.

Die bloß pauschale **Aneinanderreihung von Rechtsfragen** ohne Bezugnahme auf den konkreten Sachverhalt erfüllt nicht die Anforderungen an die gesetzmäßige Ausföhrung einer ao Revision.

Aus der weiteren Rechtsprechung des VwGH:

- Die **Zurückverweisung** nach § 28 Abs 3 zweiter Satz VwGVG ist eine Ausnahme von der grundsätzlichen meritorischen Entscheidungszuständigkeit der Verwaltungsgerichte und ist nur bei krassen bzw besonders **gravierenden Ermittlungslücken** zulässig. Die **Bindungswirkung** an den

**Beschlussentwurf** der **federführenden Aufsichtsbehörde** besteht nur für die in Art 60 Abs 6 DSGVO **genannten Aufsichtsbehörden**. Sie gilt nicht für weitere Aufsichtsbehörden und auch nicht für das mittels gerichtlichen Rechtsbehelfs angerufene Gericht. Diese fehlende Bindungswirkung für das BVwG korreliert mit dem in Art 78 DSGVO verankerten **Recht auf einen wirksamen gerichtlichen Rechtsbehelf** gegen eine Aufsichtsbehörde. Eine Aufhebung und Zurückverweisung kann nicht auf eine Verletzung des Parteigehörs durch die belangte Behörde gestützt werden, da diese durch die Möglichkeit der Stellungnahme im Rechtsmittelverfahren saniert wird. Die DSGVO enthält keine Regelung, dass die Bindungswirkung gemäß Art 60 Abs 6 DSGVO beseitigt wäre, wenn das Gericht den Beschluss der Aufsichtsbehörde behebt. Eine derartige Bindungswirkung kann nur bei unveränderter Sach- oder Rechtslage bestehen ([VwGH 20.08.2025, Ra 2023/04/0260](#)).

- Die **Bezeichnung des Verantwortlichen** hat nach § 24 Abs 2 Z 2 DSG nur zu erfolgen, soweit dies dem Betroffenen zumutbar ist. Kann der Betroffene den Verantwortlichen nicht bestimmen, obliegt dessen Ermittlung der DSB. Wird die falsche Behörde als Verantwortliche bestimmt, ist der Bescheid ersatzlos zu beheben, da ein **Austausch der Person des Verantwortlichen** im verwaltungsgerichtlichen Verfahren nicht zulässig ist ([VwGH 20.08.2025, Ra 2025/04/0049](#)).
- Eine Datenschutzbeschwerde ist **missbräuchlich**, wenn sie zur Erzielung eines nicht durch die datenschutzrechtlichen Bestimmungen geschützten Zwecks (zB Publicity, Feindseligkeit, Sensationslust) erhoben wird, insb jedoch dann, wenn der Betroffene die Unrichtigkeit ihres Rechtsstandpunktes bewusst sein muss, etwa, weil sie dieselbe oder ähnliche Beschwerden bereits erfolglos erhoben hat. Die **Exzessivität** hängt nicht davon ab, ob die konkrete Beschwerde zu einer **Überlastung der Aufsichtsbehörde** führt, sodass die **Zahl der aktuell anhängigen Datenschutzbeschwerden** derselben Betroffenen irrelevant ist ([VwGH 21.08.2025, Ra 2025/04/0143](#), [21.08.2025, Ra 2025/04/0147](#)).

### **Rechtsprechung des BVwG**

[BVwG 29.07.2025, W211 2310137-1](#)

### **Auskunftsrecht, Negativauskunft, private Notizen**

- Ein Lehrer ersuchte die zuständige Personalvertretung um Auskunft über sämtliche zu seiner Person verarbeiteten Daten, insbesondere Protokolle und Aufzeichnungen

zu angeblichen Dienstrechtsverfehlungen und Mobbingvorwürfen. Die Personalvertretung erteilte eine Negativauskunft und erklärte, es gebe keine entsprechenden Protokolle oder systematisch gespeicherten Aufzeichnungen, sondern lediglich private, handschriftliche Notizen einzelner Mitarbeitender. Der Lehrer erhob daraufhin Datenschutzbeschwerde bei der DSB und behauptete, es sei ungläubwürdig, dass keine Aufzeichnungen existieren. Gegen den abweisenden Bescheid der DSB erhob der Lehrer (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Das Recht auf Auskunft nach Art 15 DSGVO verpflichtet den Verantwortlichen, Auskunft über tatsächlich verarbeitete personenbezogene Daten zu erteilen. Wird keine Verarbeitung vorgenommen, ist eine **Negativauskunft** ausreichend. Die Auskunftspflicht bezieht sich nur auf Daten, die im Zeitpunkt des Einlangens des Auskunftersuchens verarbeitet werden. Im Fall einer nichtautomatisierten Verarbeitung muss es sich um die Verarbeitung personenbezogener Daten handeln, die in einem **Dateisystem** gespeichert sind oder gespeichert werden sollen. Ein Dateisystem ist nach der Definition des Art 4 Z 6 DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird. Einzelne **handschriftliche Notizen** von Mitarbeitenden weisen nicht das Kriterium eines **formellen Ordnungsschemas** einer strukturierten Sammlung auf. Sie fallen demnach nicht in den Anwendungsbereich der DSGVO. Die Negativauskunft wurde – wenn auch verspätet – vollständig erteilt. Ein **Anspruch auf Feststellung** der Verspätung besteht nicht.

[BVwG 29.07.2025, W211 2294217-1](#)

### **Verjährung, Vorfrage, Antragsänderung**

- Ein Bezieher der **Berufsunfähigkeitspension** wurde von Mitarbeitern der **PVA** im Jahr 2019 im privaten Lebensbereich gefilmt und fotografiert, um einen unberechtigten Bezug der Berufsunfähigkeitspension nachzuweisen. Im Jahr 2024 erhob der Pensionsbezieher Datenschutzbeschwerde an die DSB. Diese wies die Datenschutzbeschwerde als verfristet zurück. Dagegen erhob der Pensionsbezieher (erfolglose) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: "Sache" eines Beschwerdeverfahrens vor dem BVwG ist im Fall eines Rechtsmittels gegen einen zurückweisenden Bescheid ausschließlich die Frage der **Rechtmäßigkeit der Zurückweisung**.

Der Anspruch auf Behandlung einer Beschwerde erlischt nach der **Präklusivfrist** des § 24 Abs 4 DSGVO nach einem Jahr ab Kenntnis von dem beschwerenden Ereignis (**subjektive Frist**), längstens aber binnen drei Jahren, nachdem das behauptete Ereignis stattgefunden hat (**objektive Frist**). Diese Frist ist von Amts wegen zu beachten.

Bei in der Vergangenheit angefertigten Bild- und Videoaufnahmen beginnt die objektive dreijährige Frist mit der **Erstellung der Aufnahmen** zu laufen. Die subjektive Frist des § 24 Abs 4 DSGVO verlangt "**Kenntnis**" über die Tatsache der Datenverarbeitung und die **persönliche Betroffenheit**. Es kommt nicht darauf an, ob sich der Betroffene erst später rechtlich mit dem Sachverhalt auseinandergesetzt hat.

Ein **sozialrechtliches (Ermittlungs-)Verfahren** ist keine Vorfrage zur Prüfung einer möglichen Datenschutzverletzung.

[BVwG 24.07.2025, W605 2256082-1](#)

#### **Gesundheitsdaten, Vergleich, Erforderlichkeit, Beweiserheblichkeit**

- Nach einer Operation griff ein Chirurg trotz Beendigung des Behandlungsvertrags mit seinem Patienten mehrfach auf die **Patientendokumentation** zu und verwendete diese (Angaben zu Medikamenteneinnahmen, Depressionen, Schlafstörungen, etc) für Schriftsätze im zivilrechtlichen Schadenersatzprozess. Zwar schlossen die beiden einen Vergleich, der Patient erachtete sich aber dennoch in seinem Recht auf Geheimhaltung verletzt und erhob Datenschutzbeschwerde bei der DSB. Diese gab der Datenschutzbeschwerde statt. Der Chirurg erhob (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Den **Vergleichsumfang** und damit die Grenzen der Bereinigungswirkung bestimmen die Parteien. Mit dem geschlossenen Vergleich wurden jene wechselseitigen Ansprüche beglichen, die konkret aus der Operation resultierten. Wenngleich die **Datenverarbeitung** durch den Chirurg mit dem Schadenersatzprozess in einem engen Zusammenhang stand, ist sie **keine unmittelbare Vorfallsfolge**. Auch angesichts der Feststellung der Datenschutzverletzung war der Vergleichsumfang nicht so auszulegen, dass dieser Anspruch ebenfalls mitbereinigt werden sollte.

Die Ausnahmeregelung des Art 9 Abs 2 lit h DSGVO erlaubt die Verarbeitung von **Gesundheitsdaten** für bestimmte "**Gesundheitsleistungen**". Die Datenverarbeitung muss auf Unionsrecht, innerstaatlichem Recht oder einem Vertrag mit einem Angehörigen eines Gesundheitsberufs beruhen. Zusätzlich sind die in **Art 9 Abs 3 DSGVO** genannten Bedingungen und Garantien

einzuhalten. Da der Chirurg zum Zeitpunkt der Einsichtnahme nicht mehr behandelnder Arzt war, erfolgte die Verarbeitung weder mit Einverständnis des Patienten noch zu einem von der Bestimmung gedeckten Zweck.

Gemäß Art 9 Abs 2 lit f DSGVO kann die Verarbeitung sensibler Daten bei der **Geltendmachung oder Verteidigung von Rechtsansprüchen** rechtmäßig erfolgen, soweit sie erforderlich ist. Die Erforderlichkeit ist aus einer **ex-ante-Sicht** zu beurteilen. Zudem bedarf die Einbeziehung sensibler Daten einer **plausiblen Begründung der Beweiserheblichkeit**. Im Zweifel ist eine **Interessenabwägung** durchzuführen. Erforderlichkeit ist gegeben, wenn die Information für die gerichtliche Entscheidung zwingend notwendig ist. Eine **bloße Zweckdienlichkeit** reicht jedenfalls nicht aus und auch das **Ansinnen einer "bestmöglichen Effizienz"** macht die Datenverarbeitung noch nicht zu einer erforderlichen. Da gelindere Mittel wie die zeugenschaftliche Einvernahme des Patienten oder ein Antrag auf Vorlage von Urkunden zur Verfügung standen, lag keine Erforderlichkeit vor. Zwar bestand ein rechtlicher Konflikt, jedoch **kein Beweisnotstand**, weil nicht schon das allgemeine Interesse jeder Partei, über ein besonders beweiskräftiges Beweismittel zu verfügen, ausreicht.

#### Aus der weiteren Rechtsprechung des BVwG:

- Eine **Videoüberwachung** kann nach Art 6 Abs 1 lit f DSGVO zulässig sein, wenn sie der Wahrung berechtigter Interessen dient. Das Interesse am **Schutz des Eigentums** ist ein berechtigtes Interesse. Die kontinuierliche Videoüberwachung einer Zufahrtsstraße mit einer **Dienstbarkeit** und der Personen, die diese rechtmäßig nutzen – über das eigene Grundstück hinaus – ist jedoch nicht erforderlich und verletzt den **Grundsatz der Datenminimierung** ([BVwG 28.07.2025, W211 2301653-1](#))
- Aus dem **ORF-Beitrags-Gesetz 2024** sind sowohl die zu verarbeitenden Datenarten als auch der Zweck eindeutig zu erkennen. Es bestehen auch keine verfassungsrechtlichen Bedenken im Hinblick auf die Berechtigung der ORF-Beitrags Service GmbH zur Verarbeitung personenbezogener Daten ([BVwG 23.07.2025, W298 2315584-1](#)).

#### EU-Rechtsakte

- Am **15.09.2025** ist die "**Delegierte Verordnung (EU) 2025/1125 der Kommission vom 5. Juni 2025 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung der Informationen in einem Antrag auf**

Zulassung zum öffentlichen Angebot vermögenswertereferenzierter Token oder ihre Zulassung zum Handel", [ABI L 2025/1125](#), kundgemacht worden. Mit dieser **DelegiertenVO** ergänzt die Kommission die "VO (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über **Märkte für Kryptowerte [...]**" (kurz: **MiCAR**) und **präzisiert** die **anzugebenden Informationen** in einem **Antrag auf Zulassung** zum öffentlichen Angebot **vermögenswertereferenzierter Token**.

- Am **15.09.2025** ist die "**Durchführungsverordnung** (EU) 2025/1126 der Kommission vom 5. Juni 2025 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates im Hinblick auf die Festlegung von Standardformularen, Mustertexten und Verfahren für die in den Antrag auf Zulassung zum öffentlichen Angebot vermögenswertereferenzierter Token und ihre Zulassung zum Handel aufzunehmenden Informationen", [ABI L 2025/1126](#), kundgemacht worden. Auch diese **DurchführungsVO** wurde auf Grundlage der **MiCAR** erlassen und enthält Standardformulare, Mustertexte sowie Verfahren für den **Antrag auf Zulassung** zum öffentlichen Angebot **vermögenswertereferenzierter Token**.
- Am **16.09.2025** hat die Kommission einen **Call for evidence** (Einholung von Erkenntnissen/Stellungnahmen) betreffend **Omni-busvorschriften für den Digitalbereich**, [Ares\(2025\)7724296](#), veröffentlicht. Die Kommission möchte die Vorschriften für **Daten, Cybersicherheit** und **künstliche Intelligenz** vereinfachen. Stellungnahmen können bis zum 14.10.2025 abgegeben werden.



to the point

# Datenschutzmonitor. 39/2025 vom 01.10.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH SA 25.09.2025, C-474/24, *NADA* (Doping, Gesundheitsdaten, strafrechtliche Daten)

- **Rechtsprechung der Justiz**

OGH 09.09.2025, 10b91/25a (COFAG, abgabenrechtliche Geheimhaltungspflicht)

OLG Wien 13.09.2025, 16R92/25d (Auskunft, Prozessposition, Geschäftsgeheimnis)

- **Rechtsprechung des BVwG**

BVwG 13.08.2025, W291 2272970-1 (Cookie-Banner, Pay or Okay, Medien)

BVwG 29.07.2025, W211 2307081-1 (Kriminalpolizei, Sozialversicherungsdaten, Verhältnismäßigkeit)

BVwG 24.07.2025, W101 2163119-1 (Bürgerumfrage, Meldebehörde, zeitlicher Anwendungsbereich)

BVwG 24.07.2025, W101 2315598-1 (Säumnisbeschwerde, Entscheidungsfrist, Zurückweisung)

BVwG 28.07.2025, W254 2308986-1 (Beschreibungsbeschwerde, Zurückweisung)

- **Nationale Rechtsakte**

Resilienz kritischer Einrichtungen-Gesetz (RKEG)

Politische-Werbung-Gesetz (Pol-W-G)

## To the Point:

### Rechtsprechung des EuGH

EuGH SA 25.09.2025, C-474/24, *NADA*

#### **Doping, Gesundheitsdaten, strafrechtliche Daten**

- Die Namen und weitere Daten mehrerer Sportler, die des Dopings überführt wurden und von der wettkampfmäßigen Sportausübung gesperrt worden sind, wurden auf der Webseite der Nationalen Anti-Doping Agentur Austria GmbH (**NADA**) und der Österreichischen Anti-Doping Rechtskommission (**ÖADR**) veröffentlicht. Auf der Webseite der ÖADR wurde zusätzlich die verwendete Dopingsubstanz veröffentlicht. Da von der Veröffentlichung auch Gesundheitsdaten und Informationen zu Straftaten umfasst waren, reichten mehrere Sportler eine gemeinsame (erfolglose) Datenschutzbeschwerde bei der DSB ein. Das daraufhin angerufene BVwG legte dem EuGH mehrere Fragen hinsichtlich der Vereinbarkeit von Anti-Doping-Regelungen mit der DSGVO vor.

Der Generalanwalt hat erwogen: Die in Art 2 Abs 2 lit a DSGVO vorgesehene Ausnahme vom Anwendungsbereich der DSGVO ist **eng auszulegen**. Weder die Zuständigkeit der Mitgliedstaaten für den Sport noch der fehlende wirtschaftliche Charakter der Dopingbekämpfung rechtfertigen eine Ausnahme, weshalb die DSGVO auch für die Veröffentlichung von Sperrlisten durch NADA/ÖADR gilt.

Sowohl Daten über physische und psychische **Erkrankungen** als auch Daten zu **Krankheitsrisiken** zählen zu den **Gesundheitsdaten** nach der DSGVO. Daten, die Aufschluss über ein Krankheitsrisiko geben, sind zB Informationen zu übermäßigem Alkohol-, Tabak- oder Drogenkonsum.

Die Information über die verwendete Dopingsubstanz lässt einen Rückschluss auf ein zukünftiges Krankheitsrisiko zu. Die Nennung von Namen, Dauer und Gründen einer Sperre ist nur **in Kombination** mit der Dopingsubstanz ein Gesundheitsdatum nach Art 9 Abs 1 DSGVO. Wird nur die Sperre wegen Dopings, ohne Nennung der genutzten Substanz, veröffentlicht, liegt regelmäßig **kein Gesundheitsdatum** vor.

Die Beurteilung, ob Daten iSd Art 10 DSGVO strafrechtlicher Natur sind, erfolgt nach den vom EGMR entwickelten "**Engel-Kriterien**". Bewertet wird dabei die Zuwiderhandlung im innerstaatlichen Recht, die Art der Zuwiderhandlung und der Schweregrad der drohenden Sanktion.

Verstöße gegen Anti-Doping-Regelungen von Sportverbänden sind grundsätzlich **disziplinarrechtlicher** Natur. Unter bestimmten Umständen, insbesondere bei

**repressiver Zielsetzung** und erheblichem **Schweregrad** der Sanktion, wie dies bei einem lebenslangen Ausschluss von der Wettbewerbsteilnahme der Fall ist, kann die Sanktion jedoch als strafrechtlich iSd Art 10 DSGVO qualifiziert werden. Die Tätigkeit oder Entscheidung von Behörden, sohin auch der NADA/ÖADR, die mit der Aufsicht über die Verarbeitung von Daten zu strafrechtlichen Verurteilungen und Straftaten betraut sind, muss einer **gerichtlichen Kontrolle** zugänglich sein.

Die Veröffentlichung der Namen, Sperrdauer und Gründe muss **verhältnismäßig** sein und darf nicht automatisch und unbegrenzt erfolgen. Vor der Veröffentlichung braucht es eine Interessenabwägung im Einzelfall zwischen dem öffentlichen Interesse und den Persönlichkeitsrechten der Betroffenen. Die Veröffentlichung ist nur zulässig, wenn keine weniger eingriffsintensiven Alternativen bestehen.

Eine Datenschutzbeschwerde, die auf das Recht auf Löschung nach Art 17 DSGVO gestützt ist, kann nicht gegen eine **zukünftige Datenverarbeitung**, auch wenn diese unmittelbar bevorsteht, geltend gemacht werden. **Anm: Die Rechtsfragen dieses Vorabentscheidungsverfahrens wurden im ersten Rechtsgang zurückgewiesen, weil die vorliegende (österreichische) Behörde kein "Gericht" iSd Art 267 AEUV war (EuGH 07.05.2024, C-115/22, NADA). Daraufhin hat das BVwG, nach Hinzufügen einer weiteren Rechtsfrage, dieselben Rechtsfragen erneut vorgelegt. Über die Zurückweisung durch den EuGH haben wir im Schönherr Datenschutzmonitor vom 15.05.2024 berichtet. Über die erneute Vorlage durch das BVwG haben wir im Schönherr Datenschutzmonitor vom 17.07.2024 berichtet.**

### Rechtsprechung der Justiz

Aus der Rechtsprechung der Justiz:

- Das Finanzamt durfte **Ergänzungsgutachten** und die dem Gutachten **zugrundeliegenden Unterlagen** der COFAG übermitteln. Die **abgabenrechtliche Geheimhaltungspflicht** gemäß § 48a BAO stand der Übermittlung dieser Unterlagen nicht entgegen (OGH 09.09.2025, 10b91/25a). **Beachte: Auch die abgabenrechtliche Geheimhaltungspflicht ist im Zuge der Abschaffung der Amtsverschwiegenheit und der Einführung der Informationsfreiheit aufgeweicht worden.**
- Die DSGVO bietet keine Anhaltspunkte dafür, dass das Auskunftsrecht zwecks **Stärkung** der eigenen **Position in einem Rechtsstreit** verweigert werden dürfte. Aus einer Geschäftsbeziehung stammende Daten sind nicht geheim, weil sie **gemeinsame Daten** sind. Dies gilt auch dann,

wenn der Auskunftswerber zum Zeitpunkt des Auskunftersuchens auf seine Daten nicht mehr zugreifen kann. Solche "gemeinsame" Daten unterliegen **keinem Geschäftsgeheimnis** ([OLG Wien 13.09.2025, 16R92/25d](#)).

### Rechtsprechung des BVwG

BVwG 13.08.2025, W291 2272970-1

#### **Cookie-Banner, Pay or Okay, Medien**

- Ein Nutzer besuchte die Website mehrerer Medienunternehmen, auf der journalistische Inhalte und Nutzerinteraktionen angeboten wurden. Beim erstmaligen Aufruf der Website wurde ein Cookie-Banner angezeigt, über den der Nutzer entweder in Cookies für Webanalyse und digitale Werbemaßnahmen einwilligen oder ein kostenpflichtiges, werbefreies Abonnement abschließen konnte. Der Nutzer willigte in die Datenverarbeitung ein, woraufhin Cookies gesetzt und personenbezogene Daten wie IP-Adresse, Cookie-Kennungen, Browserdaten und TC-String verarbeitet und an Drittanbieter übermittelt wurden. Der Nutzer erhob Datenschutzbeschwerde bei der DSB. Die DSB gab der Datenschutzbeschwerde teilweise statt und stellte fest, dass die Medienunternehmen gegen den Grundsatz der Rechtmäßigkeit verstoßen und den Nutzer damit im Recht auf Geheimhaltung verletzt hätten. Darüber hinaus wies sie die Medienunternehmen an, den Datenbestand dahingehend zu überprüfen, ob näher bezeichnete Cookie-Werte und Browserdaten noch verarbeitet werden und bejahendenfalls entsprechende Cookie-Werte zu löschen. Die Anträge auf Untersagung der relevanten Verarbeitungsvorgänge sowie auf Verhängung einer Geldbuße wurden zurückgewiesen. Der Nutzer und die Medienunternehmen erhoben Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Der TC-String sowie die IP-Adresse und andere Kennungen wie Browserdaten und Cookie-Kennungen sind personenbezogene Daten, weil sie die **Identifizierung** des Nutzers ermöglichen.

Da die Medienunternehmen darüber entschieden haben, welche Unternehmen über ihr Onlineportal Cookies setzen können, sind sie **Verantwortliche**.

Obwohl die Medienunternehmen journalistisch tätig sind, greift das **Medienprivileg** des Art 85 DSGVO und § 9 DSG nicht. Denn die Datenverarbeitung *per se* liefert keinen Beitrag zu einer Debatte von allgemeinem Interesse, sondern dient ausschließlich der Erwirtschaftung von Werbeeinnahmen oder der Markenbekanntheit.

Die Rechtsvertretung des Nutzers erfüllt die Kriterien des Art 80 Abs 1 DSGVO. Das **Fehlen einer Verbandsklagebefugnis** in

Österreich hindert Mitglieder bzw Mitarbeiter eines Vereins nicht daran, individuell Beschwerden einzubringen. Dass es im Zuge der Beschwerdeerhebung zu umfangreichen vorbereitenden Tätigkeiten der Rechtsvertretung des Nutzers gekommen sein mag, ist den komplexen, technischen Gegebenheiten geschuldet. Ein rechtsmissbräuchliches Verhalten kann daraus nicht erkannt werden.

Zentrales Kriterium für eine freiwillige **Einwilligung** ist die **Granularität**. Diese fehlt, weil der Nutzer nur **pauschal** in ein **Bündel an Verarbeitungszwecken** (Webanalyse, Website-Optimierung, personalisierte Werbung, Social-Media-Plug-ins) einwilligen konnte. Eine differenzierte Auswahl war nicht möglich, sodass der Nutzer nicht frei wählen konnte, welchen Zwecken er zustimmen möchte. Auch der vermeintlich enge Zusammenhang zwischen Website-Optimierung und Werbemaßnahmen rechtfertigt keine pauschale Einwilligung. Für den Nutzer ist auch nicht ersichtlich, dass es sich um einen einzigen Zweck handeln sollte. Wird eine betroffene Person nicht hinreichend über alle Umstände iZm einer Datenverarbeitung, einschließlich des Verarbeitungszwecks und der Datenempfänger informiert, steht dies der Erteilung einer **"informierten" Einwilligung** entgegen, was zur **Rechtswidrigkeit dieser Verarbeitung** führt. Selbst wenn von einem einzigen Zweck ausgegangen werden könnte, wäre der Nutzer nicht ausreichend über die Verarbeitungszwecke informiert worden.

Ein Vorgehen, bei dem nicht einmal versucht wird, die Vorgaben hinsichtlich der Granularität einzuhalten und bei dem eine "Pauschaleinwilligung" einer kostenpflichtigen Abonnement-Variante gegenübergestellt wird, kann **kein angemessener Ausgleich** der Grundrechte nach Art 8 und 16 GRC sein. Wirtschaftliche Interessen rechtfertigen nicht, für unterschiedliche Verarbeitungsvorgänge keine gesonderten Einwilligungen einzuholen. Die **pauschale Gesamteinwilligung** in verschiedene Zwecke ist unwirksam.

Auch das **Setzen oder Auslesen von Cookies** erfordert gemäß § 165 Abs 3 TKG 2021 eine gültige Einwilligung. Da die Einwilligung unwirksam war, war die darauffolgende Datenverarbeitung unrechtmäßig.

Die Bewertung der Einwilligung als unwirksam sowie die Anordnung der Datenlöschung durch die DSB waren rechtmäßig. Rechtswidrig war hingegen die **pauschale Zurückweisung** des Antrags auf ein **Verarbeitungsverbot** ohne inhaltliche Prüfung. Die DSB hätte prüfen müssen, ob die Löschanordnung ausreicht, um dem Verstoß abzuwehren oder ob eine andere in Art 58 Abs 2 DSGVO vorgesehene Maßnahme geeignet, erforderlich und

verhältnismäßig ist. Zudem hätte sie das Ergebnis ihrer Prüfung **nachvollziehbar darlegen müssen**. Dies kann vom BVwG nicht saniert bzw nachgeholt werden, weil es aufgrund einer gegen einen Zurückweisungsbescheid erhobenen Bescheidbeschwerde nur über die Rechtmäßigkeit der Zurückweisung entscheiden darf.

BVwG 29.07.2025, W211 2307081-1

### **Kriminalpolizei, Sozialversicherungsdaten, Verhältnismäßigkeit**

- Die Polizei fragte für ein strafrechtliches Ermittlungsverfahren wegen Eigentumsdelikten die Sozialversicherungsdaten von Beschuldigten über die Online-Zugriffsmöglichkeit des Dachverbandes der Sozialversicherungsträger ("**AJ-WEB**") ab, nachdem sich diese weigerten, Angaben zu ihrem Beruf oder ihrer Erwerbstätigkeit zu machen. Die Beschuldigten erhoben Datenschutzbeschwerden, weil sie die Abfrage für nicht erforderlich und unverhältnismäßig hielten. Die DSB wies die Datenschutzbeschwerden ab. Dagegen richteten sich die (erfolglosen) Bescheidbeschwerden der Beschuldigten an das BVwG.

Das BVwG hat erwogen: Die polizeiliche Abfrage der **Sozialversicherungsdaten** im Ermittlungsverfahren ist nach § 74 Abs 1 StPO iVm § 38 DSGVO zulässig, wenn sie zur Erfüllung der kriminalpolizeilichen Aufgaben erforderlich und verhältnismäßig ist. Die **Kriminalpolizei** ist nach § 76 Abs 1 StPO berechtigt, zur Wahrnehmung ihrer Aufgaben Auskünfte von **öffentlichen Stellen** einzuholen. Da die Beschuldigten im Ermittlungsverfahren keine Angaben zu ihrer Erwerbstätigkeit machten, war die Abfrage der Sozialversicherungsdaten zur Feststellung des Berufs und zur Erfüllung der gesetzlichen Verpflichtungen (zB Verständigung der **Dienstbehörde** bei Beamten, § 76 Abs 5 StPO) erforderlich und nicht überschießend. Die **Grundsätze der Datenminimierung** und **Verhältnismäßigkeit** wurden eingehalten, weil die Polizei zunächst die Beschuldigten befragte und erst nach deren Weigerung die Datenabfrage vornahm. Die Verarbeitung stützte sich auf eine gesetzliche Grundlage und war für die Aufklärung des Sachverhalts sowie die Erfüllung strafprozessualer Nebenpflichten erforderlich.

BVwG 24.07.2025, W101 2163119-1

### **Bürgerumfrage, Meldebehörde, zeitlicher Anwendungsbereich**

- Der Bürgermeister einer Stadt erhob personenbezogene Daten (Name, Geburtsdatum, Staatsangehörigkeit, Adresse) aus dem lokalen Melderegister, um eine Bürgerumfrage durchzuführen. Dazu versendete er

Informationsschreiben mit individualisierten Teilnahmecodes und Fragebögen an die Bürger der Stadt. Ein Bürger erachtete sich in seinem Geheimhaltungsrecht verletzt und erhob eine erfolgreiche Datenschutzbeschwerde im Jahr 2016. Gegen den Bescheid der DSB erhob der Bürgermeister eine Bescheidbeschwerde. Nach mehreren Instanzenzügen, einschließlich einer Aufhebung durch den VwGH, war das BVwG erneut mit der Sache befasst und gab der Bescheidbeschwerde statt.

Das BVwG hat erwogen: Bei der Beurteilung der Rechtmäßigkeit eines – vor Inkrafttreten der DSGVO am 25.05.2018 – abgeschlossenen Vorgangs einer möglichen Datenschutzverletzung des Rechts auf Geheimhaltung ist die **alte Rechtslage** nach dem DSG 2000 anzuwenden. Eine Stadt ist als **Meldebehörde** gemäß § 20 Abs 3 Meldegesetz berechtigt, Meldedaten zu verwenden, sofern dies zur Wahrnehmung **gesetzlich übertragener Aufgaben** erforderlich ist.

Die **Informationspflicht** nach § 70 des Stadtstatuts, nach der die Einwohner über ein konkretes Vorhaben der Stadt ausreichend und zeitgerecht, möglichst noch im Planungsstadium, zu informieren waren, war eine solche **gesetzlich übertragene Aufgabe**. Die Versendung von persönlich adressierten Informationsschreiben und Fragebögen an Einwohner war erforderlich, um die Zielgruppe umfassend zu erreichen und eine effektive Partizipation (Teilnahmecode) an der Bürgerumfrage zu ermöglichen. Die Verarbeitung der personenbezogenen Daten war durch die gesetzliche Grundlage gedeckt und wahrt die datenschutzrechtlichen Grundsätze der **Erforderlichkeit** und **Verhältnismäßigkeit**. Ein schutzwürdiges Geheimhaltungsinteresse des Bürgers ist nicht verletzt.

Aus der weiteren Rechtsprechung des BVwG:

- Eine **Säumnisbeschwerde** kann erhoben werden, wenn die DSB nicht innerhalb von **sechs Monaten** entscheidet. Liegt zum Zeitpunkt des Einbringens der Säumnisbeschwerde **keine Säumnis** vor, weil die **Entscheidungsfrist** von sechs Monaten noch nicht verstrichen ist, ist die Säumnisbeschwerde unzulässig und ist **zurückzuweisen** (BVwG 24.07.2025, W101 2315598-1).
- Die **Bescheidbeschwerde** ist mangelhaft, wenn ihr nicht einmal eine Andeutung darüber entnommen werden kann, worin die Unrichtigkeit des angefochtenen Bescheids bestehen soll. Die Bescheidbeschwerde enthält insb **keine Gründe**, auf die sich die Behauptung der Rechtswidrigkeit stützt. Sie ist auch ohne "übertriebenen Formalismus" als unzulässig zu werten und

zurückzuweisen ([BVwG 28.07.2025, W254 2308986-1](#)).

### **Nationale Rechtsakte**

- Am **24.09.2025** hat der **Nationalrat** die **Regierungsvorlage** über das "**Resilienz kritischer Einrichtungen-Gesetz**" (**RKEG**) mit Zweidrittelmehrheit [angenommen](#). Das RKEG wird die RL (EU) 2022/2557 (**RKE-RL**) ins innerstaatliche Recht umsetzen. Zielsetzung ist **der Schutz zentraler Infrastrukturen** vor physischen Bedrohungen.
- Am **19.09.2025** ist der **Ministerialentwurf** betreffend das "*Bundesgesetz, mit dem ein Bundesgesetz über die **Transparenz und das Targeting politischer Werbung** erlassen wird und das KommAustria-Gesetz sowie das Mediengesetz geändert werden*", [Politische-Werbung-Gesetz \(Pol-W-G\)](#), an den Nationalrat übermittelt worden. Mit dem Pol-W-G soll die "[VO \(EU\) 2024/900 über die Transparenz und das Targeting politischer Werbung](#)" ins innerstaatliche Recht durchgeführt werden. Diese VO ist ab dem **10.10.2025** unmittelbar anzuwenden.

to the point

# Datenschutzmonitor. 40/2025 vom 08.10.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuG**

EuG 01.10.2025, T-384/20 RENV, *OC/Kommission* (OLAF, Pressemitteilung, Unschuldsumutung, Schadenersatz)

- **Rechtsprechung des VwGH**

VwGH 02.09.2025, Ro 2023/04/0027 (Finanzprokurator, Verantwortliche, Aufwändersatz)

- **Rechtsprechung der Justiz**

OLG Graz 20.08.2025, 10Bs215/25f (Datenschutzverletzung, unbedeutende Schädigung, Diversion)

- **Rechtsprechung des BVwG**

BVwG 07.08.2025, W605 2289883-1 (KKE, Löschungsersuchen, Sanierung)

BVwG 23.07.2025, W101 2255209-1 (Untersuchungsausschuss, Mandatsbescheid)

BVwG 05.08.2025, W137 2308681-1; 05.08.2025, W137 2310023-1 (Entscheidungspflicht, Kohärenzverfahren, Hemmung)

BVwG 01.08.2025, W605 2308677-1 (Kohärenzverfahren, Untätigkeitsklage, Hemmung)

BVwG 06.08.2025, W256 2279237-1 (Tod, Parteistellung)

BVwG 05.08.2025, W137 2308027-1 (Beschwer, Schadenersatz, Zuständigkeit)

BVwG 29.07.2025, W211 2311353-1 (Zurückweisung, Parteistellung, Bescheidzustellung)

- **Rechtsprechung der LVwG**

LVwG NÖ 24.09.2025, LVwG-AV-1085/001-2025 (Auskunftsanspruch, IFG)

- **EU-Rechtsakte**

DelegierteVO (EU) 2025/1264 zur MiCAR  
Fünf DurchführungsVOs zur eIDAS-VO

- **Nationale Rechtsakte**

Bundesgesetz zur Änderung des SNG, SPG, TKG, BVwGG und RStDG (Bundestrojaner)

## To the Point:

### Rechtsprechung des EuG

EuG 01.10.2025, T-384/20 RENV, OC/Kommission

#### **OLAF, Pressemitteilung, Unschuldsvermutung, Schadenersatz**

- Eine Wissenschaftlerin stellte beim Europäischen Forschungsrat den Antrag auf Förderung eines bestimmten Forschungsprojekts. Die EU-Kommission gewährte der betreffenden griechischen Universität die Förderung im Rahmen eines Fördervertrags, den sie mit einem Höchstbetrag dotierte. Nach Abrechnung der Fördergelder kam es zu einer Finanzüberprüfung durch den Europäischen Forschungsrat. Aufgrund vermeintlicher Unregelmäßigkeiten in der Finanzgebarung erstattete der Europäische Forschungsrat Anzeige an das Europäische Amt für Betrugsbekämpfung (**OLAF**), welches eine **Pressemitteilung** darüber auf seiner Website veröffentlichte. Diese enthielt zwar nicht den Namen, aber das Alter, die Staatsangehörigkeit und das Geschlecht der Wissenschaftlerin sowie die Höhe der gewährten Förderungen.

Die Wissenschaftlerin erhob Klage und begehrte Ersatz ihres durch die Veröffentlichung der Pressemitteilung entstandenen **immateriellen Schadens** iHv **EUR 1,1 Mio**. Sie berief sich auf die DSGVO, den in Art 6 Abs 2 EMRK festgelegten Grundsatz der Unschuldsvermutung sowie den in Art 41 GRC normierten Grundsatz der Verhältnismäßigkeit. Die Wissenschaftlerin argumentierte, die Pressemitteilung hätte falsche, irreführende und vertrauliche Informationen enthalten, deren Veröffentlichung weder angemessen noch zur Information der Allgemeinheit erforderlich gewesen sei.

Das EuG hat erwogen: Die personenbezogenen Daten der Klägerin wurden vom OLAF zum Zweck der Betrugsbekämpfung erhoben. Die daran anschließende Veröffentlichung ist konsequenterweise als separater Vorgang, nämlich als **Weiterverarbeitung**, zu qualifizieren. Die Veröffentlichung der Staatsangehörigkeit und des Alters der Wissenschaftlerin in der Pressemitteilung ist ein schwerwiegender Verstoß gegen den Grundsatz der Rechtmäßigkeit, den das OLAF zu verantworten hat. Dieser Verstoß kann eine Haftung der Europäischen Union gemäß Art 340 Abs 2 AEUV begründen. Ferner suggerierte die Pressemitteilung durch Verwendung des Begriffs "Betrug" eine strafgerichtliche Verurteilung, der ein Schuldurteil zugrunde liegen würde. Dies war mit dem in Art 6 Abs 2 EMRK verbrieften **Grundsatz der Unschuldsvermutung** nicht vereinbar und verstieß gegen die **Neutralitäts- und Unparteilichkeitspflicht** des OLAF. Der Wissenschaftlerin

sind daher **EUR 50.000** an immateriellem Schadenersatz zuzusprechen. **Anm: Im ersten Rechtsgang wies das EuG die Schadenersatzklage ab, weil es die Identifizierbarkeit der Wissenschaftlerin anhand der veröffentlichten Daten verneinte. Der EuGH hob dieses Ersturteil auf, weil er der Ansicht war, dass die Wissenschaftlerin anhand öffentlich zugänglicher Informationen mit einem verhältnismäßigen Aufwand von Journalisten identifiziert werden konnte (siehe zum Urteil des EuGH: [Schönherr Daten-schutzmonitor 17/2024 vom 03.05.2024](#)).**

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Die **Finanzprokurator** ist als Einrichtung des Bundes **Verantwortliche des öffentlichen Bereichs** iSd § 26 Abs 1 Z 1 DSG. Grundsätzlich hat sie daher Anspruch auf **Aufwandersatz** im Verfahren vor dem VwGH. Die Revisionsbeantwortung der Finanzprokurator wurde jedoch von keinem bevollmächtigten Rechtsanwalt eingebracht, sondern die Finanzprokurator ist **in eigener Sache** eingeschritten. Mangels Vertretung durch einen Rechtsanwalt kommt kein Ersatz des Schriftsatzaufwands in Betracht ([VwGH 02.09.2025, Ro 2023/04/0027](#)).

### Rechtsprechung der Justiz

OLG Graz 20.08.2025, 10Bs215/25f

#### **Datenschutzverletzung, unbedeutende Schädigung, Diversion**

- Eine Bedienstete der Einlaufstelle eines BG fragte ohne dienstlichen Anlass im System Verfahrensautomation Justiz (**VJ**) Daten zu einer Mahnklage für eine Arbeitskollegin ab. Wegen dieser Verfehlung wurde ein Verfahren wegen Missbrauchs der Amtsgewalt gemäß § 302 Abs 1 StGB gegen sie eröffnet. Dieses wurde diversionell erledigt. Die Staatsanwaltschaft brachte eine (erfolgreiche) Beschwerde beim OLG ein.

Das OLG hat erwogen: Das Erstgericht hat ein Verfahren durch **Diversion** zu erledigen, wenn die Tat nicht mit mehr als fünf Jahren Freiheitsstrafe bedroht ist, das Verfahren sonst nicht einzustellen ist, eine Bestrafung im Hinblick auf die Zahlung eines Geldbetrags nicht geboten erscheint, keine spezialpräventiven Gründe entgegenstehen, keine schwere Schuld vorliegt und der Angeklagte Verantwortung übernehmen will.

Ein Verfahren betreffend das Delikt des **Missbrauchs der Amtsgewalt** kann diversionell erledigt werden, wenn durch die Tat keine oder nur eine bloß geringfügige oder sonst unbedeutende Schädigung eingetreten ist und die Tat nicht auch wegen

Bestechung oder Bestechlichkeit mit Strafe bedroht ist. Die Diversion ist damit auf leichte Fälle beschränkt.

Bei der Bewertung einer **bloß geringfügigen** oder sonst **unbedeutenden Schädigung** an Rechten sind Schäden an Vermögensrechten, immateriellen Rechten, **Persönlichkeitsrechten** und öffentlichen Rechten zu prüfen. Somit ist auch das **Recht auf Geheimhaltung** nach § 1 Abs 1 DSGVO Teil der zu berücksichtigenden Rechte. Bei missbräuchlicher Amtsführung iZm **öffentlichen Registern** ist zwischen Fehleintragungen und bloßen Datenabfragen zu unterscheiden. **Vorsätzliche Fehleintragungen** können das Vertrauen in die Richtigkeit eines Registers nachhaltig erschüttern. Diese können im Gegensatz zu missbräuchlichen Abfragen **nicht diversionell** erledigt werden.

Ein geringer Handlungsunwert liegt insbesondere bei einer **einzigsten Datenabfrage** vor, die nur eine **unbedeutende Schädigung** an Rechten Dritter nach sich zieht. Die durch die Bedienstete verwirklichte Datenschutzverletzung ist als **geringfügig einzustufen**, weil die Bedienstete bereits vorab ungefähr über den Inhalt informiert war und durch die Abfrage lediglich eine Bestätigung erhielt, ohne gänzlich neue Informationen zu erlangen.

### Rechtsprechung des BVwG

BVwG 07.08.2025, W605 2289883-1

#### **KKE, Löschungsersuchen, Sanierung**

- Eine Betroffene beantragte bei der Betreiberin der **Konsumenten-Kreditevidenz (KKE)** die Löschung von Vermerken zu einem Insolvenzverfahren und eines Krediteintrags und erhob Widerspruch. Die Betreiberin der KKE lehnte die Anträge ab, woraufhin die Betroffene Datenschutzbeschwerde bei der DSB erhob. Da zum Zeitpunkt der Entscheidung durch die DSB der Krediteintrag noch gespeichert war, die Einträge zum Insolvenzverfahren aber bereits gelöscht waren, stellte die DSB eine Verletzung im Recht auf Löschung und Widerspruch fest und ordnete die Löschung des Krediteintrags an. Die Betreiberin der KKE erhob Bescheidbeschwerde beim BVwG und löschte den Krediteintrag während des laufenden Verfahrens. Das BVwG hob die entsprechenden Spruchpunkte der DSB auf und stellte das Verfahren ein.

Das BVwG hat erwogen: Da dem **Löschungsersuchen** während des Bescheidbeschwerdeverfahrens entsprochen wurde, ist das ursprüngliche **rechtliche Interesse** an einer Entscheidung über Löschung und Widerspruch weggefallen. Die eine Rechtsverletzung feststellenden Spruchpunkte des angefochtenen Bescheids und der

Leistungsauftrag sind daher **aufzuheben** und das Verfahren ist **einzustellen**.

BVwG 23.07.2025, W101 2255209-1

#### **Untersuchungsausschuss, Mandatsbescheid**

- Die Staatsanwaltschaft Wien führte ein Ermittlungsverfahren gegen mehrere Beschuldigte, in dem ein ehemaliger Beamter als Opfer iZm einem Tatverdacht nach § 310 StGB (damals: Verletzung des Amtsgeheimnisses) beteiligt war. Im Rahmen des Verfahrens wurde in der Wohnung eines Beschuldigten ein USB-Stick sichergestellt, der Daten des Mobiltelefons des Beamten enthielt. Der Geschäftsordnungsausschuss des Nationalrats fasste einen grundsätzlichen Beweisbeschluss gemäß § 24 VO-UA, mit dem ua die Bundesministerin für Justiz (**BMJ**) verpflichtet wurde, alle Akten und Unterlagen zum Untersuchungsgegenstand zu übermitteln. Der Beamte befürchtete, dass in Erfüllung dieses Auftrags auch seine im Ermittlungsakt einliegende Chat-Korrespondenz an den Untersuchungsausschuss vorgelegt werden könnte. Daraufhin brachte er eine Datenschutzbeschwerde gegen die BMJ bei der DSB ein und beantragte die Erlassung eines **Mandatsbescheids** gemäß § 22 Abs 4 DSGVO.

Die DSB stellte fest, dass die Befürchtung des Beamten, Mitglieder des Untersuchungsausschusses könnten die Informationen Dritten gegenüber offenlegen, lediglich auf hypothetischen Erwägungen beruhe. Folglich könne das Vorliegen einer konkreten Gefahrensituation iSd § 22 DSGVO nicht bescheinigt werden. Dagegen erhob der Beamte (erfolglos) Bescheidbeschwerde an das BVwG. Im April 2023 wurde der entsprechende Untersuchungsausschuss beendet.

Das BVwG hat erwogen: Gemäß **§ 22 Abs 4 DSGVO** kann die DSB die Weiterführung einer Datenverarbeitung mit Bescheid nach § 57 Abs 1 AVG untersagen, wenn eine **wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen** des Betroffenen vorliegt. Die DSB ist zur Erlassung eines **Mandatsbescheids** ermächtigt, wenn wegen (**objektiver**) **Gefahr im Verzug** eine Verfügung unaufschiebbar ist. Diese Voraussetzung ist nur gegeben, wenn ein Schaden zu erwarten ist, falls die Verfügung der DSB nicht sofort ergeht, sondern erst nach einem (vollständigen) Ermittlungsverfahren. Die "**Unaufschiebbarkeit**" iSd § 57 Abs 1 AVG ist im Verhältnis zur notwendigen Dauer des Ermittlungsverfahrens zu sehen.

Eine "**Gefahr im Verzug**" liegt vor, wenn das Unterlassen der behördlichen Maßnahme voraussichtlich dazu führt, dass Betroffene (weitere)



**Privatsphärenverletzungen** oder **Schäden** hinnehmen müssten, die durch das Erlassen der vorläufigen Untersagung der Datenverarbeitung verhindert werden könnten.

Die **Voraussetzungen zur Erlassung eines Mandatsbescheids** sind im Entscheidungszeitpunkt durch das BVwG **erneut zu prüfen**. Das BVwG hat seine Entscheidung an der zum Zeitpunkt seiner Entscheidung **maßgeblichen Sach- und Rechtslage** auszurichten.

Da der Untersuchungsausschuss beendet wurde, ist eine zwingend **erforderliche Gefährdungslage** im Entscheidungszeitpunkt durch das BVwG jedenfalls **ausgeschlossen**. Mangels "Gefahr im Verzug" besteht kein Bedarf für die Erlassung eines Mandatsbescheids.

Aus der weiteren Rechtsprechung des BVwG:

- Gemäß § 73 Abs 1 AVG ist die DSB verpflichtet, über Anträge von Parteien ohne unnötigen Aufschub, spätestens aber innerhalb von sechs Monaten zu entscheiden (**Entscheidungspflicht**). Eine **Säumnisbeschwerde** kann erst erhoben werden, wenn die DSB ihre Entscheidungspflicht verletzt hat. Gemäß § 24 Abs 10 Z 2 DSG ist die Zeit während eines **Kohärenzverfahrens** (Art 56, 60 und 63 DSGVO) in die Entscheidungsfrist nicht einzurechnen. Die Frist ist während der **federführenden Zuständigkeit** der ausländischen Aufsichtsbehörde gehemmt. Die **Hemmung tritt ex lege** mit Einbringung der Datenschutzbeschwerde ein, sofern eine grenzüberschreitende Verarbeitung vorliegt. Die DSB muss kein gesondertes Aussetzungsverfahren durchführen. Die Aufsichtsbehörde des Mitgliedstaats, in dem der Verantwortliche seine Hauptniederlassung hat, ist für grenzüberschreitende Verarbeitungen federführend zuständig. Die DSB ist in diesem Fall nur betroffene Aufsichtsbehörde. Da während des **Kohärenzverfahrens** keine Säumnis eintreten kann, ist eine Säumnisbeschwerde während dieser Zeit abzuweisen ([BVwG 05.08.2025, W137 2308681-1](#); [BVwG 05.08.2025, W137 2310023-1](#)).
- Den Betroffenen kommt gemäß Art 78 Abs 2 DSGVO die Möglichkeit einer **Untätigkeitsklage** zu, wenn die DSB eine Datenschutzbeschwerde nicht bearbeitet, die Datenschutzbeschwerde nicht an die zuständige Aufsichtsbehörde weiterleitet oder den Betroffenen nicht über den Stand oder das Ergebnis der Datenschutzbeschwerde unterrichtet. Handelt es sich um einen grenzüberschreitenden Sachverhalt, ist gemäß Art 56 DSGVO die **federführende Behörde** zuständig, welche sich nach dem Ort der Hauptniederlassung des Verantwortlichen richtet. Gemäß § 24 Abs 10 Z 2 DSG

ist die Zeit während eines Kohärenzverfahrens (Art 56, 60 und 63 DSGVO) in die Entscheidungsfrist nicht einzurechnen. Die Entscheidungsfrist ist während der federführenden Zuständigkeit der ausländischen Aufsichtsbehörde gehemmt. Der bloße Eingang der Datenschutzbeschwerde bei der DSB hemmt die Entscheidungsfrist allerdings nicht. Die **Hemmung beginnt** erst mit Einleitung des Kohärenzverfahrens. Da die DSB die Datenschutzbeschwerde in der Zwischenzeit an die maltesische Aufsichtsbehörde weitergeleitet und den Betroffenen darüber informiert hat, war die Säumnisbeschwerde jedoch abzuweisen ([BVwG 01.08.2025, W605 2308677-1](#)). **Anm: Zwischen den Senaten des BVwG ist der Zeitpunkt der Hemmung strittig. Der VwGH lehnte die Lösung dieser Rechtsfrage über Amtsrevision der DSB ab, weil das BVwG mit beiden Begründungen die Säumnisbeschwerde abweist und die DSB sohin nicht beschwert ist (vgl. [Schönherr Datenschutzmonitor 28/2025 vom 16.07.2025](#)).**

- Das Datenschutzrecht ist ein höchstpersönliches Recht, das mit dem **Tod** der natürlichen Person untergeht. Der Betroffene verliert daher mit dem Tod seine **Parteistellung** im Verfahren ([BVwG 06.08.2025, W256 2279237-1](#)).
- Eine Bescheidbeschwerde kann nur erheben, wer behauptet, durch den angefochtenen Bescheid in seinen Rechten verletzt zu sein (**Beschwer**). Wurde der Datenschutzbeschwerde stattgegeben, ist das Erheben einer Bescheidbeschwerde gegen den stattgebenden Bescheid zum Erlangen einer finanziellen Entschädigung (**immaterieller Schadenersatz**) nicht zulässig. Für Schadenersatzklagen sind die Landesgerichte **zuständig** ([BVwG 05.08.2025, W137 2308027-1](#)).
- Weist die DSB eine Datenschutzbeschwerde zurück, wird der in der Datenschutzbeschwerde namhaft gemachte Beschwerdegegner nicht zur **Partei** des mit **Zurückweisungsbescheid** abgeschlossenen Verfahrens und hat keinen Anspruch auf **Zustellung des Bescheids** ([BVwG 29.07.2025, W211 2311353-1](#)).

### **Rechtsprechung der LVwG**

Aus der Rechtsprechung der LVwG:

- Der Auskunftswerber hat **keinen Anspruch** auf Auskunft über die **Rechtsmeinung** einer Behörde oder die **subjektive Beurteilung eines Bediensteten** durch die Behörde. Ebenso wenig müssen Behörden im Wege der Auskunftspflicht ihre **Handlungen** und **Unterlassungen** begründen ([LVwG NÖ 24.09.2025, LVwG-AV-1085/001-2025](#)). **Anm: Soweit ersichtlich, ist diese Entscheidung noch auf das NÖ**

Auskunftsgesetz gestützt, das LVwG NÖ zieht aber auch Bestimmungen des neuen IFG heran. Es ist die erste im RIS veröffentlichte Entscheidung, die das neue IFG berücksichtigt.

### **EU-Rechtsakte**

- Am 03.10.2025 ist die "Delegierte Verordnung (EU) 2025/1264 der Kommission vom 27. Juni 2025 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung des Mindestinhalts der Strategien und Verfahren für das Liquiditätsmanagement für bestimmte Emittenten von vermögenswertereferenzierten Token oder E-Geld-Token", [ABI L 2025/1264](#), kundgemacht worden. Mit dieser DelegiertenVO werden die Mindestinhalte der Strategien und Verfahren für das **Liquiditätsmanagement** für bestimmte Emittenten von **vermögenswertereferenzierten Token** oder **E-Geld-Token** präzisiert.
- Am 30.09.2025 wurden die (i) "Durchführungsverordnung (EU) 2025/1942 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf **qualifizierte Validierungsdienste** für qualifizierte elektronische Signaturen und qualifizierte Validierungsdienste für qualifizierte elektronische Siegel", [ABI L 2025/1942](#); (ii) "Durchführungsverordnung (EU) 2025/1943 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards für **qualifizierte Zertifikate** für elektronische Signaturen und qualifizierte Zertifikate für elektronische Siegel", [ABI L 2025/1943](#); (iii) "Durchführungsverordnung (EU) 2025/1944 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards für Prozesse des Absendens und Empfangens von Daten in **qualifizierten Diensten** für die Zustellung elektronischer Einschreiben und in Bezug auf die Interoperabilität dieser Dienste", [ABI L 2025/1944](#); (iv) "Durchführungsverordnung (EU) 2025/1945 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die **Validierung** qualifizierter elektronischer Signaturen und qualifizierter elektronischer Siegel sowie die Validierung fortgeschrittener elektronischer Signaturen,

die auf qualifizierten Zertifikaten beruhen, und fortgeschrittener elektronischer Siegel, die auf qualifizierten Zertifikaten beruhen", [ABI L 2025/1945](#); und (v) "Durchführungsverordnung (EU) 2025/1946 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf **qualifizierte Bewahrungsdienste** für qualifizierte elektronische Signaturen und qualifizierte elektronische Siegel", [ABI L 2025/1946](#), kundgemacht. Mit diesen **fünf DurchführungsVOs** werden **Referenzstandards und Spezifikationen** unter der [eIDAS-VO](#) festgelegt.

### **Nationale Rechtsakte**

- Am **29.09.2025** wurde das "Bundesgesetz, mit dem das **Staatsschutz- und Nachrichtendienst-Gesetz**, das Sicherheitspolizeigesetz, das Telekommunikationsgesetz 2021, das **Bundesverwaltungsgerichtsgesetz** und das Richter- und Staatsanwaltschaftsdienstgesetz geändert werden", [BGBl I 2025/54](#), kundgemacht. Mit diesem Gesetz wird eine Rechtsgrundlage für die Überwachung **Ende-zu-Ende-verschlüsselter Kommunikation** (wie etwa über WhatsApp oder Signal) zur Bekämpfung verfassungsschutzrelevanter Bedrohungslagen geschaffen (**Bundestrojaner**). Für die **Bewilligung** von Ermittlungsmaßnahmen wird das **BVwG** zuständig. Dafür werden außerhalb der gerichtlichen Amtsstunden **Rufbereitschaft und Journaldienst** beim BVwG eingerichtet. Gleichzeitig wird die **Evidenzstelle des BVwG** durch eine Änderung des § 20 BVwGG entlastet. Die **Veröffentlichungspflicht** entfällt hinsichtlich jener Entscheidungen, die keine (zusätzlichen) rechtsrelevanten Informationen enthalten. **Anm: Dadurch wird auch die Zahl der im Schönherr Datenschutzmonitor veröffentlichten Entscheidungen reduziert werden.** Aufgrund des IFG und der neuen Kompetenz im SNG könnte die Zahl der inhaltlich relevanten Entscheidungen jedoch steigen.

to the point

# Datenschutzmonitor. 41/2025 vom 15.10.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des VfGH**

VfGH 11.09.2025, E1734/2025 (Universität, Verordnung, Rechtsgrundlage, Audioaufzeichnung)

VfGH 12.09.2025, G175/2024 (Gesetzesprüfung, Auswertung von Datenträgern)

VfGH 12.09.2025, G108/2025 (Gesetzesbeschwerde, Nachrichtenüberwachung)

- **Rechtsprechung des VwGH**

VwGH 20.08.2025, Ro 2020/04/0010 (Auskunft, automatisierte Entscheidungsfindung, Profiling, Geschäftsgeheimnis)

VwGH 16.09.2025, Ra 2025/04/0181 (Revision, Zulässigkeit, Rechtsfrage grundsätzlicher Bedeutung)

VwGH 11.09.2025, Ra 2024/03/0031 (Auskunft, Einsichtstermine)

- **Rechtsprechung der Justiz**

OLG Wien 28.04.2025, 12R2/25i (Auskunftsrecht, Videoaufnahme, strukturierte Datensammlung, Neuerungsverbot)

OGH 03.10.2025, 11Os83/25b (Beschlagnahme, Daten, Datenträger, StPO)

- **Rechtsprechung des BVwG**

BVwG 21.08.2025, W176 2250812-1 (Auskunft, automatisierte Entscheidungsfindung, involvierte Logik)

BVwG 25.07.2025, W258 2299744-1 (Geldbuße, Videoüberwachung, Rechtsgrundlage)

BVwG 11.07.2025, W295 2243015-1 (Energieversorgung, E-Control, Auskunfts- und Einsichtspflicht, Erforderlichkeitsvorbehalt)

BVwG 26.08.2025, W291 2309033-1 (Widerspruchsrecht, Antragspflicht)

BVwG 28.04.2025, W258 2224229-1 (PNR-System, Fluggastdaten)

- **Rechtsprechung des BFG**

BFG 30.06.2025, RV/7100116/2020 (Finanzpolizei, Datenschutz)

- **Rechtsprechung der LVwG**

LVwG NÖ 19.08.2025, LVwG-AV-1302/001-2024 (Akteneinsicht, Verfahrensabschluss, DSGVO)

- **EU-Rechtsakte**

EDSA/Kommission, Joint Guidelines on the Interplay between the DMA and the GDPR

Verordnung (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung

DelegierteVO zum DSA (Forschungsdaten)

## To the Point:

### Rechtsprechung des VfGH

Aus der Rechtsprechung des VfGH:

- Eine Richtlinie des Rektorats, die im Mitteilungsblatt der Universität kundgemacht wird und sich an Universitätsangehörige richtet, kann eine **Verordnung** iSd Verordnungsermächtigung des Art 81c Abs 1 Satz 2 B-VG sein. Das BVwG wird im fortgesetzten Verfahren prüfen müssen, ob die Richtlinie eine Verordnung ist, die die **Audiodaufzeichnungen** zu Zwecken der Protokollierung einer Departmentsitzung gemäß **Art 6 Abs 1 lit e DSGVO** rechtfertigen konnte ([VfGH 11.09.2025, E1734/2025](#)).
- Ein **Antrag auf Gesetzesprüfung** ist nur dann zulässig, wenn die verfassungsrechtlichen Bedenken präzise dargelegt werden. Eine **Bezugnahme auf andere Texte** genügt nur, wenn der Antragsteller festlegt, ob und inwieweit er die zitierten Bedenken zu seinen eigenen erhebt. Da sich das BVwG in seinem Antrag auf Gesetzesprüfung bestimmter Bestimmungen und Wortfolgen des BFA-VG betreffend die **Auswertung und Sicherstellung von Datenträgern** den Ausführungen des Beschwerdeführers des Anlassverfahrens nur "**prinzipiell anschließt**" genügt der Antrag nicht den Anforderungen des § 62 Abs 1 VfGG und ist daher unzulässig ([VfGH 12.09.2025, G175/2024](#)).
- Eine **Gesetzesbeschwerde** ist nur dann zulässig, wenn der Antragsteller seine **unmittelbare und aktuelle Betroffenheit** durch die angefochtenen Bestimmungen im Einzelnen darlegt. Die **pauschale Behauptung**, er befinde sich aufgrund der **Übermittlung von Chatverläufen** in Untersuchungshaft, genügt nicht. Der Antrag enthält keine nachvollziehbaren Angaben, anhand derer beurteilt werden könnte, ob die angefochtenen Normen unmittelbar und aktuell in die Rechtssphäre des Antragstellers eingreifen. **Bloße Kritik an der geltenden Rechtslage** reicht nicht aus; erforderlich ist ein **konkreter Bezug zum eigenen Verfahren**. Da dem Antrag ein unbehebbares Prozesshindernis entgegensteht, ist er zurückzuweisen ([VfGH 12.09.2025, G108/2025 ua](#)).

### Rechtsprechung des VwGH

VwGH 20.08.2025, Ro 2020/04/0010

#### **Auskunft, automatisierte Entscheidungsfindung, Profiling, Geschäftsgeheimnis**

- Eine Betroffene erachtete sich in ihrem Auskunftsrecht verletzt und erhob Datenschutzbeschwerde bei der DSB, weil eine Wirtschaftsauskunftei im Zuge eines Bonitätsscorings keine hinreichend

aussagekräftigen Informationen über die involvierte Logik der automatisierten Entscheidungsfindung erteilt hätte. Die DSB gab der Datenschutzbeschwerde teilweise statt und trug der Wirtschaftsauskunftei auf, eine ergänzende Auskunft zu erteilen. Die Wirtschaftsauskunftei erhob Beschwerde beim BVwG. Dieses bestätigte die Verletzung im Recht auf Auskunft gemäß Art 15 Abs 1 lit h DSGVO hinsichtlich der fehlenden Erläuterung der Logik der automatisierten Berechnung; im Übrigen wurde die Auskunft als vollständig erachtet. Die Wirtschaftsauskunftei erhob ordentliche Revision, die der VwGH nach Aussetzung des Verfahrens aufgrund der Entscheidungen des EuGH in den Rechtssachen *SCHUFA* (C-634/21) und *Dun & Bradstreet Austria* (C-203/22) abwies.

Der VwGH hat erwogen: **Art 15 Abs 1 lit h DSGVO** sieht bei einer Entscheidung gemäß Art 22 Abs 1 DSGVO ein Recht auf Auskunft über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling sowie auf aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen vor. Nach der EuGH-Rechtsprechung umfasst dieses Auskunftsrecht ein **echtes Recht auf Erläuterung des Verfahrens und der Grundsätze** der konkret angewandten automatisierten Verarbeitung, und zwar in präziser, transparenter, verständlicher und leicht zugänglicher Form. Weder die bloße Nennung allgemeiner Einflussfaktoren noch pauschale Hinweise auf "gleichwertige" Gewichtungen genügen. Ebenso wenig reicht die Offenlegung einer komplexen Formel oder eine abstrakte Beschreibung ohne Bezug zum individuellen Ergebnis.

Die Wirtschaftsauskunftei hat nicht nachvollziehbar dargelegt, **welche Daten auf welche Art in den Score eingeflossen sind** und in welchem Ausmaß **Abweichungen einzelner Parameter das Ergebnis verändert hätten**. Ohne solche Informationen kann die betroffene Person ihre Rechte, insbesondere jene nach Art 22 Abs 3 DSGVO (Darlegung des eigenen Standpunkts, Anfechtung der Entscheidung), nicht effektiv ausüben.

**Geschäftsgeheimnisse** schließen den Auskunftsanspruch nicht pauschal aus. Es bedarf einer **Einzelfallabwägung** zwischen dem Auskunftsrecht und dem Schutz fremder Rechte. Die DSGVO verlangt keine Offenlegung des vollständigen Algorithmus oder der detaillierten mathematischen Formel. Gefordert ist eine konkrete, verständliche Beschreibung des tatsächlich angewandten Verfahrens und der maßgeblichen Grundsätze, die es der betroffenen Person erlaubt, die Entscheidung inhaltlich nachzuvollziehen. Der pauschale Verweis auf ein

Betriebsgeheimnis ersetzt diese Erläuterung nicht.

#### Aus der weiteren Rechtsprechung des VwGH:

- Ein Revisionswerber behauptete, das BVwG hätte bei vollständiger Sachverhaltsfeststellung erkennen müssen, dass die mitbeteiligte Partei nicht als Auftragsverarbeiter, sondern als Verantwortlicher einzustufen war. Eine **Revision**, bei der das Vorbringen unkonkret ist und die einen bloßen Hinweis auf fehlende Rechtsprechung enthält, der vom festgestellten Sachverhalt abweicht, begründet **keine Rechtsfrage von grundsätzlicher Bedeutung** und ist daher zurückzuweisen ([VwGH 16.09.2025, Ra 2025/04/0181](#)).
- Bei einem Umfang der begehrten **Auskunft** von mindestens 2.000 A4-Seiten darf die Auskunftserteilung nicht **durch Einsichtstermine** erfolgen, bei denen die Anfertigung von Fotos und Kopien von Dokumenten untersagt ist. Es ist eine andere, für die Auskunftserteilung geeignete Form zu wählen ([VwGH 11.09.2025, Ra 2024/03/0031](#)).  
**Anm: Diesem Rechtsstreit lag noch das Wiener Auskunftspflichtgesetz zugrunde. Unter dem nunmehr geltenden IFG gilt dies umso mehr.**

#### Rechtsprechung der Justiz

OLG Wien 28.04.2025, 12R2/25i

#### **Auskunftsrecht, Videoaufnahme, strukturierte Datensammlung, Neuerungsverbot**

- Der Bewohner eines Wohnhauses filmte zum Nachweis von Lärm durch andere Hausbewohner den Hausflur mit seinem Mobiltelefon. Das Video zeigte keine Personen, zu hören war nur unverständliches Geschrei. Der Bewohner erstattete Anzeige bei der Polizei, zeigte dieser die Aufnahme und löschte sie anschließend. Geolokalisierung und Cloud-Dienste wurden nicht genutzt. Eine Nachbarin verlangte Auskunft und Datenkopie nach Art 15 DSGVO und § 1 Abs 3 DSG. Der Bewohner lehnte ihr Auskunftersuchen unter Verweis auf die Haushaltsaufnahme ab und erklärte, keine personenbezogenen Daten der Nachbarin zu verarbeiten. Die Nachbarin klagte auf Auskunft. Nachdem das LG das Klagebegehren abwies, erhob sie (erfolglose) Berufung an das OLG Wien.

Das OLG hat erwogen: Das Auskunftsrecht des § 1 Abs 3 DSG bezieht sich nur auf Daten, die in strukturierten Datensammlungen, nämlich automationsunterstützten Datenanwendungen oder manuellen Dateien, enthalten oder zur Verarbeitung in solchen bestimmt sind.

Soweit die Nachbarin geltend macht, der Bewohner sei seiner Auskunftspflicht im

Hinblick auf ihr Antwortschreiben, das er erfasst und per E-Mail beantwortet habe, nicht nachgekommen, verstößt sie gegen das im Berufungsverfahren geltende Neuerungsverbot. Gleiches gilt für das Vorbringen, die Mitteilung des Nachbarn an die Polizei habe ihre personenbezogenen Daten enthalten.

Eine Erfassung des Antwortschreibens in der E-Mail ist keine Weitergabe personenbezogener Daten an andere Empfänger. Die E-Mail richtet sich an die Rechtsvertretung der Nachbarin, die den Bewohner zuvor zur Auskunft aufgefordert hat. Unter einer Übermittlung ist die Weitergabe personenbezogener Daten an **andere Empfänger** als die Betroffene zu verstehen.

Auch erschließt sich nicht, welche personenbezogenen Daten der Bewohner an die Polizei weitergegeben haben soll, wenn er dieser lediglich mitteilte, das Video nicht mehr zu besitzen. Auf dem Video wurde die Nachbarin weder bildlich noch akustisch oder in sonstiger Form aufgenommen.

#### Aus der weiteren Rechtsprechung der Justiz:

- Die **Beschlagnahme** von **Datenträgern** und **Daten** ist gemäß **§ 115f Abs 1 StPO** nur zulässig, wenn dies aus Beweisgründen erforderlich ist und aufgrund bestimmter Tatsachen anzunehmen ist, dass dadurch Informationen ermittelt werden können, die für die Aufklärung einer Straftat wesentlich sind ([OGH 03.10.2025, 110s83/25b](#)).

#### Rechtsprechung des BVwG

[BVwG 21.08.2025, W176 2250812-1](#)

#### **Auskunft, automatisierte Entscheidungsfindung, involvierte Logik**

- Ein ehemaliger Arbeitnehmer richtete ein Auskunftersuchen an seinen ehemaligen Arbeitgeber, das sich insbesondere auf Bonitätsbewertungen iZm einer Kreditvergabe aus dem Jahr 2010 bezog. Der ehemalige Arbeitnehmer erachtete die fristgerecht erteilte Auskunft als unvollständig und erhob Datenschutzbeschwerde bei der DSB. Diese stellte eine Verletzung im Recht auf Auskunft fest und verpflichtete den ehemaligen Arbeitgeber zur Übermittlung aussagekräftiger Informationen über die Logik, Tragweite und Auswirkungen der automatisierten Entscheidung. Dagegen erhob der ehemalige Arbeitgeber (erfolgreiche) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Das **Auskunftsrecht** soll Betroffenen ermöglichen, ihre personenbezogenen Daten zu überprüfen, insbesondere im Hinblick auf Richtigkeit und Zulässigkeit der Verarbeitung. Nach Erhalt der Auskunft müssen Betroffene in der Lage sein, weitere Datenschutzrechte auszuüben.

Die **Rechtsgrundlage** der Verarbeitung muss grundsätzlich nicht mitgeteilt werden, kann aber Teil des Auskunftsrechts sein, wenn sie für die Kontrolle der Rechtmäßigkeit erforderlich ist. Die **Zwecke** der Verarbeitung müssen hinreichend konkret angegeben werden, ohne die Detailtiefe eines Verzeichnisses der Verarbeitungstätigkeiten zu erreichen, sofern eine Rechtmäßigkeitskontrolle möglich bleibt.

Art 15 Abs 1 lit h DSGVO setzt eine **automatisierte Entscheidungsfindung einschließlich Profiling** voraus. Eine solche liegt vor, wenn eine Entscheidung an einen ermittelten Kreditscore anknüpft oder wenn der Scorewert maßgeblich in die Entscheidung einfließt und deren wesentliche Grundlage bildet. Kein Verstoß liegt vor, wenn ein Sachbearbeiter bei einem ungünstigen Scorewert frühzeitig eine **entscheidungsbefugte Person** hinzuzieht, die die automatisierte Vorgabe inhaltlich prüft und gegebenenfalls korrigiert. Diese **Korrekturkompetenz** sollte dokumentiert werden. Die involvierte Logik umfasst den Aufbau, die Struktur und den Ablauf der Datenverarbeitung. Dazu gehören Informationen darüber, welche erhobenen Daten bzw Faktoren mit welcher Gewichtung in die Berechnung des Scorewerts einfließen und wie sich die Scorewerte gegenseitig beeinflussen.

Ist Verfahrensgegenstand eine Datenverarbeitung, die vor Inkrafttreten der DSGVO und des DSG stattfand, ist die **zum damaligen Zeitpunkt geltende Rechtslage** anzuwenden. Art 15 Abs 1 DSGVO statuiert gegenüber § 26 DSG 2000 ein erweitertes Auskunftsrecht, weil nach § 49 Abs 3 iVm § 26 DSG 2000 lediglich der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form darzulegen war. Das Auskunftsbegehren des ehemaligen Arbeitnehmers richtete sich auf Auskunft, welche Entscheidungen getroffen werden und Angaben zu der verwendeten Logik, Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung. Eine Bewertung einer Bonitätsverarbeitung aus dem Jahr 2010 nach der damals noch nicht anwendbaren DSGVO ist unzulässig.

BVwG 25.07.2025, W258 2299744-1

### **Geldbuße, Videoüberwachung, Rechtsgrundlage**

- Ein Unternehmen betrieb eine Filiale mit zahlreichen Innen- und Außenkameras. Einige Innenkameras waren auf die Selbstbedienungskassen gerichtet, die Außenkameras erfassten ua Gehsteige, Zugänge, Fahrradabstellanlagen und Teile öffentlicher Verkehrsflächen. Nach einer anonymen Anzeige leitete die DSB ein amtswegiges Prüfverfahren ein, das nach Beseitigung

einzelner Kameras eingestellt wurde. Aufgrund der Ermittlungsergebnisse wurde jedoch ein Verwaltungsstrafverfahren eingeleitet. Die DSB erachtete alle Kameras als unzulässig und verhängte eine Geldbuße iHv EUR 1,5 Mio wegen Verstößen gegen Art 5 Abs 1 lit a und c sowie Art 6 Abs 1 DSGVO. Das Unternehmen erhob (teilweise erfolgreich) Beschwerde an das BVwG. Das BVwG behob das Straferkenntnis der DSB zwar hinsichtlich zweier Kameras, setzte die Geldbuße jedoch nicht herab.

Das BVwG hat erwogen: Der Betrieb jener Kameras, die keine PIN-Eingaben an den Selbstbedienungskassen erfasst haben, verstößt nicht gegen die DSGVO.

Eine Kamera im Innenbereich erfasste die **PIN-Eingaben** von etwa 637 Personen und speicherte diese für 72 Stunden. Aufgrund der Identifizierbarkeit der Kunden und der Erfassung ihrer PIN-Eingaben liegen **personenbezogene Daten** vor. Das Erfassen und Speichern der PIN-Eingaben verstößt gegen den **Grundsatz der Datenminimierung** gemäß Art 5 Abs 1 lit c DSGVO. Die auf Art 6 Abs 1 lit f DSGVO gestützte Datenverarbeitung war auch unrechtmäßig, da die PIN-Eingaben für den Schutz des Eigentums nicht erforderlich waren.

Sofern das Unternehmen den Betrieb der Außenkameras ua auf den Schutz der Mitarbeiter und Kunden stützt, ist zu berücksichtigen, dass im Verhältnis zu den erfassten zehntausenden Personen nur wenige tatsächlich gefährdet waren, die Wahrscheinlichkeit von Übergriffen gering war und die überwachten Bereiche stark frequentiert sind. Zudem standen andere Schutzmaßnahmen wie patrouillierendes Wachpersonal oder ausreichende Beleuchtung zur Verfügung. In einer Gesamtabwägung überwiegen daher die Grundrechte und schutzwürdigen Geheimhaltungsinteressen der von der Videokamera erfassten Personen. Die Videoüberwachung verstößt daher gegen den Rechtmäßigkeitsgrundsatz des Art 5 Abs 1 iVm Art 6 Abs 1 DSGVO. Eine Zurechnung des Handelns einer bestimmten natürlichen Person an das Unternehmen als juristische Person ist nicht erforderlich. § 30 Abs 1 und 2 DSG haben unangewendet zu bleiben.

Dem Unternehmen ist **grobe Fahrlässigkeit** vorzuwerfen, weil die Kameras in Betrieb genommen wurden, bevor erforderliche Privatzone maskierungen überprüft oder eingerichtet waren. Auch nach Bekanntwerden der Fehler wurden die Maskierungen nicht sofort umgesetzt, obwohl eine schnelle Korrektur möglich gewesen wäre.

### **Energieversorgung, E-Control, Auskunfts- und Einsichtspflicht, Erforderlichkeitsvorbehalt**

- Eine im Bereich der Energieversorgung tätige Konzernmutter wurde von der E-Control mittels Bescheid zur Übermittlung von Wirtschaftsprüfungsberichten und Jahresabschlüssen der Konzernunternehmen und weiteren Daten einer bereitgestellten Anforderungsliste gemäß § 34 des Energie-Control-Gesetzes (E-Control-Gesetz) iVm §§ 10 und 48 des Elektrizitätswirtschafts- und -organisationsgesetzes 2010 (EIWOG 2010) verpflichtet, um konzerninterne Verrechnungen zu prüfen. Dagegen erhob die Konzernmutter (erfolgreich) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die Konzernmutter unterliegt als Elektrizitätsunternehmen der **Auskunfts- und Einsichtspflicht** gegenüber der E-Control in alle **betriebswirtschaftlich relevanten Unterlagen und Auskünfte** wie Wirtschaftsprüfungsberichte, Jahresabschlüsse und Saldenlisten.

Diese Pflicht besteht **jederzeit**, auch ohne konkreten Anlassfall, wenn die benötigten Unterlagen oder Auskünfte als Entscheidungsgrundlage für künftig durchzuführende Verfahren benötigt werden. Die Auskunfts- und Einsichtsrechte werden jedoch Beschränkungen unterworfen. So besteht etwa – mit Blick auf § 1 Abs 1 DSGVO – ein **Erforderlichkeitsvorbehalt**. Den Behörden kommt zwar ein erheblicher Spielraum zu, Daten bzw Unterlagen anzufordern, diese müssen jedoch für die Wahrnehmung der Überwachungs- und Aufsichtsbefugnisse erforderlich sein.

Die E-Control handelte rechtsrichtig im Rahmen ihres Handlungsspielraums, indem sie die Unterlagen in einem gesonderten, zeitlich vorgelagerten Auskunftsverfahren anforderte. Da § 10 EIWOG 2010 **keine zeitliche Begrenzung** der Auskunftspflicht enthält, ist die Anforderung von Unterlagen ab 2015 zulässig, wenn ein Kostenanstieg ab 2015 einen Prüfbedarf auslöst.

#### Aus der weiteren Rechtsprechung des BVwG:

- Die in den **Art 15 bis 22 DSGVO** geregelten Rechte bestehen – anders als die Informationspflicht nach Art 14 DSGVO – nicht unabhängig von einem **vorherigen Antrag** der betroffenen Person. Auch Art 12 DSGVO spricht von einem Antrag der Betroffenen auf Wahrnehmung ihrer Rechte nach Art 15 bis 22 DSGVO. Hat die Betroffene keinen Antrag auf Widerspruch nach Art 21 DSGVO an den Verantwortlichen gestellt, kann sie nicht im Recht auf Widerspruch verletzt worden sein ([BVwG 26.08.2025, W291 2309033-1](#)).

- Das **PNR-System** darf nur zur Bekämpfung schwerer Kriminalität eingesetzt werden. Nach § 4 Abs 4 PNR-G dürfen **Fluggastdaten** bis zu sechs Monate gespeichert werden, wenn **objektive Anhaltspunkte für terroristische Straftaten oder schwere Kriminalität** bestehen, die mit der Reise der Fluggäste zusammenhängen. Die Fluggastdatenzentralstelle muss prüfen, ob ein Treffer der schweren Kriminalität zuzurechnen ist und daher weiter zu bearbeiten ist oder gelöscht werden muss ([BVwG 28.04.2025, W258 2224229-1](#)).

#### Rechtsprechung des BFG

- **Finanzpolizeiliche Erhebungsergebnisse** unterliegen dem **Datenschutz** und haben keinen Einfluss auf die Vergabe von **Baufträgen der Stadt Wien**, weil die Finanzpolizei eine Bundesbehörde ist. Die Geschäftsdaten betreffend den Zeitpunkt der Zahlungen für Miete, Strom und Telefon sowie die Höhe der variablen Anteile bei Strom- und Telefonkosten unterliegen dem Datenschutz ([BFG 30.06.2025, RV/7100116/2020](#)). **Anm: Da bei Vergabeverfahren Verwaltungsstrafregister des Bundes standardmäßig abgefragt werden, erscheint der Verweis auf die Eigenschaft der Finanzpolizei als Bundesbehörde zu pauschal.**

#### Rechtsprechung der LVwG

##### Aus der Rechtsprechung der LVwG:

- Das Recht auf **Akteneinsicht** besteht für Verfahrensparteien auch **nach Abschluss** des Verfahrens weiter. Der bloße Verweis auf die Einhaltung der **DSGVO** – ohne die Schutzwürdigkeit von (irgendwelchen) personenbezogenen Daten zu behaupten –, ist zur Verweigerung der Akteneinsicht nicht ausreichend ([LVwG NÖ 19.08.2025, LVwG-AV-1302/001-2024](#)). **Anm: Die Geltung des Rechts auf Akteneinsicht über den Abschluss des Verfahrens hinaus ist in Hinblick auf das neue IFG relevant, weil, solange und soweit das Recht auf Akteneinsicht besteht, das IFG nicht zur Anwendung gelangt (§ 16 IFG).**

#### EU-Rechtsakte

- Am **09.10.2025** veröffentlichten der EDSA und die Europäische Kommission einen gemeinsamen Entwurf von **Leitlinien**, die das **Zusammenspiel zwischen dem DMA und der DSGVO** erläutern sollen. Zum Entwurf können im Rahmen einer öffentlichen Konsultation bis zum 04.12.2025 Stellungnahmen abgegeben werden. Die Leitlinien behandeln insbesondere die Datenverarbeitung von Betroffenen durch

Gatekeeper(plattformen) iSd DMA. Das "Pay-or-Ok"-Modell wird als argumentierbar unanwendbar angesehen, wenn sich Gatekeeper darauf berufen wollen. Zudem werden Details zur Datenportabilität sowie zum effektiven, kontinuierlichen und Echtzeit-Zugang zu von Nutzern generierten Daten festgelegt. Darüber hinaus wird die Verantwortlichkeit für die Einholung der Endnutzer-Einwilligung zum Datenzugang durch gewerbliche Nutzer geklärt und es werden Details zur koordinierten Durchsetzung und konsistenten Anwendung durch die Behörden behandelt.

- Am **10.10.2025** ist die "*Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz und das Targeting politischer Werbung*" **in Geltung** getreten. Ziel ist es, ein einheitliches und hohes Maß an Transparenz bei politischen Werbedienstleistungen innerhalb der EU zu gewährleisten. Gleichzeitig soll der gezielten Informationsmanipulation und Beeinflussung durch politische Werbung entgegengetreten werden. Politische Anzeigen sollen eindeutig als solche erkennbar sein.
- Am **09.10.2025** ist die "*Delegierte Verordnung (EU) 2025/2050 der Kommission vom 1. Juli 2025 zur Ergänzung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates durch Festlegung der technischen Bedingungen und Verfahren, unter denen die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen zugelassenen Forschenden Daten zur Verfügung stellen müssen*", [ABLL 2025/2050](#), kundgemacht worden. Gemäß Art 40 Abs 4 der VO (EU) 2022/2065 ([DSA](#)) haben die Anbieter **sehr großer Online-Plattformen** oder **sehr großer Online-Suchmaschinen** auf begründetes Verlangen des örtlich zuständigen **Koordinators für digitale Dienste** zur Durchführung von **Forschungsarbeiten**, die der Erforschung systemischer Risiken dienen, **Zugang zu Daten** zu gewähren. Die DelegierteVO legt das Verfahren und die technischen Bedingungen für die Zugangsgewährung über ein **Datenzugangsportale** fest. Die Kommission wird als **Auftragsverarbeiterin** hinsichtlich des DSA-Datenzugangsportals benannt.



# Datenschutzmonitor. 42/2025 vom 23.10.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Abonnieren Sie auch unsere anderen periodischen Newsletter, **Digital Law Monitor**, **Technology & Digitalisation**, **Financial Regulation** und **Healthcare & Life Sciences** für regelmäßige, prägnante Updates [hier](#).

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH SA 16.10.2025, C-484/24, *NTH Haustechnik* (Gerichtbarkeit, Beweisverwertung, Speicherbegrenzung)

EuG 15.10.2025, T-291/23, *MeSoFa* (Dokumentenzugang, Geschäftsinteresse, Personenbezug, berufliche Daten)

#### NACHTRAG

EuGH 30.09.2025, C-40/25, *CRIF* (Streichung)

- **Rechtsprechung des VfGH**

VfGH 24.09.2025, E1925/2025 (strafgerichtliche Verurteilung, Staatsbürgerschaft)

- **Rechtsprechung des VwGH**

VwGH 16.09.2025, Ra 2023/04/0008 (Rollenverteilung, StVO, städtischer Magistrat)

VwGH 22.09.2025, Ra 2023/04/0108 (Beschwerdegegner)

- **Rechtsprechung der Justiz**

OLG Linz 30.06.2025, 4R89/25y (Auskunft, Beweismittelbeschaffung, Rechtsmissbrauch)

OLG Wien 24.02.2025, 1R125/24w (Rollenqualifikation, Rechtsfrage)

OLG Linz 11.09.2025, 10Bs198/25a (Akteneinsicht, Datenschutz, überwiegende private Interessen)

- **Rechtsprechung des BVwG**

BVwG 10.06.2024, W148 2291941-1 (WiEreG, public watchdog, Einsichtsrecht)

BVwG 11.07.2025, W292 2291080-1 (Medien, Bürgerjournalismus, Verschwörungstheorien)

BVwG 14.08.2025, W298 2309032-1 (ELGA, Auskunft, Feststellungsinteresse, Erkundungsbeweis)

BVwG 26.02.2025, W101 2284403-1 (Videoüberwachung, Geldbuße, Kennzeichnung, öffentlicher Raum)

BVwG 18.07.2025, W292 2235791-1 (Auskunft, Empfänger, Auftragsverarbeiter)

- **Rechtsprechung der LVwG**

LVwG Tirol 06.10.2025, LVwG-2025/S2/1049-8 (Vergabeverfahren, Rollenverteilung, Auftragsverarbeiter, Pseudonymisierung)

LVwG NÖ 23.09.2025, LVwG-M-32/001-2025 (Datenweitergabe, Zuständigkeit, DSB)

- **Rechtsprechung der DSB**

DSB 12.09.2025, 2025-0.703.379 (IFG, Auskunftspflicht, sachlicher Anwendungsbereich)

DSB 16.08.2024, 2023-0.680.196 (Videoüberwachung, Geldbuße)

- **EU-Rechtsakte**

Entwurf einer DelegiertenVO zur CRA

- **Nationale Rechtsakte**

Resilienz kritischer Einrichtungen-Gesetz (RKEG)

Novelle des ORF-Beitrags-Gesetzes (OBG)

## To the Point:

### Rechtsprechung des EuGH

EuGH SA 16.10.2025, C-484/24, NTH Haustechnik

#### **Gerichtbarkeit, Beweisverwertung, Speicherbegrenzung**

- Ein Arbeitgeber (**AG**) kündigte einer Arbeitnehmerin (**AN**), gewährte ihr aber weiterhin Zugang zu betriebseigenen EDV-Geräten. Die AN hat unter Verwendung des Betriebscomputers über ihr privates eBay-Konto Betriebsmittel des (ehemaligen) AG veräußert, was dem AG durch spätere Einsicht in das private eBay-Konto ersichtlich wurde. Das vorliegende Gericht sah dadurch ggf eine unrechtmäßige Datenverarbeitung vorliegen und ging davon aus, dass dies auch auf die Verwertung der erhobenen Daten im Rahmen der eigenen justiziellen Tätigkeit durchschlagen könnte. Deshalb legte es dem EuGH Fragen zur Auslegung (i) des Prinzips der Speicherbegrenzung und der Ausnahme davon für Zwecke der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen sowie (ii) zur gerichtlichen Verarbeitung von unrechtmäßig erlangten oder gespeicherten Daten im Rahmen eines nationalen Gerichtsverfahrens vor.

Der GA hat erwogen: Die Verarbeitung personenbezogener Daten im **Gerichtsverfahren** fällt unter Art 6 Abs 1 lit e DSGVO, wonach die Verarbeitung rechtmäßig ist, wenn sie "für die **Wahrnehmung einer Aufgabe** erforderlich [ist], die **im öffentlichen Interesse** liegt oder in **Ausübung öffentlicher Gewalt** erfolgt". Der Grundsatz der **Speicherbegrenzung** betrifft nur die Anforderungen, denen die Aufbewahrung personenbezogener Daten genügen muss und beantwortet nicht die Frage, welche Auswirkungen es auf die justizielle Verarbeitung personenbezogener Daten durch ein nationales Gericht hat, wenn ein erster Verantwortlicher gegen den Grundsatz der Speicherbegrenzung personenbezogener Daten verstoßen hat.

Einem **Gericht** ist es nicht untersagt, Daten zu verarbeiten, die eine der Parteien des Rechtsstreits unter **Verstoß** gegen den Grundsatz der Speicherbegrenzung gewonnen haben soll. Das Unionsrecht regelt die Frage der **Zulässigkeit von Beweismitteln** in nationalen Gerichtsverfahren nicht.

Dies ist **Sache der Mitgliedstaaten**, die unter Beachtung der unionsrechtlichen Grundsätze der Effektivität und Äquivalenz entsprechende nationale Regelungen treffen müssen. Es obliegt daher dem vorliegenden Gericht, die einschlägigen Bestimmungen des nationalen Rechts sowie die Rechtsprechung des betreffenden Mitgliedstaats zu ermitteln. Zu prüfen ist, ob diese mit den

Grundsätzen der Äquivalenz und der Effektivität vereinbar sind und einem im öffentlichen Interesse liegenden Zweck entsprechen, sowie ob sie dafür erforderlich sind und in einem angemessenen Verhältnis zu diesem Zweck stehen. Das vorliegende Gericht hat zu ermitteln, ob die personenbezogenen Daten als **Beweismittel zulässig** sind und welche Modalitäten nach Maßgabe der Umstände des Einzelfalls und der Verfahrensart für deren **Verwertung** gelten.

#### Aus der Rechtsprechung des EuGH/EuG:

- Der **Zugang zu einem Dokument** einer EU-Institution darf zur Wahrung bestimmter geschützter Interessen verweigert werden. Nicht alle Informationen über ein Unternehmen und seine Geschäftsbeziehungen können als schutzbedürftig angesehen werden. Um den Zugang verweigern zu können, muss nachgewiesen werden, dass die betreffenden Dokumente Elemente enthalten, deren Offenlegung die **Geschäftsinteressen einer juristischen Person** ernsthaft beeinträchtigen könnte. Dies ist insbesondere dann der Fall, wenn die angeforderten Dokumente **wirtschaftlich sensible Informationen** enthalten, die sich etwa auf die Geschäftsstrategien der betroffenen Unternehmen oder auf deren **Kundenbeziehungen** beziehen, oder wenn sie unternehmensspezifische Informationen enthalten, die Rückschlüsse auf deren Fachkenntnisse zulassen. Ebenso darf der Zugang zum Schutz personenbezogener Daten **verweigert** werden, wobei es für den **Personenbezug** genügt, wenn es möglich ist, die in einem Dokument enthaltenen Informationen mit einer natürlichen Person zu verknüpfen. Personenbezogen sind zudem auch **berufliche Daten** ([EuG 15.10.2025, T-291/23, MeSoFa](#)).

#### **NACHTRAG**

- Der EuGH hat die Rs C-40/25, CRIF aus seinem **Register gestrichen**. ([EuGH 30.09.2025, C-40/25, CRIF](#)). Das OLG Wien fragte den EuGH, ob unter der DSGVO ein Anspruch auf **Unterlassung** der (rechtswidrigen) Weitergabe personenbezogener Daten besteht, wenn die Löschung der personenbezogenen Daten nicht verlangt wird. Nachdem der EuGH diese Rechtsfrage in der Rs *Quirin Privatbank* ([C-655/23](#)) beantwortet hat, zog das OLG Wien sein Vorabentscheidungsersuchen zurück.

#### Rechtsprechung des VfGH

##### Aus der Rechtsprechung des VfGH:

- Bereits getilgte **strafgerichtliche Verurteilungen** (Daten iSd Art 10 DSGVO) dürfen bei der

**Staatsbürgerschaftsverleihung** für die (negative) Prognoseentscheidung berücksichtigt werden ([VfGH 24.09.2025, E1925/2025](#)).

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Die datenschutzrechtliche **Verantwortlichenstellung** ist im **öffentlichen Bereich** einzelfallbezogen zu beurteilen. Maßgeblich sind die **funktionelle Zuständigkeit** und die **organisatorische Einbindung** des Handelnden. Zwar kann eine Behörde oder Einrichtung grundsätzlich Verantwortlicher sein; die Frage, ob in einer konkreten Konstellation der Geschäftsapparat oder nur das monokratische Organ Verantwortlicher ist, ist jedoch nach den Umständen des Einzelfalls zu beantworten. Diese einzelfallbezogene Beurteilung ist – sofern verfahrensrechtlich einwandfrei und vertretbar – nicht revisibel. In einem Verwaltungsstrafverfahren nach der **StVO** handelt der **städtische Magistrat nicht als eigenständiger Verantwortlicher**, sondern lediglich als Hilfsorgan des Bürgermeisters, der die Zuständigkeit für die betreffenden Verwaltungsstrafverfahren innehat ([VwGH 16.09.2025, Ra 2023/04/0008](#)). **Anm: Das könnte betreffend die Stadt Wien anders gesehen werden.**
- Das aufgrund einer Datenschutzbeschwerde geführte Verfahren ist ein **antragsgebundenes Verfahren**. Die **Benennung des Beschwerdegegners** liegt grundsätzlich in der **Disposition des Betroffenen**. Benennt der Betroffene unmissverständlich bzw unzweifelhaft eine bestimmte Person als Verantwortlichen, hat die **DSB keine Möglichkeit**, das Verfahren gegen eine andere Person zu führen ([VwGH 22.09.2025, Ra 2023/04/0108](#)).

### Rechtsprechung der Justiz

Aus der Rechtsprechung der Justiz:

- Das **Recht auf Auskunft** steht unter **keinen Voraussetzungen** und muss nicht mit einem **Rechtsschutzinteresse** begründet werden. Eine Auskunftspflicht besteht auch dann, wenn das Auskunftersuchen nicht den in dem ErwGr 63 genannten Zwecken (Überprüfung der Rechtmäßigkeit, Bewusstsein der Verarbeitung) dient. Ein Auskunftersuchen kann nicht bloß deswegen abgelehnt werden, weil damit primär die **Beweismittelbeschaffung** beabsichtigt wird. Auch liegt **keine** offenkundige Unbegründetheit oder **Rechtsmissbrauch** vor, wenn mit dem Ersuchen **datenschutzfremde Ziele** verfolgt werden. Rechtsmissbrauch liegt nur vor, wenn die zwischen den verfolgten eigenen Interessen und den

beeinträchtigten Interessen des anderen ein krasses Missverhältnis besteht. Das Einklagen von einem allfälligen Saldo ist ein legitimes Interesse. Das **Geheimhaltungsinteresse** gemäß § 4 Abs 6 DSGVO greift nicht, wenn es sich bei den begehrten Daten um Daten aus einer **gemeinsamen Geschäftsverbindung** handelt ([OLG Linz 30.06.2025, 4R89/25y](#)).

- Was zwischen den Streitparteien vereinbart wurde und welcher Vertrag abgeschlossen wurde, sind **Rechtsfragen**. Zur RechtsEbene gehört es auch, zu beurteilen, wer **Verantwortlicher oder Auftragsverarbeiter** ist und ob die "Überprüfung der Provisionsabrechnungen" ein zulässiger **Verarbeitungszweck** ist ([OLG Wien 24.02.2025, 1R125/24w](#)).
- **Akteneinsicht** durch einen Dritten führt regelmäßig zu einem Eingriff in die Grundrechte auf **Datenschutz** und auf Achtung des **Privat- und Familienlebens**. Der Gewährung der Akteneinsicht stehen jedoch **keine überwiegenden privaten Interessen** entgegen, wenn der Einsichtswerber über die im Akt enthaltenen Informationen bereits Kenntnis hat ([OLG Linz 11.09.2025, 10Bs198/25a](#)).

### Rechtsprechung des BVwG

BVwG 10.06.2024, W148 2291941-1

#### **WiEReG, public watchdog, Einsichtsrecht**

- Ein Investigativjournalist beantragte beim Bundesminister für Finanzen (**BMF**) Einsicht in das Register der wirtschaftlichen Eigentümer (**WiERe**) zu einer bestimmten Gesellschaft, einschließlich mehrerer Auszüge und eines Compliance-Packages. Er berief sich auf seine Tätigkeit im Bereich der Geldwäscheprävention, Terrorismusfinanzierung und Sanktionsumgehung und seine Rolle als "**public watchdog**". Der BMF wies den Antrag zurück, weil der Journalist nicht zu den in § 9 Abs 1 WiEReG genannten Verpflichteten gehöre und nicht über die Berechtigungen für Auszüge sowie für Einsicht verfüge. Einsicht sei nur nach § 10 WiEReG bei Nachweis eines berechtigten Interesses möglich. Gegen den Zurückweisungsbescheid erhob der Journalist (erfolglos) Beschwerde an das BVwG.

Das BVwG hat erwogen: § 9 Abs 1 WiEReG zählt taxativ die zur Einsicht in das **WiERe** berechtigten Verpflichteten auf. § 10 WiEReG berechtigt natürliche Personen und Organisationen, die ein berechtigtes Interesse nachweisen können, zur Einsicht in das **WiERe**. Ein solches berechtigtes Interesse ist bei Angehörigen von journalistischen Berufen anzunehmen, die einen Bezug zur Verhinderung der Geldwäsche, der Terrorismusfinanzierung oder der Umgehung von

vorgenannten Sanktionsmaßnahmen aufweisen.

Der Unterschied zwischen den nach § 9 und § 10 WiEReG zur **Einsicht Berechtigten** liegt in deren Betroffenheit. Während die Verpflichteten sowie die öffentlichen Einrichtungen persönlich betroffen sind, sind die nach § 10 WiEReG zur Einsicht Berechtigten nicht persönlich betroffen, sondern es besteht ein vom Gesetz anerkanntes berechtigtes Interesse zur Einsicht. Schon aus dieser Systematik erschließt sich, dass aus § 9 WiEReG kein erweitertes Einsichtsrecht zur Wahrung gesamtgesellschaftlicher Interessen interpretiert werden kann.

Der Gesetzgeber hat die Aufgabe der Journalisten als "public watchdog" in § 10 WiEReG anerkannt und ihnen (bestimmte) **Einsichtsrechte** zugestanden. Dieses Einsichtsrecht umfasst *expressis verbis* nicht die begehrten Auszüge oder Compliance-Packages. Da der Journalist kein Verpflichteter ist, steht ihm ein **erweitertes Einsichtsrecht** nach § 9 Abs 5a WiEReG nicht zu.

BVwG 11.07.2025, W292 2291080-1

### **Medien, Bürgerjournalismus, Verschwörungstheorie**

- Ein Journalist betrieb als Medieninhaber eine Website, auf welcher ua Aufrufe zu Demonstrationen, Diskussionsveranstaltungen, Buchvorstellungen und Beiträge zum Gaza-Konflikt veröffentlicht wurden. Die Texte stammten von verschiedenen Autoren, darunter auch vom Journalisten selbst. Der Journalist bezeichnet sich als Chefredakteur der Website. Die Struktur der Redaktion ist nicht das entscheidende "Zentralorgan", sondern es sollen Entscheidungen über zu publizierende Inhalte in Diskussion mit den selbständigen Mitgliedsgruppen und dem Team getroffen werden. Im Jahr 2023 veröffentlichte der Journalist einen Beitrag, in dem er das Vorgehen der Polizei bei Versammlungen kritisierte. Dem Artikel war eine ungeschwärzte Lagebeurteilung beigelegt, in der der vollständige Name eines Beamten als Verfasser aufschien. Zu einem nicht feststellbaren Zeitpunkt wurde der Name von der Website entfernt. Die DSB sah in der Veröffentlichung des Namens des Beamten auf der Website eine Verletzung seines Rechts auf Geheimhaltung. Sie trug dem Journalisten auf, die personenbezogenen Daten zu löschen. Dagegen erhob dieser (erfolglos) Beschwerde an das BVwG.

Das BVwG hat erwogen: Ein **Vergleich** mit einer Veröffentlichung von Informationen in einem **Printmedium** ist **nicht geboten**, weil einmal im öffentlich zugänglichen Internet veröffentlichte Informationen nicht

ohne Weiteres wieder entfernt werden können.

Die Bestimmung des neuen § 9 Abs 1 DSGVO (**Medienprivileg**) erfasst wie bisher den Kreis der professionell am Journalismus mitwirkenden Organe und Personen. Daneben gilt das Medienprivileg nach § 9 Abs 1a DSGVO auch für journalistisch selbständig tätige Personen außerhalb von Medienunternehmen, sog **Bürgerjournalismus**, allerdings in sachlich eingeschränkter Form.

Ein **Medieninhaber** nach dem MedienG wird iSd **§ 1 Abs 1 Z 6 MedienG** erst dann zum Medienunternehmer, wenn er über den Zweck der bloßen Verbreitung von Inhalten hinaus ein Unternehmen betreibt, dessen Unternehmenszweck die inhaltliche Gestaltung der Website ist, die von einer Redaktion und einer Vielzahl angestellter bzw freier Medienmitarbeiter vorgenommen wird. Entsprechendes konnte für die Website allerdings nicht festgestellt werden. Auch das Privileg des **§ 9 Abs 1 DSGVO** findet auf den Journalisten als datenschutzrechtlich Verantwortlichen iSd Art 4 Z 7 DSGVO **keine Anwendung**.

Zwar kann die Tätigkeit des Journalisten unter die Bestimmung des § 9 Abs 1a DSGVO subsumiert werden, jedoch enthält diese Bestimmung – im Unterschied zu § 9 Abs 1 Z 2 DSGVO – **keinen eigenständigen Erlaubnistatbestand** für Verarbeitungsvorgänge zu journalistischen Zwecken, sondern erklärt lediglich die Ausnahmetatbestände des § 9 Abs 1 Z 1, Z 4 und Z 13 DSGVO für anwendbar. Hieraus folgt, dass die Verarbeitung personenbezogener Daten zu **journalistischen Zwecken**, sofern diese nicht in einem Medienunternehmen iSv § 1 Abs 1 Z 6 DSGVO erfolgt, im Rahmen der **Erlaubnistatbestände der Art 6, 9 und 10 DSGVO** zu beurteilen ist.

Der Beitrag erweist sich jedenfalls als unsachlich. Er weist verschwörerische und antisemitische Meinungen auf und rückt Organwalter der Versammlungsbehörde in die Nähe eines faschistischen Regimes. Mit dem Online-Beitrag des Journalisten liegt somit kein Beitrag zu einer **Debatte von allgemeinem Interesse vor**. Auch eine Betätigung im Bürgerjournalismus erfordert eine in Grundzügen ausgewogene Darstellung des Meinungsdiskurses. Eine agitative und ins verschwörungstheoretische abgleitende Rhetorik ist hingegen geeignet, die Grenzen einer sachlich geführten Debatte im allgemeinen Interesse zu überschreiten. Folglich hat der Journalist mit der Veröffentlichung **kein (legitimes) berechtigtes Interesse** iSd Art 6 Abs 1 lit f DSGVO verfolgt.

### **ELGA, Auskunft, Feststellungsinteresse, Erkundungsbeweis**

- Ein Auskunftswerber richtete ein Auskunftersuchen an die **ELGA GmbH**. Zusätzlich verlangte er die Beantwortung mehrerer allgemeiner Fragen. Die ELGA GmbH hatte vor dem Auskunftersuchen keine Daten des Auskunftswerbers, lediglich die Daten aus dem Ersuchen. Nachdem die Beantwortungsfrist verstrich und die Fragen seines Erachtens nicht beantwortet wurden, richtete er eine Datenschutzbeschwerde an die DSB. In dieser machte er eine Verletzung im Recht auf Auskunft, im Recht auf fristgerechte Auskunft sowie im Recht auf Information geltend. Die DSB stellte das Verfahren hinsichtlich der nicht erteilten Auskunft ein und wies die Datenschutzbeschwerde bezüglich der Mangelhaftigkeit der Auskunft ab. Dagegen richtete der Auskunftswerber eine (erfolglose) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die Bestimmungen der DSGVO verlangen **keine Feststellung** einer Rechtsverletzung. Weder Art 77 DSGVO noch Art 15 DSGVO sehen dies vor. Das Auskunftsrecht muss einem Betroffenen die Möglichkeit einräumen, zu erfahren, zu welchen Zwecken personenbezogene Daten verarbeitet werden, wie lange sie gespeichert werden und wer die Empfänger der Daten sind. Im Falle einer automatisierten Entscheidungsfindung einschließlich Profiling muss auch eine Information zu der Logik, nach der die Verarbeitung der Daten erfolgt, und zu den möglichen Folgen einer solchen Verarbeitung erteilt werden.

Es ist nicht erforderlich, eine **Feststellung** über eine Rechtsverletzung zu treffen, wenn der Auskunftspflichtige dem Ersuchen während des laufenden Verfahrens **nachkommt**. Diesfalls hat der Betroffene sein **Rechtsschutzziel** erreicht. Die Frage der verspäteten Auskunft wird in dem Verfahren über das Ersuchen auf Auskunftserteilung nicht geklärt und steht einem **Schadenersatzanspruch** wegen der verspätet erteilten Auskunft nicht entgegen. Feststellungen der Aufsichtsbehörde sind keine Voraussetzung für eine Schadenersatzklage vor den Zivilgerichten. Eine **entscheidende Erleichterung** bei der Geltendmachung weiterer Ansprüche begründet kein rechtliches Interesse an einem Feststellungsbescheid.

Ist ein Betroffener nach einer Auskunft der Meinung, es wurden nicht alle Daten beauskunftet, muss er dies im Vorbringen **substantiiert darlegen**. Ein bloß allgemeines Vorbringen ist ein unzulässiger **Erkundungsbeweis**, zu dessen Aufnahme das Verwaltungsgericht nicht verpflichtet ist.

Verarbeitet ein Verantwortlicher keine Daten eines Betroffenen, ist ein Nachweis für

die Einhaltung der Grundsätze der Verarbeitung nach Art 5 Abs 1 DSGVO nicht möglich.

#### Aus der weiteren Rechtsprechung des BVwG:

- Eine Videoüberwachung gemäß Art 6 Abs 1 lit f DSGVO kann zulässig sein, wenn sie der Wahrung berechtigter Interessen dient. Eine **kontinuierliche Videoüberwachung**, die auch den **öffentlichen Raum** und dort zufällig vorbeikommende Fußgänger und Verkehrsteilnehmer erfasst, ist jedoch nicht erforderlich und verletzt den **Grundsatz der Datenminimierung**. Weiters wird gegen das **Transparenzgebot** und die **Informationspflicht** verstoßen, weil die Videoüberwachung **nicht gekennzeichnet** wurde. Die Unbescholtenheit des Verantwortlichen sowie die umgehende Einstellung der Videoüberwachung nach Zustimmung der Aufforderung zur Rechtfertigung waren als strafmildernd zu berücksichtigen. Die Geldbuße ist daher von EUR 3.190 auf EUR 1.100 herabzusetzen ([BVwG 26.02.2025, W101 2284403-1](#)).
- Ist dem Verantwortlichen nicht bekannt, welche konkreten personenbezogenen Daten an welche konkreten Empfänger weitergegeben wurden und kann dies auch nicht rekonstruiert werden, ist die Auskunft vollständig erteilt, wenn alle Auftragsverarbeiter aufgelistet werden und bekanntgegeben wird, für welche Zwecke personenbezogene Daten an welche konkreten Empfänger weitergegeben werden konnten ([BVwG 18.07.2025, W292 2235791-1](#)).

#### Rechtsprechung der LVwG

LVwG Tirol 06.10.2025, LVwG-2025/S2/1049-8

#### **Vergabeverfahren, Rollenverteilung, Auftragsverarbeiter, Pseudonymisierung**

- Eine **öffentliche Auftraggeberin** schrieb die Belieferung mit Herzschrittmachern plus Elektroden und Zubehör europaweit aus. Die Ausschreibungsunterlagen enthielten spezielle Regelungen zu telemedizinischen Leistungen, die ua datenschutzrechtliche Fragen betrafen. Die Auftraggeberin sah darin datenschutzrechtlich getrennte Rollen vor, wonach die Auftragnehmer als Verantwortliche für die Systemverarbeitung im externen Datenraum zuständig sein sollten. Daher sah die Auftraggeberin keinen Anlass, einen Auftragsverarbeitungsvertrag iSd Art 28 DSGVO abzuschließen. Ein Interessent wies die Auftraggeberin darauf hin, dass der Auftragnehmer lediglich als **Auftragsverarbeiter** im Auftrag der Auftraggeberin tätig werden würde. Die Ausschreibung würde daher der DSGVO widersprechen und sei rechtswidrig. Nachdem die Auftraggeberin an ihrer

Rechtsauffassung festhielt und die Ausschreibung nicht berichtigte, beantragte der Interessent eine Nachprüfung der Ausschreibung. Das LVwG Tirol wies den Nachprüfungsantrag ab.

Das LVwG Tirol hat erwogen: Während der Verantwortliche die Zwecke und Mittel der Verarbeitung festlegt, dh, das "Warum" und "Wie" der Verarbeitung, muss der Auftragsverarbeiter personenbezogene Daten im Auftrag und nach den Weisungen des Verantwortlichen verarbeiten.

Die Auslesung der Daten nach dem Einsetzen des Herzschrittmachers wird durch ein externes Gerät des Auftragnehmers erfolgen, das diverse Daten speichern wird. Der Auftragnehmer wird die technische Infrastruktur (Cloud, Geräte, Plattformen) zur Erhebung und Speicherung der Daten vollkommen eigenständig betreiben. Dabei wird der Auftragnehmer selbst über die **Verarbeitungsmodalitäten** wie zB verwendete Datenkategorien, Speicherdauer, Sicherheitsmaßnahmen etc, entscheiden, die zumindest teilweise als **wesentliche Mittel** zu qualifizieren sind.

Zudem kann davon ausgegangen werden, dass der Auftragnehmer die Volldatensätze zur **internen Qualitätssicherung**, Systemwartung und Verbesserung sowie zur **Produktentwicklung** verwenden wird.

Die vom Auftragnehmer gesammelten Daten sind personenbezogene Daten. Das Argument des Interessenten, dass es sich um keine personenbezogenen Daten handeln würde, weil eine **Pseudonymisierung** erfolgen würde und daher weder Klarnamen noch Geburtsdatum der Patienten ersichtlich sei, greift nicht. Auch wenn der Patientenname nicht unmittelbar nachverfolgt werden kann, ist eine Verknüpfung dadurch möglich, dass jedem Patienten über die Seriennummer des Herzschrittmachers die entsprechenden personenbezogenen Daten zugeordnet werden können. Eine Pseudonymisierung schließt das Vorliegen von personenbezogenen Daten nicht aus. Der Auftragnehmer wird somit die Daten einerseits für die Ärzte und Kliniken erheben und andererseits zur Weiterentwicklung seiner eigenen Produkte verwenden. Vor diesem Hintergrund ist der Auftragnehmer zweifelsfrei als **Verantwortlicher** zu qualifizieren.

Die Verantwortlichkeit der Auftraggeberin wiederum setzt erst dann ein, wenn die gespeicherten Volldatensätze zum Zweck der Behandlung des Patienten beim Arzt oder in der Klinik abgefragt und weiterverarbeitet werden. Die Auftraggeberin ist daher in ihrer Ausschreibung zu Recht von einer **getrennten datenschutzrechtlichen Verantwortlichkeit** ausgegangen.

Aus der weiteren Rechtsprechung der LVwG:

- Für die Beurteilung der Zulässigkeit der Weitergabe personenbezogener Daten ist die **DSB zuständig** ([LVwG NÖ 23.09.2025, LVwG-M-32/001-2025](#)).

### **Rechtsprechung der DSB**

[DSB 12.09.2025, 2025-0.703.379](#)

### **IFG, Auskunftspflicht, sachlicher Anwendungsbereich**

- Ein Bürger richtete unter Berufung auf das Auskunftspflichtgesetz (AuskPflG) zwei Anfragen an die DSB. Am 01.09.2025 stellte er eine weitere Anfrage nach dem neuen Informationsfreiheitsgesetz (**IFG**). Die Anfragen betrafen ua Bewertungen angeblicher Rechtsmissbrauchsfälle, Begründungen für behördliches Vorgehen, künftige Bearbeitungszeiten, die Vorgehensweise iZm der Sicherung von datenschutzrechtlichen Betroffenenrechten sowie die Zulässigkeit elektronischer Zustellungen.

Die DSB hat erwogen: Mit 01.09.2025 sind das AuskPflG und die entsprechende verfassungsrechtliche Bestimmung außer Kraft getreten. Gleichzeitig wurde ein neues Grundrecht auf Zugang zu Informationen geschaffen, das auf einfachgesetzlicher Ebene durch das IFG geregelt wird.

Die noch nach dem AuskPflG gestellten Anfragen sind daher in Ermangelung anderslautender **Übergangsbestimmungen** nach der nunmehr geltenden Rechtslage und damit nach Art 22a Abs 2 B-VG bzw dem IFG zu beurteilen.

Da die vom **VwGH** zum AuskPflG erarbeiteten **Leitlinien übertragbar** sind, sind Behörden im Rahmen ihrer Auskunftspflicht nicht verpflichtet, ihre **Handlungen und Unterlassungen** anfragenden Bürgern gegenüber zu begründen und damit letztlich zu rechtfertigen. Unter die Informationspflicht fällt auch nicht die **Äußerung von Rechtsmeinungen**, weil die Verwaltung nicht zu umfangreichen Ausarbeitungen oder zur Erstellung von (Rechts-)Gutachten verpflichtet ist. Auch dient das IFG nicht dazu, Antragstellern die Möglichkeit zu bieten, ihr **"Unbehagen"** an Bescheiden oder der sonstigen Vorgangsweise einer Behörde kundzutun.

Die vom Antragsteller erfragten Rechtsmeinungen und Begründungen von behördlichem Handeln sind nicht unter den Informationsbegriff nach § 2 Abs 1 IFG zu subsumieren und daher **nicht vom Anwendungsbereich** des IFG erfasst. Informationen über den Bearbeitungszeitpunkt von Verfahren sind zum Zeitpunkt der Anfrage nicht bekannt. Es handelt sich dabei um zukünftige Willensbildungen der Datenschutzbehörde. **Anm: Tatsächlich enthält Art 151**

Abs 68 letzter Satz B-VG eine entsprechende Übergangsbestimmung.

bisher – als Auftragsverarbeiter, sondern als **Verantwortliche** gelten.

Aus der weiteren Rechtsprechung der DSB:

- Die Videoüberwachung der **Eingabetastatur** von **Selbstbedienungskassen** ist ohne Verpixelung nicht erforderlich. Der Verantwortliche hat mit solchen und weiteren Videokameras, deren Aufnahmebereiche unangemessen waren, gegen die DSGVO verstoßen und ist mit **Geldbuße** iHv **EUR 1,5 Mio** zu bestrafen ([DSB 16.08.2024, 2023-0.680.196](#)). **Anm: Dieses Straferkenntnis der DSB ist vom BVwG mit Erkenntnis vom 25.07.2025, W258 2299744-1, der Höhe nach bestätigt worden. Die Zusammenfassung kann im Schön-herr Datenschutzmonitor 41/2025 vom 15.10.2025 nachgelesen werden.**

### **EU-Rechtsakte**

- Am **16.10.2025** ist der Entwurf der "*Commission Delegated Regulation supplementing Regulation (EU) 2024/2847 of the European Parliament and of the Council by specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications*", [Ares\(2025\)8809980](#), veröffentlicht worden. Mit dieser DelegiertenVO wird die **Cyberresilienzverordnung 2024/2847 (CRA)** dahingehend konkretisiert werden, dass Bedingungen für die Verzögerung der Übermittlung einer Sicherheitsmeldung durch das nationale Reaktionsteam für IT-Sicherheitsvorfälle (**CSIRT**) unter außergewöhnlichen Umständen festgelegt werden.

### **Nationale Rechtsakte**

- Am **16.10.2025** wurde das "*Bundesgesetz, mit dem das Bundesgesetz zur Sicherstellung eines hohen Resilienzniveaus von kritischen Einrichtungen (Resilienz kritischer Einrichtungen-Gesetz; RKEG) erlassen und das Tilgungsgesetz 1972 geändert wird*", [BGBl I 2025/60](#), kundgemacht. Mit dem RKEG wird die RL (EU) 2022/2557 über die **Resilienz kritischer Einrichtungen (RKE-RL)** ins innerstaatliche Recht umgesetzt. Als zuständige Behörde und datenschutzrechtlich Verantwortlicher ist der **Bundesminister für Inneres** festgelegt worden. **Anm: Die NIS-2-RL ist noch nicht umgesetzt.**
- Am **16.10.2025** wurde das "*Bundesgesetz, mit dem das ORF-Beitrags-Gesetz 2024 geändert wird*", [BGBl 2025/59](#), kundgemacht. Das ORF-Beitrags-Gesetz (**OBG**) wird ua dahingehend novelliert, dass beauftragte **Inkassounternehmen** nicht mehr – wie

to the point

# Datenschutzmonitor. 43/2025 vom 29.10.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Abonnieren Sie auch unsere anderen periodischen Newsletter, **Digital Law Monitor**, **Technology & Digitalisation**, **Financial Regulation** und **Healthcare & Life Sciences** für regelmäßige, prägnante Updates [hier](#).

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des VfGH**

VfGH 07.10.2025, G62/2025 (WiEReG, public watchdog, Interessenabwägung, Gleichheitsgrundsatz)

VfGH 07.10.2025, G26/2025 (BilDokG, Interessenabwägung, Verfassungswidrigkeit)

VfGH 07.10.2025, G116/2025 (Offenlegungspflicht, Jahresabschluss, Beugemittel)

- **Rechtsprechung des VwGH**

VwGH 25.09.2025, Ra 2023/04/0279 (Melderegisterabfrage, Aufgabe im öffentlichen Interesse, Unzulässigkeit)

- **Rechtsprechung der Justiz**

OLG Wien 10.01.2025, 33R157/24m; 11.04.2025, 16R21/25p (Auskunftsrecht, Identitätsprüfung, Vollmacht, Kostenrekurs)

OLG Wien 19.05.2025, 33R10/25w (AGB, elektronische Post, Rechtsgrundlage)

OLG Wien 26.06.2025, 2R37/25p (Geschäftsführer, interne Datenübermittlung)

OLG Linz 10.09.2025, 4R114/25z (Akteneinsicht, Geheimhaltung, schutzwürdige Interessen)

- **Rechtsprechung des BVwG**

BVwG 19.08.2025, W292 2307870-1 (Auskunft, Formalismus)

BVwG 15.09.2025, W256 2317747-1 (Beschreibbeschwerde, Voraussetzungen)

BVwG 04.09.2025, W252 2301118-1 (fehlende Betroffenheit, Zurückweisung)

BVwG 04.09.2025, W252 2312918-1 (Auskunftsrecht, Datenkopien, Beweislast)

BVwG 10.09.2025, W258 2299744-1 (aufschiebende Wirkung, Strafvollzug)

- **Rechtsprechung des BFG**

BFG 14.10.2025, RV/7103129/2025 (Spenden, Identifikationsdaten)

- **Rechtsprechung der LVwG**

LVwG NÖ 09.10.2025, LVwG-AV-436/001-2025 (KFZ-Zulassungsevidenz, rechtliches Interesse)

- **Nationale Rechtsakte**

Initiativantrag StrEU-AG 2025

Ministerialentwurf zu Transparenz und das Targeting politischer Werbung



## To the Point:

### Rechtsprechung des VfGH

VfGH 07.10.2025, G62/2025

#### **WiEReG, public watchdog, Interessenabwägung, Gleichheitsgrundsatz**

- Ein Journalist beantragte beim Bundesminister für Finanzen (**BMF**) als Registerbehörde die Übermittlung eines (i) **Auszugs** aus dem Register der wirtschaftlichen Eigentümer ("**Register**"), (ii) **erweiterten Auszugs** sowie (iii) **Compliance-Packages**, jeweils gestützt auf unterschiedliche Bestimmungen des § 9 WiEReG.

Der BMF wies den Antrag des Journalisten mit Bescheid zurück, weil Auszüge gemäß § 9 WiEReG nur von Verpflichteten iSd § 9 WiEReG übermittelt werden dürfen. Eine Einsicht ins Register aufgrund von **berechtigten Interessen** sei nur nach § 10 WiEReG vorgesehen. Die Bescheidbeschwerde des Journalisten wurde vom BVwG abgewiesen, weil dem Journalisten kein über § 10 WiEReG hinausgehendes Einsichtsrecht zukomme und die Aufgabe von Journalisten als "**public watchdogs**" durch die Regelung des § 10 WiEReG ausreichend berücksichtigt sei.

Der VfGH fasste einen Prüfungsbeschluss zur Überprüfung der Verfassungskonformität des § 10 WiEReG. Der VfGH hegte Bedenken wegen der (i) Beschränkung des **Personenkreises**, dem nach § 10 WiEReG ein Einsichtsrecht in das Register zukommt, (ii) womöglich unverhältnismäßigen **Beschränkung des Einsichtsrechts** dieses Personenkreises sowie (iii) unterschiedlichen Ausgestaltung des Einsichtsrechts der Verpflichteten nach § 9 WiEReG und der Personen mit berechtigtem Interesse nach § 10 WiEReG, die gegen den **Gleichheitsgrundsatz** verstoßen könnte. Die Bedenken des VfGH zu Pkt i und iii konnten im Gesetzgebungsverfahren zerstreut werden. Die Bedenken zu Pkt ii wurden bestätigt.

Der VfGH hat erwogen: Mit dem Anknüpfen an ein **spezifisches berechtigtes Interesse** hat der Gesetzgeber im Einklang mit den unionsrechtlichen Grundlagen und der Rechtsprechung des EuGH eine **sachliche Interessenabwägung** getroffen, indem er den **Personenkreis** mit Einsichtsrecht auf solche Personen beschränkte, die einen Bezug zu den die Datenerhebung tragenden Zwecken aufweisen.

Die **Beschränkung des Umfangs des Einsichtsrechts** in § 10 WiEReG war jedoch unverhältnismäßig, weil auch Informationen von **öffentlichem Interesse** angenommen wurden, an denen kein überwiegendes schutzwürdiges Interesse der Rechtsträger, deren Daten ins Register eingetragen sind, bestand.

Die **Differenzierung** zwischen Verpflichteten iSd § 9 WiEReG und den Personen mit berechtigtem Interesse gemäß § 10 WiEReG verletzt den **Gleichheitsgrundsatz** nicht, weil die Verpflichteten zur Einsicht ins WiEReG verpflichtet sind und sie die abgefragten Informationen nur **vertraulich und zweckgebunden** behandeln dürfen. Die Aufgabe der Personen mit berechtigtem Interessen ("**public watchdogs**") ist hingegen gerade, diese Informationen der **Öffentlichkeit** zur Verfügung zu stellen.

Da die entsprechende Bestimmung des WiEReG zur Beschränkung des Umfangs des Einsichtsrechts bereits außer Kraft getreten ist, hat sich der VfGH auf die **Feststellung der Verfassungswidrigkeit** dieser Bestimmung zu beschränken.

VfGH 07.10.2025, G26/2025

#### **BilDokG, Interessenabwägung, Verfassungswidrigkeit**

- Ein Journalist richtete ein Auskunftsbegehren an den Bundesminister für Bildung, Wissenschaft und Forschung (**BMBWF**) betreffend schulstandortbezogene Daten zur Zentralmatura für die Jahre 2018 bis 2023, gegliedert nach Fächern, Terminen und Ergebnissen samt Kompensationsprüfungen. Der BMBWF verweigerte die Auskunft unter Hinweis auf § 21 Abs 5 Bildungsdokumentationsgesetz (BilDokG) und übermittelte das Auskunftsbegehren betreffend eines Bescheids an die Bildungsdirektion für Vorarlberg als zuständige Bildungsbehörde. Nachdem die Bildungsdirektion einen abweisenden Bescheid erließ, erhob der Journalist Bescheidbeschwerde an das BVwG und äußerte Zweifel an der Verfassungsmäßigkeit des § 21 Abs 5 BilDokG. Das BVwG teilte seine Bedenken und leitete ein Gesetzesprüfungsverfahren beim VfGH ein. Da die Bestimmung mit 01.09.2025 außer Kraft getreten ist, stellte der VfGH bloß ihre Verfassungswidrigkeit fest.

Der VfGH hat erwogen: § 21 Abs 5 BilDokG verbot die Auskunft über **schulstandortbezogene Daten** – auch in aggregierter Form – und galt nicht nur für personenbezogene Daten iSd Art 4 Z 1 DSGVO, sondern auch für sonstige Daten.

Ein **Zugang zu Informationen** fällt unter Art 10 Abs 1 EMRK, wenn er für die **Ausübung der Meinungsfreiheit** maßgeblich ist. Dabei ist zu beachten, ob **journalistische Recherche** vorliegt, die Offenlegung im **öffentlichen Interesse** liegt, die Information **bereit und verfügbar** ist und die Person als Journalist die Funktion eines "**public watchdogs**" ausübt. Ein Eingriff kann gemäß Art 10 Abs 2 EMRK gerechtfertigt sein, wenn eine gesetzliche Grundlage vorliegt, ein legitimes Ziel verfolgt wird und der Eingriff verhältnismäßig ist. Die

gesetzliche Grundlage muss eine **Abwägung** zwischen **Geheimhaltungsinteressen** und **Informationsinteressen** ermöglichen. Ziel des § 21 Abs 5 BildDokG war der Schutz eines unbeeinträchtigten und ordnungsgemäßen Schulablaufs. Allerdings sah § 21 Abs 5 BildDokG ein **absolutes Verbot** vor und umfasste auch **nichtpersonenbezogene Daten**. Da die Bestimmung keine einzelfallbezogene Interessenabwägung zwischen Verschwiegenheitspflichten und Auskunftsinteressen vorsah, die zentrale Rolle von Medien als public watchdogs missachtete und geeignet war, journalistische Tätigkeit in unverhältnismäßiger Weise zu behindern oder sogar auszuschließen, verstieß sie gegen das Grundrecht auf freie Meinungsäußerung und Informationsfreiheit gemäß Art 10 EMRK.

Aus der weiteren Rechtsprechung des VfGH:

- Die Pflicht zur Offenlegung des **Jahresabschlusses** gemäß § 277 UGB und das **Zwangsstrafenverfahren** nach § 283 UGB verstoßen weder gegen den Gleichheitsgrundsatz noch gegen das Recht auf Eigentum oder auf Datenschutz. Die Ausnahme von Personengesellschaften ist aufgrund der unterschiedlichen Haftungssituation sachlich gerechtfertigt. Die wiederholte Verhängung gestaffelter, begrenzter Zwangsstrafen ist ein zulässiges Beugemittel ([VfGH 07.10.2025, G116/2025](#)).

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Gemäß § 16a Abs 4 MeldeG ist der Bundesminister für Inneres (BMI) ermächtigt, Organen von Gebietskörperschaften auf deren Verlangen eine **Abfrage im Zentralen Melderegister** in der Weise zu eröffnen, dass sie, soweit dies zur **Besorgung einer gesetzlich übertragenen Aufgabe** erforderlich ist, den Gesamtdatensatz bestimmter Menschen im Datenfernverkehr ermitteln können. Nach § 20 Abs 3 MeldeG sind Organen der Gebietskörperschaften **auf Verlangen** die im Melderegister oder im Zentralen Melderegister enthaltenen Meldedaten von den Meldebehörden zu übermitteln. Dies gilt, sofern diese für den Empfänger zur **Wahrnehmung der ihm gesetzlich übertragenen Aufgaben** eine wesentliche Voraussetzung bilden. Die **Kontrolle der Einhaltung der Vorschriften des Tierschutzgesetzes** ist eine der Tierschutzbehörde übertragene, im öffentlichen Interesse liegende Aufgabe. Die Meldedatenabfrage war zur Erfüllung dieser Aufgabe geeignet und erforderlich ([VwGH 25.09.2025, Ra 2023/04/0279](#)).

### Rechtsprechung der Justiz

OLG Wien 10.01.2025, 33R157/24m; 11.04.2025, 16R21/25p

#### **Auskunftsrecht, Identitätsprüfung, Vollmacht, Kostenrekurs**

- Zwei Spieler forderten über ihre anwaltliche Vertretung von einer maltesischen Online-Glücksspielanbieterin Auskunft über ihre Ein- und Auszahlungen, Einsätze, Gewinne, Verluste sowie Kopien personenbezogener Daten. Den Auskunftersuchen waren Vollmachten und Ausweiskopien der Spieler angeschlossen. Die Glücksspielanbieterin verweigerte die Auskünfte und forderte "handschriftlich in Tinte" unterzeichnete Vollmachten. Nachdem Klagen erhoben wurden, übermittelte die Glücksspielanbieterin sämtliche geforderte Daten. In Folge der Erfüllung der Klagebegehren schränkten die Spieler ihre jeweilige Klage auf Kosten ein. Das Erstgericht sprach ihnen die Prozesskosten zu. Dagegen erhob die Glücksspielanbieterin (erfolglos) Kostenrekurse an das OLG Wien.

Das OLG hat erwogen: Voraussetzung für einen Kostenanspruch nach § 45 ZPO ist, dass der Anspruch berechtigt ist, der Beklagte ihn bei erster Gelegenheit anerkennt und dieser **keinen Anlass zur Klage** gegeben hat.

Gemäß Art 12 Abs 6 DSGVO darf ein Verantwortlicher zusätzliche Informationen anfordern, wenn **begründete und einzelfallbezogene Zweifel** an der Identität bestehen. Diese Bestimmung ermächtigt aber zu **keiner routinemäßigen Identitätsüberprüfung**. Als Nachweis genügt bei einem schriftlichen Auskunftersuchen eine Ausweiskopie oder eine **digitale Signatur**.

Da die Anwältin **schriftliche Vollmachten** samt **Ausweiskopien** vorgelegt hatte, bestanden keine berechtigten Zweifel an den Identitäten. Aufgrund des **regelmäßigen Kontakts** über Auskunftersuchen war der Glücksspielanbieterin auch bekannt, dass die Anwältin potenziell geschädigte Spieler vertritt. Angesichts der **disziplinarrechtlichen Verantwortung** von Rechtsanwältinnen gab es keinen Grund, daran zu zweifeln, dass die Spieler die Anwältin bevollmächtigt hatten, oder anzunehmen, dass die Vollmachten ge- oder verfälscht waren.

Aus der weiteren Rechtsprechung der Justiz:

- Für **elektronische Direktwerbung** nach § 174 Abs 3 TKG ist eine vorherige **Einwilligung** erforderlich, die den Anforderungen des Art 4 Z 11 DSGVO entspricht. Ein bloßes **Opt-out** (Nicht-Ankreuzen eines Widerspruchskästchens) genügt nicht. Eine **AGB-Klausel** ist auch dann unzulässig, wenn die in § 174 Abs 4 Z 2 TKG vorgesehene Beschränkung auf eigene ähnliche Produkte

oder Dienstleistungen fehlt. § 174 TKG regelt als *lex specialis* die Zusendung elektronischer Nachrichten, während vorgelagerte Verarbeitungen der DSGVO unterliegen. Eine Verarbeitung auf Basis **berechtigter Interessen** setzt eine **transparente Benennung der konkreten Rechtsgrundlage** in der Datenschutzerklärung und eine **tragfähige Interessenabwägung** voraus. Ein pauschaler Verweis auf Art 6 DSGVO genügt nicht ([OLG Wien 19.05.2025, 33R10/25w](#)).

- Einen aus einer GmbH ausgeschiedenen Geschäftsführer trifft die Pflicht, sämtliche **Geschäftsunterlagen** (Geschäftsbücher, Verträge, Korrespondenzen, E-Mails und sonstige elektronische Unterlagen) an die Gesellschaft herauszugeben. Das Recht auf Schutz von **Betriebs- und Geschäftsgeheimnissen** sowie **datenschutzrechtliche Einwände** stehen der Herausgabe nicht entgegen. Dies gilt auch für **anwaltschaftliche Korrespondenz**. Bei der **Rückgabe von Unterlagen** an die Gesellschaft handelt es sich um eine **interne Datenübermittlung**, nicht um eine Weitergabe an Dritte ([OLG Wien 26.06.2025, 2R37/25p](#)).
- Das rechtliche Interesse an der **Akteneinsicht** kann nicht schon deshalb verneint werden, weil der Dritte die Einsicht wegen einer **geplanten Rechtsverfolgung** von Ansprüchen gegen eine der Parteien erwägt. Einer Partei kann nämlich ein schutzwürdiges Interesse an der Geheimhaltung ihrer Daten nicht deshalb zuerkannt werden, damit sie sich ihren **privatrechtlichen Verpflichtungen** gegenüber dem Dritten entziehen kann. Pauschale Hinweise auf einen Eingriff in das Recht auf Datenschutz, Familien- und Privatleben aufgrund einer möglichen Einsicht in Konto- oder Geschäftsunterlagen genügen nicht zur Begründung überwiegender Interessen ([OLG Linz 10.09.2025, 4R114/25z](#)).

### **Rechtsprechung des BVwG**

#### Aus der Rechtsprechung des BVwG:

- An das **Auskunftsersuchen** dürfen keine zu hohen Voraussetzungen geknüpft werden. Zwar muss aus dem Antrag bzw der Anfrage hervorgehen, worauf der Betroffene abzielt, jedoch führen **falsche Bezeichnungen** nicht zur **Mangelhaftigkeit** des Antrags selbst. Weder die DSGVO noch andere in Betracht kommende gesetzliche Grundlagen sehen vor, dass ein Auskunftsersuchen **gewisse Formulierungen** aufweisen oder eine **konkrete Rechtsgrundlage** angeführt werden muss. Da an das Einlangen eines Auskunftsersuchens **unmittelbare Verpflichtungen**, wie die Auskunftserteilung innerhalb der gesetzlichen Frist, geknüpft sind, muss für den

Empfänger jedoch erkennbar sein, dass es sich um ein datenschutzrechtliches Auskunftsersuchen handelt ([BVwG 19.08.2025, W292 2307870-1](#)).

- Bei der Prüfung, ob eine **Bescheidbeschwerde** ausreichend begründet ist, ist kein übertriebener Formalismus geboten. Enthält die Bescheidbeschwerde nur allgemeine, floskelartige Vorbringen, ist dies jedoch unzureichend. Entspricht der Beschwerdeführer einem entsprechenden Verbesserungsauftrag nicht, ist die Bescheidbeschwerde **zurückzuweisen** ([BVwG 15.09.2025, W256 2317747-1](#)). **Anm: Soweit ersichtlich, ist mit diesem Beschluss die erste Bescheidbeschwerde gegen einen Bescheid des Parlamentarischen Datenschutzkomitees (PDK) zurückgewiesen worden. Das BVwG entschied durch einen Senat mit drei Berufsrichtern, weil gemäß § 35h DSG über Bescheidbeschwerden gegen Bescheide des PDK im Senat zu entscheiden ist, aber – anders als nach § 27 Abs 2 DSG – keine Mitwirkung von fachkundigen Laienrichtern vorgesehen ist. In solchen Fällen haben drei Berufsrichter zu entscheiden (§ 7 BVwGG).**
- Das bloße **Inbetrachtziehen**, Daten zu übermitteln, ist für die Beschwerdelegitimation nicht ausreichend. Eine **nicht erfolgte Datenverarbeitung** kann im Wege einer Datenschutzbeschwerde keiner Überprüfung zugeführt werden. Fehlt die Beschwerdelegitimation, ist die Datenschutzbeschwerde **zurückzuweisen** ([BVwG 04.09.2025, W252 2301118-1](#)).
- **Art 15 Abs 3 DSGVO** legt die praktischen Modalitäten für die Erfüllung des Auskunftsrechts in Form einer "**Kopie**" fest. Daraus ergibt sich jedoch kein generelles Recht, Kopien ganzer Dokumente zu erhalten. Um zu gewährleisten, dass die bereitgestellten Informationen leicht verständlich sind, kann sich allerdings die Reproduktion von Auszügen aus Dokumenten oder gar von ganzen Dokumenten als unerlässlich erweisen, wenn die Kontextualisierung der verarbeiteten Daten erforderlich ist, um ihre Verständlichkeit zu gewährleisten, wobei insoweit die Rechte und Freiheiten anderer zu berücksichtigen sind. Die **Beweislast**, dass die Übermittlung von Kopien im Hinblick auf die Verständlichkeit oder zur wirksamen Ausübung der ihm durch die DSGVO gewährten Rechte unerlässlich wäre, liegt beim Betroffenen selbst. Generell kann das Auskunftsrecht nur dazu herangezogen werden, um die Privatsphäre zu schützen, nicht aber, um sich Zugang zu **Verwaltungsdokumenten** zu sichern, wie dies etwa bei rechtlichen Analysen in einem **Asylbescheid** der Fall ist ([BVwG 04.09.2025, W252 2312918-1](#)).
- Einer Revision ist **aufschiebende Wirkung** zuzuerkennen, wenn für die

Revisionswerberin mit dem Vollzug des angefochtenen Erkenntnisses ein **unverhältnismäßiger Nachteil** verbunden wäre. Der Vollzug eines Strafbetrags iHv EUR 1,5 Mio vor Entscheidung durch den VwGH wäre eine **nicht unwesentliche finanzielle Belastung**, wohingegen bei einer Abweisung der Revision die Zahlung des Strafbetrags weiterhin möglich wäre. Auch steht der aufschiebenden Wirkung kein **zwingendes öffentliches Interesse** entgegen ([BVwG 10.09.2025, W258 2299744-1](#)).

### **Rechtsprechung des BFG**

- **Spenden** können gemäß § 18 Abs 8 EstG 1988 nur dann als Sonderausgaben anerkannt werden, wenn der Empfänger die **Identifikationsdaten** des Spenders (Vor- und Zuname, Geburtsdatum) dem Finanzamt übermittelt. Verweigert der Spender diese Angaben, ist eine **Datenübermittlung** an das Finanzamt durch den Empfänger nicht möglich und die Spende kann steuerlich **nicht als Sonderausgabe berücksichtigt** werden. Die Regelung des § 18 Abs 8 EstG 1988 dient dem **öffentlichen Interesse**, weil sie dem **Finanzamt** die **Erfüllung seiner gesetzlichen Aufgaben** ermöglicht und steht im Einklang mit der DSGVO ([BFG 14.10.2025, RV/7103129/2025](#)).

### **Rechtsprechung der LVwG**

Aus der Rechtsprechung der LVwG:

- Privatpersonen sind auf eine Anfrage, in der das Kennzeichen, die Motornummer oder die Fahrgestellnummer eines KFZ angegeben ist und ein **rechtliches Interesse** glaubhaft gemacht wird, der Name und die Anschrift des Zulassungsbesitzers aus der **KFZ-Zulassungsevidenz** bekanntzugeben. Unter dem Begriff "Privatpersonen" sind auch **juristische Personen** zu verstehen. Das rechtliche Interesse kann sowohl aus **subjektiv öffentlichen Rechten** als auch aus **Privatrechten** erfließen. Die **Glaubhaftmachung** des rechtlichen Interesses ist jedoch eine **Obliegenheit des Antragstellers**, für deren Erfüllung vom Antragsteller initiativ **Bescheinigungsmittel** vorzulegen sind. Das Vorbringen, wonach der Antragsteller über eine Gewerbeberechtigung als Inkassoinstitut verfügt, genügt nicht ([LVwG NÖ 09.10.2025, LVwG-AV-436/001-2025](#)).

### **Nationale Rechtsakte**

- Am **23.10.2025** ist das Strafrechtliche EU-Anpassungsgesetz 2025 (**StrEU-AG 2025**), [416/A](#), aufgrund eines formalen Fehlers bei der Beschlussfassung erneut, als **Initiativantrag**, beim Justizausschuss des

Nationalrats eingebracht worden. Mit dem StrEU-AG 2025 soll insb die VO (EU) 2019/816 zur **Einrichtung eines zentralisierten Systems** für Informationen zu **Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN)** in das innerstaatliche Recht durchgeführt werden. Geregelt werden sollen ua die Abnahme und Verarbeitung von **Fingerabdrücken** im **Strafregister** sowie die Einholung von **Strafregisterauskünften** aus anderen EU-Mitgliedstaaten und dem Vereinigten Königreich.

- Am **19.09.2025** ist der **Ministerialentwurf** zum "**Bundesgesetz über die Transparenz und das Targeting politischer Werbung; KommAustria-Gesetz, Medien-gesetz, Änderung**", [49/ME](#), beim Nationalrat eingelangt. Mit diesem Bundesgesetz soll die VO (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung (**TTPW-VO**) in das innerstaatliche Recht durchgeführt werden. Die TTPW-VO ist seit dem 10.10.2025 unmittelbar anzuwenden.

to the point

# Datenschutzmonitor. 44/2025 vom 05.11.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht, das **Digitalisierungsrecht** sowie das **IFG** schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

**Aktuell:** Unser **IFG-Musterpaket** stellen wir Ihnen auf Anfrage gerne zur Verfügung.

Abonnieren Sie auch unsere anderen periodischen Newsletter, **Digital Law Monitor**, **Technology & Digitalisation**, **Financial Regulation**, **Healthcare & Life Sciences** sowie **White Collar Crime** für regelmäßige, prägnante Updates [hier](#).

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH/EuG**

EuG 29.10.2025, T-590/23, *De Capitani* (Dokumentenzugang, Entscheidungsprozess)

EuGH 30.10.2025, C-2/23, *FL und KM Baugesellschaft* (Kronzeugenerklärung, Geheimhaltung)

- **Rechtsprechung des VfGH**

VfGH 07.10.2025, E599/2025 (BildDokG, Anlassfall, verfassungswidrige Gesetzesanwendung)

- **Rechtsprechung des VwGH**

VwGH 29.09.2025, Ra 2025/04/0089 (Tatzeitraum, Strafbemessung, Leistungsfähigkeit)

VwGH 24.09.2025, Ra 2024/04/0322 (verfahrensrechtliche Präklusivfrist)

VwGH 09.10.2025, Ra 2025/03/0087 (AuskunftspflichtG, IFG, Übergangsbestimmung, Geheimhaltungsgrund)

- **Rechtsprechung der Justiz**

OLG Wien 11.02.2025, 3R5/25i (Auskunft, Vollmacht, Erleichterungsgebot)

- **Rechtsprechung des BVwG**

BVwG 11.09.2025, W258 2241500-1 (Staatsanwaltschaft, StPO, Akteneinsicht)

BVwG 04.09.2025, W258 2232927-1 (Kohärenzverfahren, Dringlichkeitsverfahren, Wiederaufnahme)

BVwG 15.09.2025, W258 2242162-1 (Video, Treu und Glauben, Transparenz)

BVwG 02.09.2025, W256 2250819-1 (Rollenverteilung, Mitarbeiter)

BVwG 26.08.2025, W252 2307842-1 (Exzess, Missbrauchsabsicht, Feindseligkeit)

BVwG 19.08.2025, W292 2314174-1 (Recht auf Einschränkung, antragsbedürftig, Sache des Verfahrens)

- **Rechtsprechung der DSB**

DSB 04.09.2025, 2025-0.699.550 (Data Breach, Mitarbeiter, Strafbemessung)

- **EU-Rechtsakte**

DelgierteVO zur eCallVO

Zwei DurchführungsVOs zu eIDAS

## To the Point:

### Rechtsprechung des EuGH/EuG

EuG 29.10.2025, T-590/23, De Capitani

#### **Dokumentenzugang, Entscheidungsprozess**

- Ein ehemaliger Politiker beantragte beim Rat der EU Zugang zu Arbeitsdokumenten des Generalsekretariats aus laufenden Gesetzgebungsverfahren zum Migrations- und Asylpaket. Der Rat verweigerte ihm mit Beschluss den Zugang unter Verweis auf den Schutz des Entscheidungsprozesses nach Art 4 Abs 3 der VO (EG) 1049/2001. Der Rat begründete seinen Beschluss mit der Sensibilität des Bereichs, dem vorläufigen Charakter der Dokumente und der möglichen Schwächung der Verhandlungsposition. Der ehemalige Politiker erhob Nichtigkeitsklage gegen den Beschluss und die "fortdauernde explizite Entscheidung" des Rats, legislative Dokumente, zu denen Zugang gewährt wurde, nicht im **Ratsregister** zu veröffentlichen. Nach Klageerhebung wurden die Gesetzgebungsverfahren abgeschlossen und die Arbeitsdokumente als öffentlich eingestuft.

Das EuG hat erwogen: Das **Recht auf Zugang zu Dokumenten** der Organe, Einrichtungen und sonstigen Stellen der Union kann durch Verordnung eingeschränkt werden. Art 15 Abs 3 AEUV sieht zwar den **Grundsatz der Offenheit legislativer Dokumente**, nicht aber deren ausnahmslose Veröffentlichung vor. Unionsorgane können daher nach Art 4 Abs 3 der VO (EG) 1049/2001 den Zugang zu bestimmten legislativen Dokumenten verweigern, wobei die Ausnahmen eng auszulegen sind.

Die Ausnahmebestimmung des Art 4 Abs 3 der VO (EG) 1049/2001 erfordert den Nachweis, dass der Zugang den **Entscheidungsprozess** konkret und ernstlich beeinträchtigen würde, und diese Gefahr absehbar und nicht rein hypothetisch ist. Eine **ernstliche Beeinträchtigung** liegt vor, wenn sich die Verbreitung der Dokumente wesentlich auf den Entscheidungsprozess auswirkt. Die Organe müssen keine Beweise für das Vorliegen einer solchen Gefahr vorlegen. Es genügt, dass der Beschluss **objektive Gründe** darlegt, die zeigen, dass die Gefahr einer Beeinträchtigung des Entscheidungsprozesses absehbar ist.

Der **vorläufige Charakter** der Erörterungen über den Gesetzgebungsvorschlag und der Umstand, dass noch kein Konsens erzielt wurde, können für sich genommen nicht belegen, dass die Verbreitung dieser Dokumente eine ernstliche Beeinträchtigung des Entscheidungsprozesses zur Folge gehabt hätte. Auch der **technische Charakter** eines Dokuments ist kein relevantes Kriterium.

Die Rechtfertigungsgründe sind allgemein und abstrakt. Die nunmehr öffentlichen Dokumente zeigen, dass der Rat ihren Inhalt und den besonderen Kontext der Gesetzgebungsvorschläge näher hätte beschreiben können, ohne dadurch konkrete Standpunkte einzelner Mitgliedstaaten preiszugeben. Greifbare Beweise, dass der Zugang die Zusammenarbeit zwischen den Mitgliedstaaten beeinträchtigt hätte, wurden nicht vorgelegt, sodass die behauptete Gefahr **hypothetisch** erscheint.

#### Aus der Rechtsprechung des EuGH:

- Die vor der nationalen Wettbewerbsbehörde oder dem für Kartellsachen zuständigen nationalen Gericht abgegebenen **Kronzeugenerklärungen** und **Vergleichsausführungen** dürfen einer Staatsanwaltschaft (**StA**) im Rahmen eines Amtshilfemechanismus nur übermittelt werden, sofern ein solcher Mechanismus den Schutz der Kronzeugenerklärung und der Vergleichsausführungen nicht beeinträchtigt. **Beschuldigten** des Verfahrens vor der StA ist zur Ausübung ihrer Verteidigungsrechte Zugang zu diesen Dokumenten **zu gewähren**. Nichtbeschuldigten Beteiligten des strafrechtlichen Ermittlungsverfahrens, die als **Geschädigte** Schadenersatzklage erheben wollen, ist der Zugang zu Kronzeugenerklärungen und Vergleichsausführungen hingegen **zu verwehren** ([EuGH 30.10.2025, C-2/23, FL und KM Baugesellschaft](#)).

### Rechtsprechung des VfGH

#### Aus der Rechtsprechung des VfGH:

- Der VfGH hat mit Erkenntnis vom 07.10.2025, G 26/2025, ausgesprochen, dass der ehemalige § 21 Abs 5 **BildokG** verfassungswidrig war. Die Aufhebung eines Gesetzes wirkt auf den **Anlassfall** zurück. Das BVwG wandte bei Erlassung des angefochtenen Erkenntnisses diese als verfassungswidrig erkannte Gesetzesbestimmung an. Es ist daher nicht ausgeschlossen, dass diese Gesetzesanwendung für die Rechtsstellung des Beschwerdeführers nachteilig war. Der Beschwerdeführer wurde somit wegen Anwendung eines **verfassungswidrigen Gesetzes** in seinen Rechten verletzt ([VfGH 07.10.2025, E599/2025](#)). **Anm:** Die Zusammenfassung des Erkenntnisses vom 07.10.2025, G 26/2025 kann im Schönherr [Datenschutzmonitor 43/2025](#) vom 29.10.2025 nachgelesen werden.

### Rechtsprechung des VwGH

#### Aus der Rechtsprechung des VwGH:

- Die **Ausdehnung des Tatzeitraums** durch das Verwaltungsgericht ist keine (grundsätzlich zulässige) Präzisierung der rechtlichen Grundlage der Bestrafung. Sie ist eine **unzulässige Erweiterung des Tatvorwurfs**. Die **Bestimmung des Höchstbetrags** ist von der Bemessung der Geldstrafe zu unterscheiden. Die **Strafbemessung** ist eine **Ermessensentscheidung**, die unter Bedachtnahme auf die in Art 83 Abs 1 DSGVO genannten Voraussetzungen (wirksam, verhältnismäßig und abschreckend) vorzunehmen ist. Dabei sind auch die in Art 83 Abs 2 DSGVO sowie in § 19 VStG festgelegten Kriterien und bei zu bestrafenden Unternehmen iSd Art 101 und 102 AEUV deren Größe zu berücksichtigen. Da sich die Wortfolge "seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres" eines Unternehmens iSd Art 101 und 102 AEUV in Art 83 Abs 4 bis 6 DSGVO nur auf die **Bestimmung des dynamischen Strafrahmens** bezieht, ist bei der **Strafzumessung** auf die **tatsächliche** oder **materielle Leistungsfähigkeit** des Unternehmens abzustellen ([VwGH 29.09.2025, Ra 2025/04/0089](#)).
- Gemäß Art 130 Abs 2a B-VG erkennen die Verwaltungsgerichte (VwG) selbst über Beschwerden von Personen, die sich durch das jeweilige VwG in ihren Datenschutzrechten als verletzt erachteten. Für Beschwerden an das LVwG Tirol ist eine subjektive einjährige Beschwerdefrist vorgesehen (§ 12a Abs 3 TLVwGG). Diese Beschwerdefrist ist eine **verfahrensrechtliche Präklusivfrist**, weshalb das Postlaufprivileg nach § 33 Abs 3 AVG anzuwenden ist. Maßgeblich sind die gesetzssystematische Einordnung, die Orientierung an § 24 Abs 4 DSG sowie die Materialien, aus denen hervorgeht, dass es sich um eine verfahrensrechtliche Präklusivfrist handelt. Eine am letzten Tag der Frist zur Post gegebene Beschwerde ist daher fristwährend ([VwGH 24.09.2025, Ra 2024/04/0322](#)). **Anm: Aus diesem Erkenntnis des VwGH geht implizit hervor, dass auch die Präklusivfristen nach dem DSG verfahrensrechtliche Fristen sind.**
- Informationen über den **Wissens- bzw Ausbildungsstand** einer Person sind personenbezogene Daten iSd § 1 Abs 1 DSG. Stellt ein Betroffener ein Auskunftsbegehren an das Gericht, in dem er um Mitteilung ersucht, ob bestimmte Richter eine Schulung abgeschlossen haben, muss eine Interessenabwägung durchgeführt werden. Der Geheimhaltungsanspruch gilt nur bei einem schutzwürdigen Interesse der betroffenen Richter; überwiegende berechnigte Interessen eines anderen lassen die Geheimhaltung zurücktreten. Da das VwG keine ausreichende konkrete inhaltliche Feststellung zum schutzwürdigen Interesse getroffen

hat, war das Erkenntnis aufzuheben. Aufgrund der **ex-tunc-Wirkung** des aufhebenden Erkenntnisses durch den VwGH ist von einem am 01.09.2025 anhängigen Verfahren auszugehen. Mit Blick auf die Übergangsbestimmung des Art 151 Abs 68 letzter Satz B-VG ist nicht das Informationsfreiheitsgesetz, sondern das **Auskunfts-pflichtgesetz** anzuwenden ([VwGH 09.10.2025, Ra 2025/03/0087](#)).

## **Rechtsprechung der Justiz**

### Aus der Rechtsprechung der Justiz:

- Beauftragt eine Betroffene einen Rechtsanwalt mit der Durchsetzung ihres **Auskunftsrechts**, muss ein Verantwortlicher des privaten Bereichs die **Identität der Betroffenen** und die **Vollmacht** prüfen. Weitere Informationen zur Bestätigung der Identität dürfen nicht generell, sondern nur bei begründeten Zweifeln an der Identität verlangt werden. Eine **Ausweiskopie** ist ein geeigneter Identitätsnachweis. Der **Bevollmächtigungsvertrag** ist an keine speziellen Formerfordernisse geknüpft. Teilt der Verantwortliche lediglich mit, keine elektronischen Vollmachten zu akzeptieren, ohne Zweifel an der Echtheit der Unterschrift zu äußern, ist für die Betroffene nicht ersichtlich, ob berechtigterweise weitere Nachweise zur Erfüllung des Auskunftsersuchens verlangt werden. Da der Verantwortliche die allenfalls bestehenden Zweifel iSd Art 12 Abs 6 DSGVO nicht einzelfallbezogen dargelegt hat, wurde die Klageerhebung durch den Verantwortlichen veranlasst ([OLG Wien 11.02.2025, 3R5/25j](#)).

## **Rechtsprechung des BVwG**

[BVwG 11.09.2025, W258 2241500-1](#)

### **Staatsanwaltschaft, StPO, Akteneinsicht**

- In einem einheitlich geführten Ermittlungsverfahren wurde gegen die Erstbeschuldigte wegen versuchten Raubs zum Nachteil des Zweitbeschuldigten und wegen schwerer Körperverletzung zum Nachteil eines Dritten ermittelt. Gegen den Zweitbeschuldigten wurde wegen Körperverletzung zum Nachteil der Erstbeschuldigten ermittelt. Zur Feststellung der Verletzungsfolgen des Dritten ließ die Staatsanwaltschaft (**StA**) ein medizinisches Gutachten erstellen. Bei der Akteneinsicht legte die StA dem Zweitbeschuldigten dieses Gutachten offen. Durch die Offenlegung des Gutachtens sah sich die Erstbeschuldigte in ihrem Recht auf Geheimhaltung verletzt und erhob erfolgreich Datenschutzbeschwerde bei der DSB. Dagegen erhob die StA erfolgreiche Beschwerde an das BVwG, welches den Spruch der DSB in eine Abweisung abänderte.

Das BVwG hat erwogen: Die Verarbeitung personenbezogener Daten im Rahmen strafprozessualer Ermittlungsverfahren fällt in den Anwendungsbereich der **DSRL-PJ**. Gerichte sind nach § 31 Abs 1 zweiter Satz DSG im Rahmen ihrer justiziellen Tätigkeit von der **Aufsichtszuständigkeit** der DSB ausgenommen. Staatsanwaltschaften sind aber **keine unabhängigen Justizbehörden** und unterliegen der Aufsichtszuständigkeit der DSB.

Die Einschränkung des Rechts auf Geheimhaltung personenbezogener Daten kann zur Wahrung **überwiegenden berechtigter Interessen** zulässig sein. Im Fall von Eingriffen durch staatliche Behörden darf dies nur durch **Gesetz** erfolgen. Eingriffstatbestände in das Grundrecht auf Datenschutz sind für die Aufklärung und Verfolgung von Straftaten in einem strafrechtlichen Ermittlungsverfahren durch die StA im dritten Hauptstück des DSG geregelt. Die Regelungen über die Akteneinsicht aus der StPO gehen dem dritten Hauptstück des DSG als *lex specialis* vor.

Ein Beschuldigter kann gemäß § 51 Abs 1 erster Satz StPO Einsicht in die vorliegenden Ergebnisse des Ermittlungs- und des Hauptverfahrens nehmen. Dieses nach Art 6 EMRK verfassungsrechtlich geschützte Recht kann nur in den in § 51 Abs 2 StPO genannten Ausnahmefällen beschränkt werden. Die StPO sieht vor, die **Akteneinsicht** betreffend Opfer, Privatbeteiligte oder Privatankläger zur Wahrung ihrer Interessen **zu beschränken**. Im Verhältnis zu einem **Mitbeschuldigten** sieht die StPO **keine** derartige Interessenabwägung vor.

Da das Gutachten zumindest **abstrakt** zur Feststellung der Glaubwürdigkeit, zur Feststellung des Tathergangs und zur Verteidigung des Zweitbeschuldigten beizutragen geeignet war, war die **Akteneinsicht zu gewähren**.

BVwG 04.09.2025, W258 2232927-1

### **Kohärenzverfahren, Dringlichkeitsverfahren, Wiederaufnahme**

- Eine Nutzerin sah sich durch die Verarbeitung ihrer personenbezogenen Daten durch ein in Irland ansässiges soziales Netzwerk in ihrem Recht auf Geheimhaltung verletzt. Die der Nutzung des Netzwerks vorgelagerten Datenschutzrichtlinien und Nutzungsbedingungen enthielten ihrer Ansicht nach unzulässige Einwilligungen zur Datenverwendung. Im Jahr 2018 brachte die Nutzerin eine Datenschutzbeschwerde bei der DSB ein. Die DSB setzte das Verfahren mit Bescheid bis zur Entscheidung der federführenden Aufsichtsbehörde bzw des Europäischen Datenschutzausschusses aus. Sie begründete dies damit, dass eine grenzüberschreitende Verarbeitung vorliege und die

irische Datenschutzbehörde (**Data Protection Commission, DPC**) als **federführende Aufsichtsbehörde** zuständig sei. Im Jahr 2020 beantragte die Nutzerin die **Wiederaufnahme** des ausgesetzten Verfahrens. Sie führte aus, die DPC habe in ihrem **Ermittlungsbericht** (*inquiry report*) erklärt, bestimmte Teile ihrer Datenschutzbeschwerde nicht zu behandeln. Daher müsse die DSB das Verfahren in diesen Punkten fortführen und selbst eine Entscheidung erlassen. *In eventu* beantragte sie, die DSB solle die DPC um Amtshilfe ersuchen oder ein Dringlichkeitsverfahren einleiten.

Die DSB wies die Anträge der Nutzerin auf Wiederaufnahme des ausgesetzten Verfahrens und Fällung einer meritorischen Entscheidung zurück. Den Eventualantrag auf Amtshilfeersuchen gemäß Art 61 Abs 1 DSGVO wies die DSB ab. Dagegen erhob die Nutzerin (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Ein **Antrag auf Wiederaufnahme** setzt gemäß § 69 AVG voraus, dass das wiederaufzunehmende Verfahren "durch Bescheid abgeschlossen" worden ist. Der Nutzerin steht kein Recht zu, die Fortführung eines ohnehin fortzuführenden Verfahrens zu beantragen.

Für grenzüberschreitende Verarbeitungen sieht **Art 56 DSGVO** grundsätzlich die Zuständigkeit der "federführenden Aufsichtsbehörde" vor. Dies ist die Aufsichtsbehörde der **Hauptniederlassung** des Verantwortlichen. **Ausgenommen** von diesem Grundsatz sind "**lokale Fälle**", bei denen die nicht federführende Aufsichtsbehörde zuständig ist, wenn die Datenschutzbeschwerde nur eine Niederlassung oder Betroffene ihres Mitgliedstaats betrifft und die federführende Behörde den Fall nicht an sich zieht. Ausgenommen sind auch Fälle, in denen eine Aufsichtsbehörde im **Dringlichkeitsverfahren** nach Art 66 DSGVO bei außergewöhnlichen Umständen sofort einstweilige Maßnahmen treffen kann, wenn dringender Handlungsbedarf zum Schutz der Rechte und Freiheiten Betroffener besteht.

Es liegt eine **grenzüberschreitende Verarbeitung** vor, für die die irische Aufsichtsbehörde als Aufsichtsbehörde der in Irland gelegenen Hauptniederlassung des Verantwortlichen die zuständige federführende Aufsichtsbehörde ist. Die Ausnahme des Art 56 Abs 2 bis 5 DSGVO gelangt nicht zur Anwendung, weil weder nur Personen in Österreich betroffen sind noch die Verarbeitung nur mit einer Niederlassung in Österreich in Zusammenhang steht. Die Ausnahme des Art 66 Abs 1 DSGVO kommt nicht zur Anwendung, weil die DSB **kein Dringlichkeitsverfahren** eingeleitet hat. Die DSB war daher nicht dafür zuständig,



eine **meritorische Entscheidung** zu treffen.

Für einen selbständigen Abspruch über die allfällige Ablehnung eines Teils einer Datenschutzbeschwerde durch die federführende Aufsichtsbehörde gibt es keine rechtliche Grundlage. Die DSB darf gemäß Art 60 DSGVO erst dann einen Bescheid erlassen, wenn ein für sie **verbindlicher Beschlussentwurf iSd Art 60 DSGVO** vorliegt. Ein Ermittlungsbericht (*inquiry report*), der nur als Grundlage für einen Beschlussentwurf durch die federführende Aufsichtsbehörde dienen soll, kann die DSB weder binden noch sie zur Erlassung eines Bescheids verpflichten.

Gemäß **Art 61 Abs 1 DSGVO** übermitteln die Aufsichtsbehörden einander maßgebliche Informationen und gewähren einander Amtshilfe und treffen Vorkehrungen für eine wirksame Zusammenarbeit. Die DSGVO und die nationale Rechtsordnung räumen Betroffenen **kein subjektives öffentliches Recht** darauf ein, dass die DSB andere Behörden um **Amtshilfe** ersucht oder auf eine bestimmte Art mit der federführenden Aufsichtsbehörde zusammenarbeitet. Die **Ausgestaltung dieser Zusammenarbeit** liegt im **Ermessen der DSB**.

[BVwG 15.09.2025, W258 2242162-1](#)

#### **Video, Treu und Glauben, Transparenz**

- Eine Betroffene erachtete sich in ihrem Recht auf Geheimhaltung dadurch verletzt, dass ihr Nachbar eine **Wildkamera** installiert habe, um die damit angefertigten Aufnahmen ihrem ehemaligen Lebensgefährten zuzusenden. Sie erhob Datenschutzbeschwerde an die DSB. Diese gab der Datenschutzbeschwerde statt. Die hiergegen vom Nachbarn an das BVwG erhobene Bescheidbeschwerde blieb erfolglos.

Das BVwG hat erwogen: Der Nachbar hat von der Betroffenen **Lichtbilder** erstellt, indem er, ohne ihre Zustimmung, einen der Betroffenen zugeordneten Garagenplatz betreten und dort eine Kamera versteckt hat. Im Anschluss hat er die Lichtbilder an einen Dritten weitergegeben.

Weder die Erhebung noch die Weitergabe der Daten entsprachen dem, womit die Betroffene im Lichte der gesamten Rechtsordnung rechnen musste. Die Erhebung und Weitergabe der Daten verstieß daher gegen den Grundsatz der Verarbeitung nach "**Treu und Glauben**" nach Art 5 Abs 1 zweiter Fall DSGVO.

Aufgrund der verdeckten Aufnahme von Bilddaten war der Betroffenen auch nicht bewusst, dass und in welchem Umfang sie betreffende personenbezogene Daten verarbeitet werden. Die Datenerhebung und Datenweitergabe verstieß daher auch

gegen den **Transparenzgrundsatz**. Im Ergebnis waren die Erstellung und Weitergabe der Lichtbilder rechtswidrig.

Aus der weiteren Rechtsprechung des BVwG:

- Bei der **Zuweisung der Verantwortung** ist bevorzugt das jeweilige Unternehmen oder die Stelle als **Verantwortliche** zu betrachten und nicht die bestimmte (für die Organisation handelnde) **Person innerhalb des Unternehmens** oder der Stelle. Das Unternehmen oder die Stelle trägt letztlich die Verantwortung für die Datenverarbeitung. Sofern natürliche Personen jedoch Daten für ihre eigenen Zwecke außerhalb des Tätigkeitsbereichs ihrer Organisation verarbeiten, können sie selbst Verantwortliche werden. Die Frage der Verantwortlichenstellung ist unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalles zu beurteilen. Um zu klären, ob eine Person als Verantwortliche (bzw. allenfalls als gemeinsam Verantwortliche gemäß Art 26 Abs 1 DSGVO) angesehen werden kann, ist zu prüfen, ob sie unter Berücksichtigung der besonderen Umstände des Falles aus **Eigeninteresse** auf die betreffende Verarbeitung personenbezogener Daten Einfluss genommen hat. Dabei ist auch zu beurteilen, ob sie allenfalls gemeinsam mit anderen die **Zwecke** und die **Mittel** zur fraglichen Verarbeitung festgelegt hat. Es kommt daher darauf an, welche natürliche oder juristische Person jeweils die Entscheidung sowohl über den Zweck – das "**warum**" – als auch über die Mittel – "**auf welche Weise**" – in Bezug auf die konkrete Handlung getroffen hat ([BVwG 02.09.2025, W256 2250819-1](#)).
- Bei **offenkundig unbegründeten oder exzessiven** Datenschutzbeschwerden darf die DSB eine **Gebühr** verlangen oder sich **weigern**, tätig zu werden (Art 57 Abs 4 DSGVO). Die Aufsichtsbehörde trägt die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Datenschutzbeschwerde. Der EuGH legt Art 57 Abs 4 DSGVO dahingehend aus, dass Anfragen nicht allein aufgrund ihrer Anzahl als exzessiv eingestuft werden können. Die DSB muss unter Berücksichtigung der einzelfallbezogenen Umstände das Vorliegen einer **Missbrauchsabsicht** der anfragenden Person nachweisen. Eine Missbrauchsabsicht liegt vor, wenn Datenschutzbeschwerden eingereicht werden, ohne dass dies objektiv erforderlich ist, um die Rechte aus der DSGVO zu schützen. Da der Betroffene die Datenschutzbeschwerde als Vergeltungsmaßnahme nutzte, um seine **Feindseligkeit** gegenüber Personen und Behörden auszuleben, durfte die DSB die Behandlung der Datenschutzbeschwerden wegen rechtsmissbräuchlicher und

exzessiver Ausübung des Beschwerderechts iSd Art 57 Abs 4 DSGVO ablehnen ([BVwG 26.08.2025, W252 2307842-1](#)).

- Die Betroffenenrechte gemäß Art 15 bis Art 22 DSGVO sind **antragsbedürftige Rechte**. Die Geltendmachung setzt zunächst einen **entsprechenden Antrag** an den Verantwortlichen voraus. Da der Betroffene keinen Antrag auf **Einschränkung der Verarbeitung** seiner personenbezogenen Daten an den Verantwortlichen gestellt hatte, konnte er nicht in seinem Recht iSd Art 18 DSGVO verletzt werden. Das BVwG ist in seiner Entscheidung auf die **Sache** des angefochtenen Bescheids beschränkt, weshalb eine Prüfung darüberhinausgehender datenschutzrechtlicher Rechtsverletzungen nicht zulässig war ([BVwG 19.08.2025, W292 2314174-1](#)).

### **Rechtsprechung der DSB**

DSB 04.09.2025, 2025-0.699.550

#### **Data Breach, Mitarbeiter, Strafbemessung**

- Eine Werbeagentur betrieb als Verantwortliche neben ihrer Hauptdomain eine ungesicherte Subdomain-Website als Development-Server, über die unbefugte Dritte auf Kundendaten (ua Name, E-Mail, Geburtsdatum, Telefonnummer) zugreifen konnten. Ein erster Hinweis im Januar 2025 wurde von einer Mitarbeiterin als Spam eingestuft und nicht eskaliert, worauf am 16.02.2025 ein weiterer Hinweis eines IT-Vereins erfolgte, der in Kopie an die DSB gesendet wurde. Die Agentur schloss noch am selben Tag die Sicherheitslücke und dokumentierte den Vorfall intern, erstattete aber keine Meldung an die DSB. Die DSB leitete daraufhin ein amtswegiges Prüfverfahren ein, und verhängte mittels **Straferkenntnis** eine Geldbuße iHv EUR 870 (zzgl Verfahrenskosten) wegen Verstoßes gegen Art 33 Abs 1 DSGVO.

Die DSB hat erwogen: Art 33 DSGVO verpflichtet im Falle eines Datensicherheitsvorfalls (**Data Breach**) zur unverzüglichen Meldung binnen 72 Stunden an die zuständige Aufsichtsbehörde. Eine Ausnahme davon liegt nur vor, wenn kein Risiko für Rechte und Freiheiten natürlicher Personen besteht. Die Drittanzeige eines Hinweisgebers ersetzt nicht die **Verantwortlichenmeldung**. Nur die Meldung der Verantwortlichen einschließlich der Darstellung der Abhilfemaßnahmen ermöglicht der Aufsichtsbehörde eine ordnungsgemäße Aufgabewahrnehmung.

Das Fehlverhalten der **Mitarbeiterin** wird der Agentur **zugerechnet**. Ab dem Zeitpunkt der ersten Verständigung hatte die Agentur "Kenntnis" von dem Vorfall iSd Art 33 Abs 1 DSGVO. Die Agentur hat fahrlässig gehandelt, weil der Ersthinweis

ignoriert wurde und weiters irrtümlich angenommen wurde, dass eine in Kopie an die DSB gesandte Drittmail für eine Meldung iSd Art 33 DSGVO genügt. Die Bußgeldbemessung war anhand der **Unternehmensgröße** nach den EDSA-Leitlinien durchzuführen. Mildernde Umstände waren zu berücksichtigen (Unbescholtenheit, Mitwirkung, nachträgliche Kooperation). Die Geldbuße iHv EUR 870 Euro erweist sich als tat- und schuldangemessen, wirksam, verhältnismäßig und abschreckend.

### **EU-Rechtsakte**

- Am **28.10.2025** wurde die "*Delegierte Verordnung (EU) 2025/1871 der Kommission vom 23. Juli 2025 zur Änderung der Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates hinsichtlich der Normen für eCalls und zur Änderung der Delegierten Verordnung (EU) 2017/79 hinsichtlich der technischen Anforderungen und Prüfverfahren für die Genehmigung von Kraftfahrzeugen, die mit auf dem **112-Notruf** basierenden bordeigenen **eCall-Systemen** ausgerüstet sind*", [ABI L 2025/1871](#), kundgemacht. Mit dieser DelegiertenVO werden **Prüfverfahren** betreffend **eCall-Systeme** iSd [eCallVO \(EU\) 2015/758](#) für neue **Fahrzeugtypen** festgelegt.
- Am **28.10.2025** wurden die (i) "*Durchführungsverordnung (EU) 2025/2160 der Kommission vom 27. Oktober 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf **Referenzstandards, Spezifikationen und Verfahren** für das Management der Risiken bei der Erbringung nichtqualifizierter Vertrauensdienste*", [ABI L 2025/2160](#); und (ii) "*Durchführungsverordnung (EU) 2025/2162 der Kommission vom 27. Oktober 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die **Akkreditierung von Konformitätsbewertungsstellen**, die qualifizierte Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste bewerten, den Konformitätsbewertungsbericht und das Konformitätsbewertungssystem*", [ABI L 2025/2162](#), kundgemacht. Mit diesen **zwei DurchführungsVOs** werden **Referenzstandards** und **Spezifikationen** sowie die **Akkreditierung von Konformitätsbewertungsstellen** unter der [eIDAS-VO](#) festgelegt.

to the point

# Datenschutzmonitor. 45/2025 vom 12.11.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht, das **Digitalisierungsrecht** sowie das **IFG** schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

**Aktuell:** Unser **IFG-Musterpaket** stellen wir Ihnen auf Anfrage gerne zur Verfügung.

Abonnieren Sie auch unsere anderen periodischen Newsletter, **Digital Law Monitor**, **Technology & Digitalisation**, **Financial Regulation**, **Healthcare & Life Sciences** sowie **White Collar Crime** für regelmäßige, prägnante Updates [hier](#).

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 06.11.2025, 46704/16, *Guyvan/Ukraine* (Personenbezogene Daten, Kommunikationsüberwachung, Arbeitsplatz)

EGMR 06.11.2025, 37639/19, *AV/Schweiz* (Haft, Korrespondenz)

- **Rechtsprechung des EuGH**

## NACHTRAG

EuGH 29.10.2025, C-206/25 P, *Kommission/Bindl* (Streithilfe, Meta Ireland)

- **Rechtsprechung des VwGH**

VwGH 29.09.2025, Ro 2023/04/0045 (Einwilligung, Prüfumfang, Kognitionsbefugnis)

VwGH 29.09.2025, Ra 2023/04/0246 (Videoüberwachung, Rechtsfrage grundsätzlicher Bedeutung)

VwGH 08.10.2025, Ra 2023/04/0117 (Erlaubnistatbestand, Informationspflicht, Geheimhaltung)

- **Rechtsprechung der Justiz**

OGH 16.10.2025, 6Ob230/24b (Geschäftsunterlagen, Offenlegungspflicht, Rechtsgrundlage)

OLG Wien 10.06.2025, 15R74/25z (Shitstorm, immaterieller Schadenersatz)

OLG Wien, 27.08.2025, 15R35/25i (Persönlichkeitsrecht, Interessenabwägung)

- **Rechtsprechung des BVwG**

BVwG 28.08.2025, W137 2311069-1 (Schengegener Informationssystem, Asylantrag, Löschergehen)

BVwG 26.09.2025, W256 2284167-1 (Massenverfahren, Aussetzung)

- **Rechtsprechung der DSB**

DSB 05.09.2025, 2025-0.712.691 (Auskunft, Marktortprinzip)

- **EU-Rechtsakte**

Gigabit Infrastructure Act (GIA)

Berichtigung des DSA

- **Nationale Rechtsakte**

Strafrechtliches EU-Anpassungsgesetz 2025

Novelle des Gesundheitstelematikgesetzes

## To the Point:

### Rechtsprechung des EGMR

EGMR 06.11.2025, 46704/16, *Guyvan/Ukraine*

#### **Personenbezogene Daten, Kommunikationsüberwachung, Arbeitsplatz**

Ein ukrainischer Arbeitnehmer nutzte sein Mobiltelefon sowohl beruflich als auch privat, wobei der Arbeitgeber die Kosten für die berufliche Nutzung, insb für Auslandsroaming während Dienstreisen, übernahm. Nachdem auf den Rechnungen internationale Roaminggebühren auftauchten, obwohl sich der Arbeitnehmer nach eigenen Angaben am Arbeitsplatz befunden hatte, leitete der Arbeitgeber **interne Ermittlungen** ein und forderte vom Mobilfunkanbieter detaillierte **Verbindungsdaten** an. Da der Arbeitgeber ihm keine Auskunft über die vom Mobilfunkanbieter erhaltenen Informationen erteilte, erhob der Arbeitnehmer Klage. Die Klage wurde abgewiesen, weil der Arbeitgeber als Inhaber der Telefonnummer berechtigt sei, diese Informationen einzuholen. Auch die höheren Instanzen bestätigten diese Auffassung und sahen in den angeforderten Informationen keine personenbezogenen Daten des Arbeitnehmers. Daraufhin wandte sich der Arbeitnehmer wegen der Verletzung seines Rechts auf Achtung des Privatlebens gemäß Art 8 EMRK (erfolgreich) an den EGMR.

Der EGMR hat erwogen: Das "Privatleben" umfasst auch Interaktionen im **beruflichen Umfeld** sowie über den **Aufenthaltsort** einer Person zu einem bestimmten Zeitpunkt. Informationen über (i) Roamingdienste, (ii) den Standort und (iii) die Mitteilungsempfänger sind personenbezogene Daten des Arbeitnehmers.

Zwar handelte es sich bei der Überwachung der Kommunikation um keinen staatlichen Eingriff, sondern einen Eingriff durch einen privaten Arbeitgeber. Art 8 EMRK verpflichtet den Staat jedoch, den Schutz des Privatlebens auch im Verhältnis zwischen Privaten zu gewährleisten ("**obligation to protect**"). IZm der Überwachung der **Kommunikation am Arbeitsplatz** sind bestimmte Kriterien wie die Unterrichtung des Arbeitnehmers, Umfang und Intensität der Überwachung, berechtigte Gründe des Arbeitgebers, weniger eingriffsintensive Alternativen, Folgen für den Arbeitnehmer sowie angemessene Garantien gegen Willkür zu berücksichtigen.

Zwar war der **Arbeitgeber** berechtigt, Informationen zur Kostenübernahme einzuholen, jedoch verfolgten seine Anträge auch den Zweck, den Aufenthaltsort des Arbeitnehmers zu bestimmten Zeiten zu ermitteln. Die erhobenen Daten – etwa Telefonnummern und Länder – waren dafür **nicht erforderlich** und griffen in die Privatsphäre des Arbeitnehmers ein. Da die nationalen Gerichte nicht prüften, ob die Datenerhebung gerechtfertigt war, wurde dem Arbeitnehmer der staatliche Schutz durch ein Gericht verweigert. **Anm: Der EGMR schließt an seine**

Rechtsprechung in der Rs *Bărbulescu* an. Dieses Urteil sollte insb von Arbeit- und Dienstgebern beachtet werden.

Aus der weiteren Rechtsprechung des EGMR:

- Die **Überwachung** der nicht geschützten Korrespondenz eines **Häftlings** durch eine **Justizanstalt** ist zulässig, wenn sie in Einklang mit den einschlägigen Gesetzen erfolgt und weder unzumutbar noch willkürlich ist ([EGMR 06.11.2025, 37639/19, AV/Schweiz](#)).

### Rechtsprechung des EuGH

Aus der Rechtsprechung des EuGH:

#### **NACHTRAG**

- Mit [Urteil vom 08.01.2025, T-354/22, Bindl/Kommission](#), hat das **EuG** der Klage eines Betroffenen teilweise stattgegeben und ua eine rechtswidrige Datenübermittlung aufgrund der Heranziehung von Meta Platforms Ireland (**Meta Ireland**) durch die Europäische Kommission (**Kommission**) festgestellt sowie einen Schadenersatz wegen eines immateriellen Schadens zugesprochen. Nachdem der Betroffene und die Kommission jeweils Rechtsmittel an den EuGH erhoben hatten, beantragte Meta Ireland, als **Streithelferin** zugelassen zu werden. Meta Ireland wird als Streithelferin **zugelassen**, weil der Ausgang des Rechtsmittels geeignet ist, ihre Rechtsstellung zu ändern und Meta Ireland daher ein **berechtigtes Interesse** daran hat, dass dem Rechtsmittel der Kommission stattgegeben wird ([EuGH 29.10.2025, C-206/25 P, Kommission/Bindl](#)).

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Ob der klaren rechtlichen Anordnung des Art 7 DSGVO zu den Bedingungen für eine **Einwilligung** im Einzelfall entsprochen wird, ist anhand der konkreten Umstände zu prüfen. Eine im Einzelfall vorgenommene rechtliche Beurteilung kann nur dann die Zulässigkeit einer Revision begründen, wenn dies wegen einer krassen Fehlbeurteilung der einzelfallbezogenen Umstände durch das Verwaltungsgericht aus Gründen der Rechtssicherheit geboten ist. Die Sache des Bescheides begrenzt den Prüfungsumfang und damit die Kognitionsbefugnis des BVwG ([VwGH 29.09.2025, Ro 2023/04/0045](#)).
- Das bloße Vorbringen, es fehle an Judikatur des VwGH zu **Videoüberwachungen** iZm der DSGVO und dem DSG, ohne eine konkrete Rechtsfrage zu relevieren, begründet keine Rechtsfrage grundsätzlicher

Bedeutung ([VwGH 29.09.2025, Ra 2023/04/0246](#)).

- Eine Verarbeitung muss unter einen der in **Art 6 Abs 1 DSGVO** vorgesehenen Fälle subsumierbar sein, um als rechtmäßig angesehen werden zu können. Demgegenüber führt nicht jede Verletzung der **Informationspflicht** *per se* zur Unrechtmäßigkeit einer Datenverarbeitung und damit zu einer Verletzung im Recht auf Geheimhaltung ([VwGH 08.10.2025, Ra 2023/04/0117](#)).

#### **Aus der Rechtsprechung der Justiz:**

- Soweit sich ein Revisionsrekurs gegen die Veröffentlichung von Namen und Geburtsdaten der Gesellschafter einer GmbH im **Firmenbuch** richtet, besteht kein Zusammenhang zu den Offenlegungspflichten der §§ 277 ff UGB. Die Rechtmäßigkeit der Offenlegung personenbezogener Daten natürlicher Personen in einem **öffentlich zugänglichen Handelsregister** ist von den nationalen Gerichten anhand der Rechtfertigungsgründe des Art 6 Abs 1 lit c und/oder lit e DSGVO zu beurteilen ([OGH 16.10.2025, 6Ob230/24b](#)).
- Ein **Online-"Shitstorm"** stellt schadenersatzrechtlich einen einheitlichen immateriellen Gesamtschaden dar. Wurde dieser Gesamtschaden bereits ausgeglichen (insb durch geleistete Zahlungen), besteht **kein erneuter Schadenersatzanspruch** aufgrund von **Art 82 DSGVO** oder anderen gesetzlichen Bestimmungen ([OLG Wien 10.06.2025, 15R74/25z](#)).
- Die Veröffentlichung eines **Bildnisses** in Verbindung mit einem Begleittext, der einen Prominenten als fremdbestimmt, leicht manipulierbar und geschäftsunfähig erscheinen lässt, verletzt berechnete Interessen iSd **§ 78 UrhG**. Bei Berührung des höchstpersönlichen Lebensbereichs überwiegt das **Persönlichkeitsschutzinteresse** und begründet einen Unterlassungsanspruch sowie Anspruch auf **immateriellen Schadenersatz** ([OLG Wien, 27.8.2025, 15R35/25i](#)).

#### **Rechtsprechung des BVwG**

[BVwG 28.08.2025, W137 2311069-1](#)

#### **Schengener Informationssystem, Asylantrag, Löschebegehren**

- Ein Inder begehrte die Löschung seiner im Schengener Informationssystem (**SIS**) gespeicherten Ausschreibung, die auf einer rechtskräftigen Rückkehrentscheidung beruhte. Die DSB wies die auf Löschung gerichtete Datenschutzbeschwerde ab. Gegen diesen Bescheid erhob der Inder (erfolglos) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die Verarbeitung personenbezogener Daten im SIS basiert auf Art 6 Abs 1 lit c und lit e DSGVO sowie der VO (EU) 2018/1860 (**SIS Rückkehr VO**). Gemäß Art 3 SIS Rückkehr VO ist die Eingabe einer Ausschreibung zur Unterstützung der Vollstreckung von Rückkehrentscheidungen verpflichtend. Ein Löschananspruch nach Art 17 DSGVO besteht nicht, weil Art 17 Abs 3 lit b DSGVO die Löschung ausschließt, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich ist.

Die SIS Rückkehr VO regelt **Löschungstatbestände** abschließend. Nach Art 14 SIS Rückkehr VO sind Daten nur dann zu löschen, wenn die zugrunde liegende Entscheidung zurückgenommen oder für nichtig erklärt wurde oder der Betroffene die Ausreise aus der EU nachweist. Auch eine Unterrichtung durch einen anderen Mitgliedstaat über die beabsichtigte bzw erfolgte Erteilung eines Aufenthaltstitels iSd Art 9 Abs 2 SIS Rückkehr VO ist nicht erfolgt.

Die Datenverarbeitung (einschließlich **besonderer Kategorien von Daten**) ist im Lichte von Art 9 Abs 2 lit g DSGVO durch ein **erhebliches öffentliches Interesse** an der Durchsetzung rechtskräftiger Entscheidungen und einem **geordneten Fremdenwesen** gerechtfertigt. Die Schutzmechanismen der SIS Regelungen gewährleisten die Wahrung des Grundrechts auf Datenschutz.

#### Aus der weiteren Rechtsprechung des BVwG:

- Ein Verfahren kann ausgesetzt werden, wenn bei einem Verwaltungsgericht in einer erheblichen Zahl von anhängigen oder zu erwartenden Verfahren eine Rechtsfrage zu lösen ist, die in einem – gleichzeitig anhängigen – Verfahren vor dem VwGH zu lösen ist. Beim BVwG sind zum selben Themenkomplex etwa 100 Bescheidbeschwerden anhängig. Damit liegt eine **erhebliche Anzahl an Verfahren** vor. Das gegenständliche Verfahren ist eines dieser Verfahren und daher **auszusetzen** ([BVwG 26.09.2025, W256 2284167-1](#)).

#### **Rechtsprechung der DSB**

[DSB 05.09.2025, 2025-0.712.691](#)

#### **Auskunft, Marktortprinzip**

- Ein Rechtsanwalt richtete im Auftrag eines Spielers ein Auskunftersuchen an ein in Curaçao ansässiges **Online-Glücksspielunternehmen**. Da dieses nur Anfragen des Spielers selbst akzeptierte, stellte der Spieler ein entsprechendes Auskunftersuchen. Dennoch blieb das Auskunftersuchen unbeantwortet, sodass der Rechtsanwalt

Datenschutzbeschwerde bei der DSB einbrachte. Trotz entsprechender Aufforderung erstattete das Glücksspielunternehmen kein Vorbringen und wirkte im Beschwerdeverfahren auch in sonstiger Weise nicht mit. Die DSB gab der Datenschutzbeschwerde statt, stellte eine Verletzung im Recht auf Auskunft fest und trug dem Glücksspielunternehmen auf, binnen vier Wochen eine Auskunft zu erteilen.

Die DSB hat erwogen: Die DSGVO findet auf **Curaçao** als niederländisches Überseegebiet nicht ohne Weiteres Anwendung, weil es über eine eigene datenschutzrechtliche Gesetzgebung verfügt und daher als **Drittstaat** gilt. Gemäß Art 3 Abs 2 lit a DSGVO findet die DSGVO jedoch auf die Verarbeitung personenbezogener Daten von in der EU befindlichen betroffenen Personen durch einen nicht in der EU niedergelassenen Verantwortlichen Anwendung, wenn die Datenverarbeitung mit dem Angebot von Waren und Dienstleistungen für die betroffene Person in Verbindung steht ("**Marktortprinzip**"). Dabei ist unerheblich, ob die Betroffenen tatsächlich Zahlungen leisten.

Der Begriff "**Dienstleistung**" ist weit auszulegen. Ob Dienstleistungen auf Personen in der EU **ausgerichtet** sind, ergibt sich aus einer Gesamtbetrachtung, bei der die **Sprache** einer Webseite, die **Endung der Top-Level-Domain-Adresse** und die Erleichterung des Zugangs zur Website zu berücksichtigen sind. Hat der Verantwortliche keine Hauptniederlassung im EWR, ist die DSB für Datenschutzbeschwerden zuständig.

Einer Behörde steht es im Rahmen ihrer freien Beweiswürdigung offen, aus der **mangelnden Mitwirkung** einer Verfahrenspartei im Ermittlungsverfahren für diese Partei negative Schlüsse zu ziehen. Dem Spieler die Erteilung jeglicher Auskunft zu verwehren, steht in diametralem Widerspruch zur DSGVO, wonach eine Betroffene ihr Auskunftsrecht problemlos wahrnehmen können soll.

## **EU-Rechtsakte**

- Seit dem **12.11.2025** ist der Gigabit Infrastructure Act (**GIA**, [VO \(EU\) 2024/1309](#)) in den Mitgliedstaaten unmittelbar anzuwenden. Geregelt werden darin Genehmigungsverfahren für den Ausbau von **Glasfaser-Telekommunikationsnetzen**. **Anm: Mehr Informationen erhalten Sie im Beitrag unserer Kollegen Christian Holzer und Simon Ferk: [Schneller Telekom-Ausbau dank Gigabit Infrastructure Act?](#)**
- Am **05.11.2025** wurde die "*Berichtigung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für*

*digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste)", [ABI L 2025/90880](#), kundgemacht. Die Berichtigung des **DSA** ist redaktioneller Art.*

## **Nationale Rechtsakte**

- Am **31.10.2025** wurde das **strafrechtliche EU-Anpassungsgesetz 2025**, [BGBl I 2025/65](#), kundgemacht. Mit dieser Sammelnovelle wird insb die [VO \(EU\) 2019/816](#) "*zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu **Verurteilungen von Drittstaatsangehörigen und Staatenlosen** (ECRIS-TCN) vorliegen ...*" ins innerstaatliche Recht durchgeführt. Novelliert werden ua das StrafregisterG, das TilgungsG, das Auslieferungs- und RechtshilfeG und das StaatsanwaltschaftsG. Geregelt werden ua die Abnahme und Verarbeitung von **Fingerabdrücken** im **Strafregister** sowie die Einholung von **Strafregisterauskünften** aus anderen EU-Mitgliedstaaten und dem Vereinigten Königreich.
- Am **03.11.2025** wurde "*das Bundesgesetz, mit dem das **Gesundheitstelematikgesetz 2012** und das Allgemeine Sozialversicherungsgesetz geändert werden*", [BGBl I 2025/71](#), kundgemacht. Mit der Novelle werden Rechtsgrundlagen für grenzüberschreitende Gesundheitsanwendungen geschaffen (**MyHealth@EU**, **EU-Rezept**, **EU-Patientenkurzakte**).

to the point

# Datenschutzmonitor. 46/2025 vom 19.11.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht, das **Digitalisierungsrecht** sowie das **IFG** schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

**Aktuell:** Unser **IFG-Musterpaket** stellen wir Ihnen auf Anfrage gerne zur Verfügung.

Abonnieren Sie auch unsere anderen periodischen Newsletter, **Digital Law Monitor**, **Technology & Digitalisation**, **Financial Regulation**, **Healthcare & Life Sciences** sowie **White Collar Crime** für regelmäßige, prägnante Updates [hier](#).

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 13.11.2025, 5778/17, *Manukyan/Armenien* (Überwachung, Drohung, Privatleben)

- **Rechtsprechung des EuGH**

EuGH 13.11.2025, C-654/23, *Integlio Media* (E-Mail-Newsletter, Direktwerbung, ePrivacy-RL)

- **Rechtsprechung des VwGH**

VwGH 17.10.2025, Ro 2022/04/0015 (Revision, konkrete Rechtsfrage)

- **Rechtsprechung des BVwG**

BVwG 07.10.2025, W137 2310624-1 (Unterhalt, Universität, ECTS, Verfahrensgesetze)

BVwG 07.08.2025, W605 2311036-1 (Untätigkeitsklage, Kohärenzverfahren)

BVwG 05.09.2025, W256 2294340-1 (Verfahrensgegenstand, Zurückziehung, Löschung)

BVwG 26.09.2025, W292 2315583-1 (Verfahrenshilfe)

BVwG 29.09.2025, W171 2316231-1 (Verbesserungsauftrag, Zurückweisung)

BVwG 07.10.2025, W137 2312914-1 (Zurückweisung, Verbesserungsauftrag)

BVwG 07.10.2025, W256 2285652-1; 07.10.2025, W256 2284218-1 (Massenverfahren, Aussetzung)

- **Rechtsprechung der DSB**

DSB 29.07.2025, 2024-0.368.729 (Wirtschaftsdaten, Abfall- und Umweltinformationen)

DSB 04.09.2025, 2025-0.178.139 (Beschäftigtendaten, Dienst-PC, Rechtsverteidigung)

DSB 07.11.2025, 2025-0.911.653 (Grundbuch, Akquise, berechnete Interessen)

DSB 05.11.2025, 2024-0.869.675 (Namensverzeichnis, strafverfahrensbezogene Daten, Speicherfristen, Interessenabwägung)

DSB 09.09.2025, 2023-0.346.325 (Staatsanwaltschaft, relativer Geheimhaltungsbegriff, Datenrichtigkeit)

DSB 03.09.2025, 2025-0.699.488 (Geheimhaltungsinteresse, Kaufvertrag, Interessenabwägung)

DSB 10.09.2025, 2025-0.607.071 (Videoüberwachung, öffentlicher Raum, Datenminimierung)

DSB 07.11.2025, 2025-0.910.735 (Disziplinaranzeige, Kinder, gelinderes Mittel)

DSB 03.09.2025, 2024-0.739.846 (Aufrufsystem im Wartebereich, Einwilligung, Kopplungsverbot, Anonymisierung)

- **EU-Rechtsakte**

Beschluss (EU) 2025/2307 zur Unterzeichnung des Übereinkommens der Vereinten Nationen gegen Cyberkriminalität

## To the Point:

### Rechtsprechung des EGMR

EGMR 13.11.2025, 5778/17, Manukyan/Armenien

#### **Überwachung, Drohung, Privatleben**

- Ein armenischer Staatsbürger, der Mitglied der Oppositionspartei in Armenien war, wurde vom Nationalen Sicherheitsdienst Armeniens (**NSS**) mit der Aufforderung zur Zusammenarbeit kontaktiert. Bei einem persönlichen Treffen sprach der NSS-Agent Drohungen gegenüber dem Mitglied aus, nachdem dieser die Zusammenarbeit verweigerte. Das Mitglied zeichnete das Gespräch heimlich auf und erstattete in der Folge eine Strafanzeige beim Generalstaatsanwalt. Nachdem dieser ein Strafverfahren ablehnte, ging das Mitglied dagegen vor, bis das Kassationsgericht eine erneute Prüfung verlangte. Auch im zweiten Anlauf lehnte der Generalstaatsanwalt die Einleitung eines Strafverfahrens mit der Begründung, es liege keine Straftat vor, ab. Eine Zusammenarbeit des NSS mit Einzelpersonen sei gesetzlich vorgesehen, um etwa Straftaten zu verhindern oder aufzudecken und somit die nationale Sicherheit zu schützen. Nach erfolglosem Ausschöpfen des Rechtswegs wandte sich das Mitglied wegen der Verletzung seines Rechts auf Achtung des Privatlebens (erfolgreich) an den EGMR.

Der EGMR hat erwogen: Die Äußerungen des Agenten betreffend angeblich vorhandene belastende Informationen über das Mitglied, dessen Angehörigen und seine Partei geben Anlass zur Annahme, dass die NSS eine beträchtliche Menge **personenbezogener Daten** erhoben hat. Diese Daten standen der NSS auch später noch zur Verfügung, was auch für eine Speicherung der Daten spricht. Die Speicherung von Informationen über das Privatleben einer Person durch eine Behörde ist ein Eingriff in das **Grundrecht auf Privatleben** iSd Art 8 EMRK, unabhängig von einer späteren Nutzung der Daten.

Der Begriff des **Privatlebens** umfasst auch die physische und psychische Integrität einer Person sowie deren persönliche Autonomie. Die im Gespräch geäußerten Drohungen waren schwerwiegend, weil sie geeignet waren, begründete Angst, Besorgnis und ein Gefühl der Unsicherheit hervorzurufen, was sich auf die psychische Integrität und das Wohlbefinden des Mitglieds auswirkte. Sie waren auch geeignet, die persönliche Autonomie des Mitglieds betreffend seine Laufbahn, öffentliche oder politische Tätigkeit und seinen Wohnort zu beeinträchtigen. Dies zeigt sich auch am späteren Umzug des Betroffenen in die Niederlande, wo ihm Asyl gewährt wurde. Zudem wiegen die Drohungen besonders schwer, weil sie

von einem Agenten des staatlichen Sicherheitsdienstes ausgingen.

Ein Eingriff ins Privatleben kann gerechtfertigt sein, wenn er im Einklang mit dem Gesetz steht, ein **legitimes Ziel** verfolgt und **erforderlich** ist. Das Vorbringen der Regierung, die Speicherung solle einer möglichen Zusammenarbeit zum Schutz der nationalen Sicherheit dienen überzeugt jedoch nicht. Das nationale Recht erlaubte nur eine freiwillige Zusammenarbeit mit Einzelpersonen. Der Versuch, das Mitglied durch Druck zu einer Zusammenarbeit zu bewegen, widerspricht diesem Erfordernis. Ebenso widerspricht der Einsatz von Zwang und Drohungen **rechtsstaatlichen Grundsätzen**.

### Rechtsprechung des EuGH

EuGH 13.11.2025, C-654/23, Integlio Media

#### **E-Mail-Newsletter, Direktwerbung, ePrivacy-RL**

- Die Betreiberin eines Online-Mediums erhob E-Mail-Adressen beim Erstellen eines kostenlosen Kontos für ein optionales Vollabo und verwendete die E-Mail-Adressen auch für den Versand eines Newsletters. Die rumänische Datenschutz-Aufsichtsbehörde verhängte eine Geldbuße wegen fehlender Einwilligungen und zweckwidriger Weiterverarbeitung der E-Mail-Adressen. Das vorlegende Gericht stellte dem EuGH Fragen zur Auslegung von Art 13 der [RL 2002/58/EG \(ePrivacyRL\)](#) sowie zu den Art 6, 83 und 95 DSGVO.

Der EuGH hat erwogen: Ein **Newsletter**, der individuell im Posteingang erscheint und mit dem ein kommerzielles Ziel verfolgt wird, ist **Direktwerbung**. Die E-Mail-Adressen der Nutzer werden iZm dem Verkauf einer Dienstleistung erhoben und verarbeitet. Das kostenlose Konto für das Abo ist Teil eines entgeltlichen Angebots (Kauf einer Dienstleistung und indirekte Vergütung über den Preis des Vollabonnements).

Nach der **Ausnahmeregel** des **Art 13 Abs 2 ePrivacyRL** kann die Zusendung von werblichen elektronischen Nachrichten an eigene Kunden bei der Bewerbung ähnlicher Produkte zulässig sein. Diese Regelung greift, sofern ein **Opt-out** des Empfängers bei der Erhebung und in jeder Nachricht klar, gebührenfrei und problemlos möglich ist. Die Rechtmäßigkeit der Verarbeitung folgt aus Art 13 Abs 2 ePrivacyRL iVm Art 95 DSGVO. Eine Prüfung nach Art 6 Abs 1 DSGVO entfällt, weil Art 13 Abs 2 der ePrivacy-RL als **spezielle Regelung** die Rechtmäßigkeit der Verarbeitung für Direktwerbung per E-Mail abschließend regelt und Art 95 DSGVO zusätzliche Pflichten der DSGVO in diesem Bereich ausschließt. **Anm: Diesem Urteil könnte erhebliche praktische Relevanz zukommen. Denn die DSB geht in**



ständiger Rechtsprechung von ihrer Zuständigkeit für die Beurteilung der Rechtmäßigkeit von E-Mail-Werbung aus. Dies ist schon aufgrund der Rechtsprechung des VfGH zum Grundrecht auf den gesetzlichen Richter kritisch zu sehen, weil das Fernmeldebüro diese Kompetenz ebenso für sich beansprucht. Ist eine Prüfung nach der DSGVO nicht (mehr) erforderlich, weil Art 13 Abs 2 ePrivacy als *lex specialis* vorgeht, erscheint die Zuständigkeit der DSB auch aus diesem Grund nicht gegeben. Dies müsste zudem auch für das Erheben von Cookies gelten.

### Rechtsprechung des VwGH

Aus der Rechtsprechung des VwGH:

- Die DSB stellte eine Verletzung des Geheimhaltungsrechts fest, weil der Verantwortliche auf seine E-Mail an den Betroffenen 37 weitere Empfänger in "Cc" setzte und damit Namen und Telefonnummer des Betroffenen offenlegte. Das BVwG wies die Bescheidbeschwerde des Verantwortlichen ab, ließ aber die Revision zu, weil Rechtsprechung des VwGH zum Grundsatz der Datenminimierung fehle. Das bloße Fehlen von Rechtsprechung des VwGH führt nicht automatisch zur Zulässigkeit der Revision. Da in der Zulässigkeitsbegründung der Revision keine **konkrete Rechtsfrage**, die der VwGH noch nicht beantwortet hat, dargelegt wurde, war die Revision **zurückzuweisen** ([VwGH 17.10.2025, Ro 2022/04/0015](#)).

### Rechtsprechung des BVwG

BVwG 07.10.2025, W137 2310624-1

#### **Unterhalt, Universität, ECTS, Verfahrensgesetze**

- Ein Vater brachte beim Bezirksgericht einen Antrag auf Einstellung der Alimentenzahlung ein. Um das zielstrebige Betreiben eines Studiums seiner Tochter nachzuweisen, ersuchte das Gericht die Universität um Übermittlung des Studienerfolgs (ECTS-Punkte). Die Universität übermittelte Studienerfolgsnachweise samt den Namen der Prüfer, ECTS-Punkte, Typ und Benotung an das Gericht. Dieses leitete die Unterlagen an den Vater weiter. Die Tochter erachtete die Übermittlung der Studienbestätigung in dieser Form als überschießend, weil das Bezirksgericht lediglich eine Übermittlung eines Nachweises über die seit Studienbeginn absolvierten ECTS-Punkte anforderte. Da im Unterhaltsverfahren bloß festzustellen sei, ob zielstrebig studiert werde, seien zusätzliche Daten irrelevant. Durch die erfolgte Offenlegung sah sie ihr Recht auf Geheimhaltung verletzt und brachte Datenschutzbeschwerde bei der DSB ein. Gegen

den abweisenden Bescheid der DSB erhob sie eine erfolglose Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Universitäten sind **staatliche Behörden** iSd § 1 Abs 2 DSG. Sie sind bei der Vollziehung der Studienvorschriften gemäß § 51 Abs 1 UG im Rahmen der Hoheitsverwaltung tätig. Der Begriff "Behörde" ist nach § 1 Abs 2 DSG im **funktionalen Sinn** zu verstehen. Darunter sind alle Stellen erfasst, die dem **Legalitätsprinzip** des B-VG unterliegen. Bei der **Beschränkung des Geheimhaltungsanspruchs** aus § 1 DSG sind auch die DSGVO und die in Art 5 DSGVO verankerten Grundsätze zur Auslegung heranzuziehen. Damit eine Verarbeitung rechtmäßig ist, muss ein Rechtfertigungsgrund nach Art 6 Abs 1 DSGVO kumulativ zu den in Art 5 Abs 1 DSGVO geregelten Grundsätzen vorliegen. Nach Art 6 Abs 1 lit c DSGVO ist die Verarbeitung von Daten rechtmäßig, wenn die Verarbeitung zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich ist, der der Verantwortliche unterliegt. Eine den **Verfahrensgesetzen** entsprechende Verwendung von Daten ist aus datenschutzrechtlicher Sicht zulässig.

Behördliche Eingriffe in das Grundrecht auf Datenschutz nach § 1 DSG sind wegen einer rechtlichen Verpflichtung erlaubt, wenn sie durch **gesetzliche Grundlagen** hinreichend bestimmt und verhältnismäßig sind. Die gesetzlichen Grundlagen müssen nach Art 8 Abs 2 EMRK **notwendig** und **ausreichend präzise** sein. Für jedermann muss **vorhersehbar** sein, unter welchen Voraussetzungen die Ermittlung oder Verwendung von personenbezogenen Daten für die Verwaltungsaufgabe erlaubt ist. Das UG enthält mit § 46 Abs 6 UG 2002 eine solche Rechtsgrundlage. Diese beschränkt die Datenübermittlung auf ein Minimum.

Als Maßstab zur Beurteilung der **Erforderlichkeit** der Datenübermittlung sind die konkrete Wortwahl sowie der Zweck des **gerichtlichen Aufforderungsschreibens** heranzuziehen. Ob ein Studium zielstrebig verfolgt wird, ist in Zusammenschau mit den erzielten Noten, absolvierten Lehrveranstaltungen, bestandenen Prüfungen oder der Art der Lehrveranstaltung zu prüfen. Nur anhand von übermittelten ECTS kann nicht nachgeprüft werden, ob Lehrveranstaltungen ohne Prüfungen oder ohne Bezug zum Studium besucht oder Fachprüfungen vermieden werden. Die Übermittlung durch die Universität war für die Zweckerreichung notwendig.

Aus der weiteren Rechtsprechung des BVwG:

- Den Betroffenen kommt gemäß Art 78 Abs 2 DSGVO das Recht auf Erheben einer **Untätigkeitsklage** zu, wenn die DSB eine

Datenschutzbeschwerde nicht bearbeitet, die Datenschutzbeschwerde nicht an die zuständige Aufsichtsbehörde weiterleitet oder den Betroffenen nicht über den Stand oder das Ergebnis der Datenschutzbeschwerde unterrichtet. Bei einem grenzüberschreitenden Sachverhalt ist gemäß Art 56 DSGVO die federführende Aufsichtsbehörde zuständig, welche sich nach dem Ort der Hauptniederlassung des Verantwortlichen richtet (**Kohärenzverfahren**). Da die DSB die Datenschutzbeschwerde an die deutsche Aufsichtsbehörde weitergeleitet und den Betroffenen darüber informiert hat, war die Säumnisbeschwerde zurückzuweisen. Die deutsche Aufsichtsbehörde unterliegt nicht der Zuständigkeit des BVwG, daher war auch die gegen sie gerichtete Säumnisbeschwerde zurückzuweisen ([BVwG 07.08.2025, W605 2311036-1](#)).

- In einem mit einer Datenschutzbeschwerde eingeleiteten Verfahren können **Gegenstand des Verfahrens** vor der DSB nur jene Rechtsverletzungen sein, die in der Datenschutzbeschwerde geltend gemacht werden. Der Betroffene hat keine Rechtsverletzung im Recht auf Löschung bzw Widerspruch betreffend Score-Werte geltend gemacht. Jene Spruchpunkte, in denen die DSB dennoch über die Score-Werte entschieden hat, waren daher ersatzlos zu beheben. Die **Zurückziehung der Datenschutzbeschwerde** im Verfahren vor dem **BVwG** bewirkt nachträglich die Unzuständigkeit der DSB und damit die Rechtswidrigkeit des Bescheids. Die Mitteilung des anwaltlich vertretenen Betroffenen, dass er aufgrund der zwischenzeitlich erfolgten **Löschung nicht mehr beschwert** ist, wird als Zurückziehung der Datenschutzbeschwerde gewertet. Der Bescheid der DSB ist daher ersatzlos zu beheben ([BVwG 05.09.2025, W256 2294340-1](#)).
- Hat der Antragsteller eines **Verfahrenshilfeantrags** ein Nettoeinkommen iHv EUR 1.000 und demgegenüber monatliche Verbindlichkeiten iHv EUR 350, aber keine Unterhaltspflichten, ist ihm die Übernahme der einmaligen Kosten der Eingabegebühr iHv EUR 30 und des Verfahrenshilfeantrags iHv EUR 15 zumutbar. Ergeben sich im Verfahren nur einfache und keine komplexen Sachverhalts- und Rechtsfragen, ist dem Antragsteller auch **kein Rechtsanwalt beizugeben**. Der Verfahrenshilfeantrag ist daher abzuweisen ([BVwG 26.09.2025, W292 2315583-1](#)). **Anm: Inzwischen sind die Kosten der Eingabegebühr auf EUR 50 und des Verfahrenshilfeantrags auf EUR 25 angehoben worden. An der Beurteilung des BVwG hätten diese Gebühren aber vermutlich nichts geändert.**
- Wird eine Datenschutzbeschwerde zurückgewiesen, darf das BVwG nur über die **Rechtmäßigkeit der Zurückweisung**

entscheiden. Ein Verbesserungsauftrag gemäß § 13 Abs 3 AVG ist nur dann gesetzmäßig, wenn der angenommene Mangel tatsächlich vorliegt. Die DSB darf bei der Prüfung der Datenschutzbeschwerde die **vorgelegten Unterlagen** (Beweismittel) **nicht übergehen** und sich nur auf die Darstellung des Sachverhalts und der Rechtswidrigkeit in der Datenschutzbeschwerde beschränken. Der **Verbesserungsauftrag** wurde von der DSB nicht zu Recht erteilt, weshalb der Zurückweisungsbescheid ersatzlos zu beheben ist ([BVwG 29.09.2025, W171 2316231-1](#)).

- Wird eine Datenschutzbeschwerde zurückgewiesen, darf das BVwG nur über die **Rechtmäßigkeit der Zurückweisung** entscheiden. Widersprechen sich die Angaben zum **Zeitpunkt** des behaupteten Datenschutzverstoßes in der Datenschutzbeschwerde und den vorgelegten Beweismitteln, ist der Verbesserungsauftrag berechtigt, weil dieser Zeitpunkt für die Beurteilung der Rechtzeitigkeit der Datenschutzbeschwerde erforderlich ist. Wird dem **Verbesserungsauftrag** nicht entsprochen, ist die Datenschutzbeschwerde zurückzuweisen. Eine Verbesserung des Mangels mit der Bescheidbeschwerde an das BVwG ist ausgeschlossen ([BVwG 07.10.2025, W137 2312914-1](#)).
- Ein Verfahren kann ausgesetzt werden, wenn bei einem Verwaltungsgericht in einer erheblichen Zahl von anhängigen oder zu erwartenden Verfahren eine Rechtsfrage zu lösen ist, die in einem – gleichzeitig anhängigen – Verfahren vor dem VwGH zu lösen ist. Beim BVwG sind zum selben Themenkomplex etwa 100 Bescheidbeschwerden anhängig. Damit liegt eine **erhebliche Anzahl an Verfahren** vor. Das gegenständliche Verfahren ist eines dieser Verfahren und daher **auszusetzen** (BVwG [07.10.2025, W256 2285652-1](#); [07.10.2025, W256 2284218-1](#)).

### Rechtsprechung der DSB

[DSB 29.07.2025, 2024-0.368.729](#)

### **Wirtschaftsdaten, Abfall- und Umweltinformationen**

- Ein Lebensmittelhändler meldete gemäß **§ 11a Abfallwirtschaftsgesetz (AWG)** gesetzlich bestimmte Lebensmitteldaten über das **EDM-Portal** an den Bundesminister für Umweltschutz (**BMU**). Der BMU veröffentlichte mit der Anzahl der Verkaufsflächen, der Gesamtmasse der unentgeltlich weitergegebenen Lebensmittel (**Spenden**) und der Gesamtmasse der Lebensmittel, die als Abfall weitergegeben wurden (**Abfall**), auch den Namen des als **Einzelunternehmer** tätigen Lebensmittelhändlers. Der Lebensmittelhändler behauptete in seiner

Datenschutzbeschwerde, wegen der gemeinsamen Veröffentlichung der Lebensmitteldaten mit seinem Namen in seinem Recht auf Geheimhaltung verletzt worden zu sein. Dies ua deshalb, weil bei der Registrierung im EDM-Portal nicht über die spätere namentliche Veröffentlichung informiert worden sei. Der BMU verwies zur Zulässigkeit der Veröffentlichung neben dem AWG auch auf das **Umweltinformationsgesetz (UIG)**, weil die gemeldeten Daten auch als **Umweltinformationen** zu qualifizieren seien. Die DSB wies die Datenschutzbeschwerde ab.

Die DSB hat erwogen: Als **Einzelunternehmer** ist der Lebensmittelhändler eine **natürliche Person**. Er hat Anspruch auf Geheimhaltung seiner personenbezogenen Daten. **Wirtschaftsdaten** sind personenbezogene Daten. Die **Veröffentlichung** von Daten auf einer Website ist eine **Datenverarbeitung**.

Als **hoheitliche Verwaltung** ist zu verstehen, wenn Verwaltungsorgane mit **Imperium**, dh mit Befehls- und Zwangsgewalt, handeln. Bei einem Verstoß gegen § 11a AWG ist eine Verwaltungsstrafe vorgesehen. Die Veröffentlichung der Lebensmitteldaten auf der EDM-Plattform ist somit als eine hoheitliche Maßnahme anzusehen.

Eine Datenverarbeitung ist ua dann zulässig, wenn sie zur Wahrnehmung einer im **öffentlichen Interesse** liegenden Aufgabe erforderlich ist. Die **Vermeidung der Lebensmittelverschwendung** und der **Umweltschutz** liegen zweifellos im öffentlichen Interesse. Die Bestimmung des § 11a AWG dient dazu, einen **Anreiz** für Lebensmittelhändler zu schaffen, weniger Abfall weiterzugeben und den Umweltschutz zu priorisieren. Dieser Anreiz hat offenbar gewirkt, denn der Lebensmittelhändler meldet stets höhere Spenden- als Abfallmengen. Die Veröffentlichung war **vorhersehbar**, weil der BMU über die gemeldeten Daten einen Bericht zu veröffentlichen hat. Der BMU ist zudem eine informationspflichtige Stelle nach dem **UIG**, weshalb ihn eine **proaktive Veröffentlichungspflicht** für bestimmte Umweltinformationen trifft.

Ein **Betriebs- oder Geschäftsgeheimnis** liegt nicht vor, weil entgegen den Ausführungen des Lebensmittelhändlers aus der unspezifischen Gesamtmenge der Spenden und Abfälle kein Rückschluss auf Verluste des Lebensmittelhändlers möglich ist.

Das Recht der Öffentlichkeit auf **Empfang von Informationen** zu Lebensmittelverschwendung und Umweltschutz überwiegt die Geheimhaltungsinteressen des Lebensmittelhändlers, denn seine Daten werden gemeinsam mit den Daten anderer Lebensmittelhändler veröffentlicht, wodurch eine **"Prangerwirkung"** ausgeschlossen wird. **Gelindere Mittel** stehen nicht zur

Verfügung, weil die **Angabe des Namens** des Lebensmittelhändlers erforderlich ist, um über den Umgang mit Abfall durch Lebensmittelhändler zu informieren.

DSB 04.09.2025, 2025-0.178.139

### **Beschäftigtendaten, Dienst-PC, Rechtsverteidigung**

- Ein Luftfahrtunternehmen wertete aufgrund von Hinweisen aus der Belegschaft den Dienst-PC eines Mitarbeiters aus und entdeckte dabei auch private Dateien, die teils besondere Kategorien personenbezogener Daten waren (ua Intimfotos, ein politisches Satirebild, private Korrespondenz, Zahlungsbelege). Die Dateien waren nicht als "privat" gekennzeichnet. Das Unternehmen legte Auszüge als Beweismittel in einer vom Mitarbeiter eingebrachten Kündigungsanfechtung vor. Der Mitarbeiter erhob Datenschutzbeschwerde an die DSB wegen Verletzung des Rechts auf Geheimhaltung, Information und Löschung. Die DSB wies die Beschwerde ab.

Die DSB hat erwogen: Die **Einsichtnahme** und **Auswertung** des **Dienst-PCs** war aufgrund eines begründeten Verdachts von **Dienstplichtverletzungen** sowie zur **Sicherung des Betriebsfortganges** gerechtfertigt. Die Verarbeitung durfte auf die Wahrung berechtigter Interessen iSd Art 6 Abs 1 lit f DSGVO und – hinsichtlich der besonderen Datenkategorien (Intimaufnahmen, politische Meinung) – auf die Verteidigung von Rechtsansprüchen gemäß Art 9 Abs 2 lit f DSGVO gestützt werden.

Maßgeblich ist, dass der Mitarbeiter die Daten selbst auf dem Dienstgerät gespeichert hatte, die Ordner **nicht als privat gekennzeichnet** waren und im arbeitsgerichtlichen Verfahren vernünftigerweise mit einer Auswertung des Dienst-PCs zu rechnen war. Die arbeitsrechtliche **Treuepflicht** (§ 1153 ABGB) verstärkt die Vorhersehbarkeit. Ein gelinderes Mittel als die PC-Auswertung stand nicht zur Verfügung. Die Heranziehung von Zeugen war kein gleich geeignetes Ersatzmittel. Die Vorlage der Daten an das Gericht war ebenfalls von Art 6 Abs 1 lit f und Art 9 Abs 2 lit f DSGVO gedeckt.

Ein Verstoß gegen **Informationspflichten** (Art 13 und 14 DSGVO) erfolgte nicht, denn der Mitarbeiter verfügte bereits vor der gegenständlichen Auswertung über die erforderlichen Informationen über die Verarbeitung. Er hatte die Daten selbst am Dienst-PC gespeichert und musste im Kontext der Kündigungsanfechtung mit der Verarbeitung rechnen. Das Lösungsersuchen (Art 17 Abs 1 DSGVO) durfte aufgrund der Ausnahme des Art 17 Abs 3 lit e DSGVO abgelehnt werden, solange die Daten zur Rechtsverteidigung im anhängigen arbeitsgerichtlichen Verfahren erforderlich waren

bzw sind. **Anm: Praxisrelevanz hat diese Entscheidung für Arbeitgeber, weil die Grenzen interner Untersuchungen beleuchtet werden.**

DSB 07.11.2025, 2025-0.911.653

### **Grundbuch, Akquise, berechnigte Interessen**

- Eine Immobilienreuhänderin ermittelte aus dem Grundbuch den Namen und die Anschrift einer vermeintlichen Erbin und verwendete diese für ein einmaliges postalisches Akquisitionsschreiben zum Kauf der Liegenschaft. Tatsächlich war die vermeintliche Erbin jedoch nicht Eigentümerin, sondern die Liegenschaft war Teil eines Verlassenschaftsverfahrens. Die vermeintliche Erbin erachtete sich in ihrem Recht auf Geheimhaltung verletzt und erhob (erfolgreich) Datenschutzbeschwerde bei der DSB. Die DSB hat erwogen: Dass es sich beim Grundbuch um ein **öffentliches Register** handelt, bedeutet nicht, dass die darin enthaltenen Daten **allgemein verfügbare Daten** iSd § 1 Abs 1 DSGVO sind. Die generelle Annahme des Nichtvorliegens einer Verletzung schutzwürdiger Geheimhaltungsinteressen für zulässigerweise veröffentlichte Daten ist mit der DSGVO nicht vereinbar.

Werden zulässigerweise veröffentlichte Daten nicht bloß reproduziert, sondern ein neues Element mit diesen Daten verknüpft – etwa die Verwendung der Daten zur möglichen Akquise – ist diese **Verknüpfung** eine Verarbeitung iSd Art 4 Z 2 DSGVO, die eines Erlaubnistatbestands nach Art 6, 9 oder 10 DSGVO bedarf.

In Betracht kommt die Rechtsgrundlage der überwiegenden berechtigten Interessen nach Art 6 Abs 1 lit f DSGVO. Da die personenbezogenen Daten im Grundbuch öffentlich zugänglich sind, ist von einer **geringeren Schutzwürdigkeit** auszugehen. Die Immobilienreuhänderin hat ein wirtschaftliches Interesse am Immobilienerwerb. Demgegenüber hat die vermeintliche Erbin ein Geheimhaltungsinteresse, nicht für Anfragen zu einem möglichen Grundstücksverkauf kontaktiert zu werden.

Bei einer bloß einmaligen Anfrage können die Interessen der Immobilienreuhänderin grundsätzlich überwiegen. Der Zweck der Verarbeitung erschöpft sich jedoch in der Kontaktaufnahme mit einer verfügungsberechtigten Eigentümerin. Da die vermeintliche Erbin keine **Verfügungsbefugnis** hat, kommt sie als Adressatin eines solchen Schreibens nicht in Betracht. Dass ihre Daten in einem Einantwortungsbeschluss aufscheinen, ändert daran nichts.

Es fehlt an der unbedingten **Erforderlichkeit** der Datenverarbeitung und damit zur

Verwirklichung des von der Immobilienreuhänderin wahrgenommenen Interesses. Da das Geheimhaltungsinteresse der vermeintlichen Erbin überwiegt, liegt eine Verletzung im Recht auf Geheimhaltung vor.

### Aus der weiteren Rechtsprechung der DSB:

- Die Speicherung **strafverfahrensbezogener Daten** im **Namensverzeichnis der Justiz** nach endgültigem Rücktritt von der Verfolgung erfordert eine **fortdauernde gesetzliche Grundlage** und eine **Interessenabwägung**. § 75 StPO normiert **Höchstfristen** für die Speicherung personenbezogener Daten im Namensverzeichnis. Eine Löschung vor Ablauf dieser Fristen ist im Einzelfall geboten, wenn die Interessen des Betroffenen an der Löschung die öffentlichen Interessen an der Weiterspeicherung überwiegen. Fehlt es an einer solchen **Interessenabwägung** oder hält die Weiterspeicherung einer Interessenabwägung nicht stand, mangelt es der Verarbeitung an einer gesetzlichen Grundlage iSd § 38 DSGVO ([DSB 05.11.2025, 2024-0.869.675](#)).
- Die DSB ist für die Behandlung von Datenschutzbeschwerden gegen **Staatsanwaltschaften (StA)** zuständig. Die StA schickte einen Brief an das Opfer eines bereits beendeten Strafverfahrens. Das Opfer wurde in jenem Strafverfahren von einer Opferschutzeinrichtung vertreten. Der StA war nicht bekannt, dass die angeführte Adresse jene der Opferschutzeinrichtung ist, weshalb sie den Brief an die Opferschutzeinrichtung, die zur Vertretung nicht mehr bevollmächtigt war, versandte. Der Bestimmung des § 1 Abs 1 DSGVO liegt ein "materieller", dh **"relativer Geheimhaltungsbegriff"** zugrunde. Die Beurteilung der Schutzwürdigkeit des Interesses erfolgt unter Berücksichtigung **aller konkreten Umstände** des Einzelfalls nach einem **objektiven Maßstab**. Der **Grundsatz der Datenrichtigkeit** würde **überspannt**, wenn ohne Anhaltspunkte für die Unrichtigkeit der Zustelladresse zu überprüfen wäre, ob eine aktunkundige Zustelladresse aktuell ist ([DSB 09.09.2025, 2023-0.346.325](#)). **Anm: Zur Gewährleistung der Datenrichtigkeit stellen Adressverlage und Direktmarketingunternehmen Produkte zur Verfügung, die einen Adressabgleich vor dem Versenden von Briefen ermöglichen. Die Nutzung solcher Produkte erfolgt jedoch zur Wahrung berechtigter Interessen (oder als Auftragsverarbeitung), worauf sich Behörden nicht stützen dürfen.**
- An der Telefonnummer und der Wohnadresse besteht ein **Geheimhaltungsinteresse**, weil diese personenbezogenen Daten nicht allgemein zugänglich sind. Die **ordnungsgemäße Abwicklung zweier Kaufverträge** ist ein berechtigtes

Interesse. Die Weitergabe der Telefonnummer und der Wohnadresse an einen Geschäftspartner war erforderlich, weil der Verantwortliche die Daten des Betroffenen erst nach mehreren fehlgeschlagenen telefonischen Kontaktaufnahmen weitergegeben hat. Die Datenweitergabe war auch **zweckmäßig**, weshalb die Geheimhaltungsinteressen des Betroffenen nicht überwogen ([DSB 03.09.2025, 2025-0.699.488](#)).

- Eine **Videüberwachung** kann gemäß Art 6 Abs 1 lit f DSGVO grundsätzlich eine zulässige Verarbeitung personenbezogener Daten sein, wenn sie der Wahrung berechtigter Interessen dient. Das Interesse am Schutz des Eigentums und am Schutz der körperlichen und psychischen Integrität sind solche Interessen. Eine kontinuierliche Videüberwachung, die auch den **öffentlichen Raum** und zufällig dort vorbeikommende Fußgänger und Nachbarn erfasst, ist jedoch nicht erforderlich und verletzt den **Grundsatz der Datenminimierung**. Dem Eigentümer des Grundstücks standen auch alternative, weniger weitreichende Maßnahmen zum Schutz seines Eigentums zur Verfügung. So wäre etwa ein eingeschränkter Aufnahmebereich und die auf die Öffnungszeiten des Lokals beschränkte Aufnahme, oder gar die Aufnahme mit einem Mobiltelefon bei einem unangemessenen Verhalten des Nachbarn ausreichend, um dieses gegebenenfalls vor Gericht nachweisen zu können ([DSB 10.09.2025, 2025-0.607.071](#)).
- Vorgesetzte sind gemäß § 109 Abs 1 BDG iVm § 280 Abs 1 und 2 BDG bei begründetem Verdacht zur Erstattung von **Disziplinaranzeigen** und damit verbundenen personenbezogenen Datenverarbeitungen befugt. Die Verarbeitung personenbezogener Daten muss jedoch entsprechend der **Erforderlichkeit** und dem **Grundsatz der Datenminimierung** erfolgen. Die Verwendung von Daten ist erheblich, wenn sie für die Erreichung des festgelegten Zwecks geeignet und erforderlich ist. Die **namentliche Nennung der Kinder** eines Bediensteten im Rahmen einer Disziplinaranzeige ist **nicht erforderlich**. Selbst wenn der Bedienstete angehalten wäre, die persönlichen Verhältnisse des Bediensteten festzustellen, hätte er zu einem **gelinderen Mittel** greifen können, indem er die Anzahl der Kinder samt deren Alter angibt, ohne diese namentlich zu nennen ([DSB 07.11.2025, 2025-0.910.735](#)).
- Vor- und Nachname sind personenbezogene Daten. Ist eine Online-Terminreservierung nur möglich, wenn gleichzeitig eine Einwilligung erteilt wird, dass der Name des Reservierenden **am Bildschirm** im Wartebereich bei Aufrufen **angezeigt** wird, liegt keine Einwilligung iSd DSGVO vor. Der Anforderung der **Freiwilligkeit** wird nämlich nicht entsprochen. Ist der Verantwortliche eine

**Einrichtung im öffentlichen Interesse**, kann für die Inanspruchnahme einer **staatlichen Leistung** keine Einwilligung verlangt werden (**Kopplungsverbot**). Das **Aufrufsystem im Wartebereich** ist in **anonymisierter Form**, zB durch die Verwendung eines **Nummernsystems**, zu realisieren ([DSB 03.09.2025, 2024-0.739.846](#)).

### **EU-Rechtsakte**

- Am **11.11.2025** wurde der "*Beschluss (EU) 2025/2307 des Rates vom 13. Oktober 2025 über die **Unterzeichnung** – im Namen der Europäischen Union – des **Übereinkommens der Vereinten Nationen gegen Cyberkriminalität**; Stärkung der internationalen Zusammenarbeit bei der Bekämpfung bestimmter mithilfe von Informations- und Kommunikationstechnologiesystemen begangener Straftaten und bei der Weitergabe von Beweismitteln in elektronischer Form für schwere Straftaten*", [ABI L 2025/2307](#), kundgemacht. Mit der **United Nations Convention against Cybercrime** sollen der Kampf gegen Cyberkriminalität und die **internationale Kooperation** auf diesem Gebiet gestärkt werden.

to the point

# Datenschutzmonitor. 47/2025 vom 26.11.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das Datenschutzrecht, das **Digitalisierungsrecht** sowie das **IFG** schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

**Aktuell:** Unser **IFG-Musterpaket** stellen wir Ihnen auf Anfrage gerne zur Verfügung.

Abonnieren Sie auch unsere anderen periodischen Newsletter, **Digital Law Monitor**, **Technology & Digitalisation**, **Financial Regulation**, **Healthcare & Life Sciences** sowie **White Collar Crime** für regelmäßige, prägnante Updates [hier](#).

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 18.11.2025, 50756/17, *Stanev and Bulgarian Helsinki Committee v Bulgaria* (Informationszugang, NGO, Watchdog-Funktion)

- **Rechtsprechung des EuGH**

EuGH 20.11.2025, C-57/23, *Policejní prezidium* (biometrische Identifizierungsmaßnahmen, Strafverfahren, Datenspeicherung)

EuG 19.11.2025, T-367/23 R, *Amazon EU/Kommission* (Amazon, DSA, VLOP)

EuGH 20.11.2025, C-327/24, *Lolach* (Telekommunikation, bauliche Anlagen, Zugangsverpflichtung)

EuG 19.11.2025, T-623/22, *SD/EMA* (EU-Organ, Dokumentenzugang, Geschäftsgeheimnis)

- **Rechtsprechung des VfGH**

VfGH 11.09.2025, G48/2025 (Spenden, Veröffentlichung, Gesetzesprüfung)

- **Rechtsprechung der Justiz**

OLG Innsbruck 01.10.2025, 4R117/25z (Auskunft, Selbstbedienungstools, Datenkopie)

OLG Wien 24.10.2025, 13R149/25i (Schadenersatz, Gesamtschaden, DSGVO)

- **Rechtsprechung des BVwG**

BVwG 10.11.2025, W176 2322793-1 (IFG, Leistungsauftrag, keine Feststellungskompetenz)

BVwG 11.11.2025, W274 2323801-1 (IFG, private Informationspflichtige, Frist)

BVwG 25.09.2025, W252 2315664-1 (Schenge-ner Informationssystem, Asylantrag, Löschergehen)

- **Rechtsprechung des LVwG**

LVwG Tirol 11.11.2025, LVwG-2025/46/2168-3 (Berichtigung, Eigendaten)

- **Rechtsprechung der DSB**

DSB 09.09.2025, 2025-0.243.414 (Löschbe-gehren, berechtigtes Interesse, Online-Auftritt)

DSB 08.10.2025, 2025-0.477.534 (Micro-soft 365 Education, Rollenverteilung, Auskunft, Löschung)

DSB 11.11.2025, 2025-0.758.101 (Bewerber-daten, Strafregisterauszug, Löschung)

DSB 17.09.2025, 2025-0.746.087 (Wahrunter-stellung, juristische Person, Videoüberwa-chung)

DSB 22.09.2025, 2025-0.742.062 (vorvertrag-liche Maßnahme, Rechtsgrundlage)

- **EU-Rechtsakte**

Entwurf der VO Digital Omnibus

Entwurf der VO Digital Omnibus on AI

Entwurf VO zu European Business Wallets

- **Nationale Rechtsakte**

Regierungsvorlage zum Netz- und Informati-onssystemsicherheitsgesetz 2026 (NISG 2026)

## To the Point:

### Rechtsprechung des EGMR

EGMR 18.11.2025, 50756/17, Stanev and Bulgarian Helsinki Committee v Bulgaria

#### **Informationszugang, NGO, Watchdog-Funktion**

- Ein Forscher des Bulgarischen Helsinki-Komitees (**BHK**) richtete im Februar 2016 ein Informationsbegehren an den Generalstaatsanwalt zu etwaigen Ermittlungen wegen zweier Todesfälle von Migranten an der bulgarisch-türkischen Grenze im Jahr 2015. Er ersuchte um Angaben zu Ermittlungseinleitungen, Stadium, Aktenzeichen, zuständigen Staatsanwälten, möglichen Anklagen und etwaigen Anklageschriften. Der Stellvertreter des Generalstaatsanwalts lehnte die Auskunft ab und verwies auf das strafprozessuale Sonderregime für Ermittlungsakten. Nach Ausschöpfung des nationalen Rechtswegs wandte sich der Forscher ua wegen der Verletzung von Art 10 EMRK erfolgreich an den EGMR.

Der EGMR hat erwogen: Der **Zugang zu amtlichen Informationen** fällt unter die durch **Art 10 EMRK** geschützte **Informationsfreiheit**, wenn er für die Ausübung dieser Freiheit entscheidend ist. Maßgeblich sind dabei der Zweck der Anfrage, die Art der begehrten Information, die Rolle des Antragstellers sowie die Verfügbarkeit der Information.

Die Anfrage diente der Erstellung des Jahresberichts einer **anerkannten Menschenrechts-NGO** über staatliche Reaktionen auf Berichte zu Todesfällen von Migranten an den Grenzen. Die Informationen betrafen die Frage, ob die Strafverfolgungsbehörden auf Medienberichte über Todesfälle von Migranten reagiert hatten. Themen wie Einwanderung und der Schutz des Lebens von Migranten gehören zum **Kernbereich des öffentlichen Interesses**. Der Antragsteller handelte als Forscher einer etablierten und anerkannten Menschenrechtsorganisation, der eine **Watchdog-Funktion** zukommt.

Die angefragten Informationen waren in den Systemen der Staatsanwaltschaft **vorhanden**. Die Anfrage enthielt konkrete Angaben zu Zeit, Ort, Herkunft der Gruppe, Anzahl der Betroffenen und den relevanten Ereignissen. Eine Auskunft über das Bestehen und den Stand etwaiger Ermittlungen hätte daher ohne Weiteres erteilt werden können.

Die **Ablehnung** des Informationszugangs ist ein **Eingriff** in die durch Art 10 EMRK geschützte Informationsfreiheit. Die Behörden beriefen sich auf die strafprozessuale Geheimhaltung und besondere Regeln der Akteneinsicht, nahmen jedoch keine

**einzelfallbezogene Abwägung** vor. Die Begründung blieb abstrakt. Eine pauschale Berufung auf das **Ermittlungsgeheimnis** ohne Berücksichtigung des Stadiums und Inhalts der Anfrage genügt nicht. Die Anfrage betraf lediglich die Existenz und das Stadium möglicher Ermittlungen, nicht den Zugang zu spezifischen Akteninhalten. Besteht keine laufende Ermittlung oder ist diese bereits abgeschlossen, entfällt typischerweise die Gefahr einer Beeinträchtigung. **Einschränkungen des Informationszugangs** dürfen nicht dazu führen, dass die Watchdog-Funktion von NGOs leerläuft. Die Ablehnung ohne **sachlich tragfähige und hinreichende Begründung** verletzte daher Art 10 EMRK.

### Rechtsprechung des EuGH/EuG

EuGH 20.11.2025, C-57/23, Policejní prezidium

#### **Biometrische Identifizierungsmaßnahmen, Strafverfahren, Datenspeicherung**

- Im Rahmen eines Strafverfahrens unterzog die tschechische Polizei einen Betroffenen trotz dessen Widerspruchs Identifizierungsmaßnahmen. Ihm wurden Fingerabdrücke abgenommen und ein Wangenabstrich zur Erstellung eines genetischen Profils durchgeführt. Zudem wurden Fotos und eine Personenbeschreibung angefertigt, die in polizeiliche Datenbanken aufgenommen wurden. Dem EuGH wurden Fragen zur Zulässigkeit der Erhebung biometrischer und genetischer Daten von Verdächtigen und Beschuldigten sowie zu den Speicherfristen sensibler Daten vorgelegt.

Der EuGH hat erwogen: Die Erhebung, Speicherung und Löschung **biometrischer und genetischer Daten** ist eine Verarbeitung personenbezogener Daten iSd RL 2016/680 (**DSRL-PJ**) und bedarf einer rechtmäßigen Grundlage. Die Mitgliedstaaten müssen in ihrem nationalen Recht Ziele und Zwecke der Verarbeitung sowie die Art der Daten klar festlegen. Als **besonders sensible Daten** unterliegen biometrische und genetische Daten **erhöhten Schutzanforderungen**.

Nach Art 6 DSRL-PJ ist grundsätzlich zwischen verschiedenen Kategorien betroffener Personen zu unterscheiden. Eine **einheitliche Behandlung von Verdächtigen und Beschuldigten** ist jedoch **zulässig**, wenn die Verarbeitungszwecke keine Differenzierung erfordern. Die Mitgliedstaaten müssen den Grundsatz der **Datenminimierung** beachten und geeignete **Garantien zum Schutz der Betroffenenrechte** sicherstellen.

Die Verarbeitung muss unbedingt **erforderlich** sein und setzt daher eine **einzelfallbezogene Prüfung** voraus. Dabei sind insbesondere die Art und Schwere der

mutmaßlichen Straftat, die Umstände des Einzelfalls, Bezüge zu anderen Verfahren, Vorstrafen sowie das individuelle Profil der betroffenen Person zu berücksichtigen.

Eine **schematische** oder **systematische Datenerhebung** ohne tragfähige Einzelfallgründe verstößt gegen Unionsrecht. Auch bei **wirtschaftsrechtlichen Straftaten** kann die Datenerhebung erforderlich sein. Nationale Vorschriften dürfen daher die Erhebung biometrischer und genetischer Daten von Verdächtigen und Beschuldigten zulassen.

Gemäß Art 4 DSRL-PJ dürfen personenbezogene Daten nicht länger gespeichert werden, als dies für die Verarbeitungszwecke erforderlich ist. Die Festlegung **angemessener Speicherfristen** obliegt den Mitgliedstaaten. Eine starre Höchstspeicherfrist ist nicht zwingend erforderlich, sofern **regelmäßige und wirksame Überprüfungen** die **fortdauernde Notwendigkeit** sicherstellen. Sind die gespeicherten Daten nicht mehr erforderlich, sind sie zu löschen.

EuG 19.11.2025, T 367/23 R, Amazon EU/Kommission

### **Amazon, DSA, VLOP**

- Amazon EU ("**Amazon**") hat die Entscheidung der EU-Kommission C (2023) 2746 angefochten, durch die der "**Amazon Store**" als sehr große Online-Plattform ("**VLOP**") iSd DSA eingestuft wurde. Beantragt wurde die Nichtigkeitsklage der Einstufung wegen Nichtanwendbarkeit des Art 33 Abs 1 DSA, hilfsweise die Nichtigkeitsklage der auf Art 38 und 39 DSA beruhenden Pflichten, jeweils unter Berufung auf die GRC ua wegen des vermeintlichen Verstoßes gegen die unternehmerische Freiheit, die Freiheit des Eigentums, den Schutz des Privatlebens und personenbezogener Daten sowie Gleichbehandlung. Das EuG wies die Klage ab.

Das EuG hat erwogen: Die Bestimmung des Art 33 Abs 1 DSA greift zwar in die **unternehmerische Freiheit** ein, jedoch beruht dieser Eingriff auf einem Gesetz, wahrt den Wesensgehalt und erscheint im Bereich des Verbraucher- und Systemrisikomanagements nicht offensichtlich unangemessen. VLOPs verursachen **systemische Risiken** iSd Art 34 Abs 1 DSA. Online-Marktplätze können illegale Inhalte verbreiten, Grundrechtsbeeinträchtigungen auslösen und Verbraucherinteressen in erheblichem Umfang berühren. Der **Schwellenwert** für die Einstufung als VLOP (45 Mio aktive Nutzer pro Monat) ist **geeignet**, da qualitative Alternativkriterien oder engere Pflichten weniger wirksam wären und die Umsetzung, Rechtssicherheit und Aufsicht erschweren würden.

Die Regelung des Art 38 DSA für **Empfehlungssysteme** fördert ein hohes Verbraucherschutzniveau. Die Bestimmung des Art 39 DSA (zusätzliche **Transparenz der Online-Werbung**) mindert systemische Risiken, ohne die Veröffentlichung erfolgssensibler oder personenbezogener Daten zu erzwingen und führt nicht zu einer beachtlichen Abwanderung von Werbekunden. Die Regelung des Art 40 DSA für **Datenzugang und Kontrolle** enthält Schutzmechanismen für Vertraulichkeit und **Geschäftsgeheimnisse** unter Sicherung der Verhältnismäßigkeit durch digitale Koordinatoren und geprüfte Forschende. Unzulässige Eingriffe in das Eigentum liegen nicht vor. Wenngleich diese Pflichten mit Kosten verbunden sind, begründen sie **vornehmlich administrative Lasten**.

Die **Differenzierung** des DSA nach **Reichweite** und **Plattformtyp** ist sachgerecht. Die Eingriffe in die Meinungs- und Informationsfreiheit durch Art 38 DSA erscheinen verhältnismäßig, insbesondere da Anbieter einer nicht-profilbasierten Variante weiterhin Profiling-Möglichkeiten behalten. Eingriffe in den Schutz des Privatlebens durch Art 39 und Art 40 DSA beschränken sich auf das Notwendige und sind zulässig.

### Aus der weiteren Rechtsprechung des EuGH/EuG:

- Gemäß Art 72 der RL (EU) 2018/1972 (Europäischer Kodex für die elektronische Kommunikation; **EKEK**) darf eine nationale Regulierungsbehörde einem **Telekommunikationsunternehmen** mit beträchtlicher Marktmacht die Verpflichtung auferlegen, **Zugang zu baulichen Anlagen** zu gewähren, auch wenn diese Anlagen keinen Teil des relevanten Marktes bilden. Sie muss jedoch prüfen, ob die Auferlegung dieser **Zugangspflicht** für das Erreichen der verfolgten Ziele notwendig und verhältnismäßig ist ([EuGH 20.11.2025, C-327/24, Lodalach](#)).
- Verweigert ein **EU-Organ** den **Zugang zu Dokumenten**, hat es das zu schützende Interesse, das konkret und tatsächlich beeinträchtigt werden könnte, darzutun. Beschließt ein Organ, bestimmte Daten offenzulegen, werden diese nicht nur demjenigen, der den Zugang beantragt hat, sondern auch der **Öffentlichkeit** zugänglich. Die bezifferten Ergebnisse eines Arzneimitteltests sind **sensible Geschäftsgeheimnisse** mit **realem wirtschaftlichen Wert**, deren Offenlegung konkurrierenden pharmazeutischen Unternehmen ermöglichen könnte, konkrete Vorteile zu ziehen. Behauptet ein Antragsteller ein **überwiegendes öffentliches Interesse** am Zugang zu bestimmten Dokumenten, hat er die konkreten Umstände, die dieses überwiegende



öffentliche Interesse begründen, anzuführen ([EuG 19.11.2025, T-623/22, SD/EMA](#)).

### Rechtsprechung des VfGH

Aus der Rechtsprechung des VfGH:

- Anlässlich der **Veröffentlichung** personenbezogener Daten eines Spenders auf der **Website des Rechnungshofs** beantragte das BVwG die **Aufhebung** einer Wortfolge in **§ 6 Abs 3 PartG** zur Veröffentlichung von Spendenangaben. Ein Gesetzesprüfungsantrag nach § 62 Abs 1 VfGG ist jedoch unzulässig, wenn die angefochtene **Wortfolge dem Rechtsbestand nicht angehört** oder nicht **eindeutig und genau erkennbar** ist, ob und bejahendenfalls welche Wortfolge bekämpft werden soll ([VfGH 11.09.2025, G48/2025](#)).

### Rechtsprechung der Justiz

OLG Innsbruck 01.10.2025, 4R117/25z

#### **Auskunft, Selbstbedienungstools, Datenkopie**

- Der Nutzer eines Onlineservices richtete per Post ein Auskunftersuchen an die Betreiberin des Dienstes und legte eine Ausweiskopie bei. Die Betreiberin reagierte nicht, weil sie postalische Auskunftersuchen mit Ausweiskopie grundsätzlich nicht bearbeitet, weil diese ihrer Ansicht nach nicht geeignet sind, die Identität des Inhabers eines Online-Kontos festzustellen. Stattdessen stellt sie ein Online-Datenexport-Tool zur Verfügung. Der Nutzer brachte beim zuständigen LG eine Auskunftsklage ein. Erst nach Klageerhebung nutzte er das Datenexport-Tool und erhielt eine Kopie seiner Daten in verschiedenen Dateiformaten. Das LG gab der Klage teilweise statt, weil es die Auskunft weiterhin für unvollständig erachtete. Dagegen erhob die Betreiberin eine (teilweise erfolgreiche) Berufung an das OLG Innsbruck. Das OLG Innsbruck änderte den Spruch des Urteils aber nur geringfügig zugunsten der Betreiberin ab.

Das OLG hat erwogen: Die DSGVO schreibt keine bestimmte Form für Auskunftersuchen vor. Verantwortliche dürfen betroffene Personen zwar auf **Selbstbedienungstools** verweisen, müssen aber auch Anträge über andere Kanäle bearbeiten. Nur Anträge, die an völlig **willkürliche oder offensichtlich falsche Adressen** gerichtet sind, müssen nicht beantwortet werden. Ein an den Firmensitz gerichtetes Auskunftersuchen ist daher zu beantworten.

Eine Ausweiskopie reicht im Onlinebereich meist nicht zur Legitimation aus. Eine Auskunft darf aber nicht gänzlich unbeantwortet bleiben, weil **Zweifel an der Identität** des Auskunftswerbers bestehen. Vielmehr muss der Verantwortliche gemäß Art 12

Abs 6 DSGVO **zusätzliche Informationen** anfordern. Spätestens innerhalb eines Monats nach Einlangen des Auskunftersuchens ist der Betroffene über die Gründe, weshalb der Verantwortliche nicht tätig wird, sowie über Beschwerderechte oder gerichtliche Rechtsbehelfe zu informieren.

Wiederholte Auskunftersuchen und anschließende Klagen sind **nicht rechtsmissbräuchlich**. Wurde der Dienst über längere Zeit aktiv genutzt, ist nicht davon auszugehen, dass ein Online-Konto ausschließlich zum Zweck der Geltendmachung von Schadenersatzforderungen eröffnet wurde.

Das Auskunftsrecht nach der DSGVO umfasst **drei Komponenten**: (i) die Bestätigung, ob personenbezogene Daten verarbeitet werden, (ii) die Auskunft über diese Daten und (iii) die Informationen über die Verarbeitung nach Art 15 Abs 1 und 2 DSGVO. **Datenkopien** können den Auskunftsanspruch vollständig erfüllen, wenn diese transparent sind. Eine bloße Kopie umfangreicher Datenbestände erfüllt das Erfordernis nicht. Transparenz kann durch strukturierte Zusammenstellungen hergestellt werden. Bei **Datenübermittlungen in Drittländer** sind die einschlägigen geeigneten Garantien mitzuteilen. Allgemeine Rahmenhinweise genügen nicht.

Die Auskunft hat in einem **gängigen elektronischen Format** zu erfolgen, das auf durchschnittlich ausgestatteten Endgeräten geöffnet werden kann. Der Verantwortliche muss bei der Auskunft konkret auf die Datenverarbeitung des jeweiligen Auskunftswerbers eingehen. Allgemeine Erläuterungen ersetzen keine auf den Betroffenen zugeschnittene Auskunft.

Aus der weiteren Rechtsprechung der Justiz:

- Hat der Kläger den Gesamtschaden bereits einbringlich gemacht, sind damit auch allfällige Schäden nach dem UrhG und **Ansprüche nach der DSGVO** abgedeckt, weil auch diese dem Begriff "**Gesamtschaden**" zu unterstellen sind ([OLG Wien 24.10.2025, 13R149/25i](#)).

### Rechtsprechung des BVwG

- Entscheidet ein Verwaltungsgericht über den **Informationszugang** nach dem IFG, hat es, wenn es zu diesem Ergebnis kommt, einen **Leistungsauftrag auf Informationsgewährung** zu erteilen. Wird die Information während des verwaltungsgerichtlichen Verfahrens **erteilt**, ist das Verfahren wegen **Gegenstandslosigkeit** einzustellen. Für die allfällige nachträgliche **Feststellung der Rechtswidrigkeit** des Verhaltens des Informationspflichtigen verbleibt kein Raum ([BVwG 10.11.2025, W176 2322793-1](#)).

- Verweigert ein **privater Informationspflichtiger** nach dem **IFG** die Erteilung der begehrten Information, kann innerhalb einer Frist von **vier Wochen** ein **Antrag auf Entscheidung der Streitigkeit** an das Verwaltungsgericht gestellt werden. Fristauslösend ist der Erhalt der **Mitteilung über die Informationsnichtgewährung**. Ein nach Ablauf dieser Frist gestellter Antrag auf Streitentscheidung durch das BVwG ist als **verspätet** zurückzuweisen ([BVwG 11.11.2025, W274 2323801-1](#)).
- Ein **Löschungsanspruch** nach Art 17 Abs 1 DSGVO ist aufgrund der Ausnahme des Art 17 Abs 3 lit b DSGVO ausgeschlossen, wenn die Verarbeitung zur Erfüllung einer unionsrechtlichen Pflicht bzw zur Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich ist. Die Verarbeitung stützt sich dann auf Art 6 Abs 1 lit c und e iVm Art 6 Abs 3 DSGVO. Ausschreibungen zur Rückkehr im **Schengener Informationssystem** (SIS) sind gemäß Art 3 VO (EU) 2018/1860 (**SIS-Rückkehr-VO**) verpflichtend einzugeben. Eine Löschung kommt nur in den **ausdrücklich geregelten Fällen** der Art 9 und 14 dieser Verordnung in Betracht. Mangels Ausreise- oder Nichtigkeitstatbestands (Art 14 SIS-Rückkehr-VO) und mangels Unterrichtung Österreichs durch Portugal über die (beabsichtigte) Erteilung eines Aufenthaltstitels (Art 9 Abs 2 SIS-Rückkehr-VO) lagen keine Lösungsgründe vor. Auch die Verarbeitung **biometrischer Daten** ist aus Gründen eines **erheblichen öffentlichen Interesses** nach Art 9 Abs 2 lit g DSGVO **zulässig** ([BVwG 25.09.2025, W252 2315664-1](#)).

### Rechtsprechung der LVwG

- Das Recht auf Berichtigung nach der DSGVO bezieht sich ausschließlich auf die **Berichtigung eigener Daten**. Ein Antrag auf Berichtigung von Daten, die eine andere Person betreffen, ist unzulässig ([LVwG Tirol 11.11.2025, LVwG-2025/46/2168-3](#)).

### Rechtsprechung der DSB

DSB 09.09.2025, 2025-0.243.414

#### **Löschbegehren, berechtigtes Interesse, Online-Auftritt**

- Ein ehemaliger Mitarbeiter ersuchte seine ehemalige Arbeitgeberin um Löschung von im Online-Auftritt enthaltenen Fotos, auf denen er abgelichtet war. Die ehemalige Arbeitgeberin lehnte das Löschersuchen ab, weil es sich bei dem ehemaligen Mitarbeiter um einen Projektmanager handelte und ein berechtigtes Interesse an der Verwendung der Fotos bestehe. Der ehemalige Mitarbeiter erachtete sich im Recht auf Löschung

verletzt und erhob Datenschutzbeschwerde bei der DSB. Diese stellte eine Verletzung im Recht auf Löschung fest und ordnete die Löschung an.

Die DSB hat erwogen: Verlangt ein Mitarbeiter nach Beendigung des Beschäftigungsverhältnisses die Löschung seiner personenbezogenen Daten, gilt eine zuvor erteilte **Einwilligung** zu diesem Zeitpunkt als **widerrufen**.

Um eine Datenverarbeitung auf ein **berechtigtes Interesse** zu stützen, müssen drei kumulative Voraussetzungen erfüllt sein: (i) die Wahrnehmung eines berechtigten Interesses des Verantwortlichen, (ii) die Erforderlichkeit der Verarbeitung zur Verwirklichung des Interesses und (iii) das Nichtüberwiegen der Grundrechte und Grundfreiheiten der betroffenen Person. Bei der **Erforderlichkeitsprüfung** ist zu beurteilen, ob das Interesse an der Verarbeitung nicht in zumutbarer Weise mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Person eingreifen. Einem auf Online-Marketing spezialisierten Unternehmen ist es **zumutbar, Inhalte zu ersetzen**, bei denen keine personenbezogenen Daten eines ehemaligen Mitarbeiters verarbeitet werden, oder einen **entgeltlichen Nutzungsvertrag** mit diesem abzuschließen.

Da das Beschäftigungsverhältnis beendet war und der Mitarbeiter bereits die Löschung verlangt hatte, war die Weiterverarbeitung der Inhalte **vernünftigerweise nicht zu erwarten**. Das **wirtschaftliche Interesse** des Online-Marketing-Unternehmens **überwiegt nicht** das Interesse eines ehemaligen Mitarbeiters, der einer weiteren Verarbeitung **ausdrücklich widersprochen** hat. Dies gilt insbesondere, wenn die Inhalte **öffentlich einsehbar** und somit einer **potenziell unbegrenzten Zahl** von Personen **zugänglich** sind. Zudem würde der ehemalige Mitarbeiter noch immer mit dem Unternehmen in Verbindung gebracht, obwohl er nicht mehr dort tätig ist.

DSB 08.10.2025, 2025-0.477.534

#### **Microsoft 365 Education, Rollenverteilung, Auskunft, Löschung**

- Der Bundesminister für Bildung, Wissenschaft und Forschung (**BMBWF**) stellt **Bundesschulen** Cloud-Dienste privater Anbieter für den IT-gestützten Unterricht zur Verfügung. Ein Gymnasium implementierte Microsoft 365 Education, wodurch eine Schülerin eine schulische E-Mail-Adresse samt Cloud-Speicher erhielt. Bei der Nutzung setzte Microsoft Cookies für Werbe-, Analyse- und betriebliche Zwecke. Weder die Schülerin noch ihr obsorgeberechtigter Vater wurden über den Einsatz der Cookies und die Datenverwendung durch Microsoft

für eigene Zwecke informiert. Eine Einwilligung lag nicht vor. Die Schülerin stellte – vertreten durch ihren Vater – Auskunftsersuchen an Microsoft und das Gymnasium. Da ihr weder Auskunft noch Information erteilt wurde, erhob sie (erfolgreich) Datenschutzbeschwerde bei der DSB.

Die DSB hat erwogen: Das **BildDokG 2020** iVm der **IKT-Schulverordnung** benennt die Schulleitung des Gymnasiums und den BMBWF im Zusammenhang mit der Bereitstellung von IT-Systemen und Diensten jeweils als **Verantwortliche** für die Einhaltung unterschiedlicher Aspekte der DSGVO. In unionsrechtskonformer Auslegung dieser Bestimmungen sind die Schulleitung und der BMBWF für den Einsatz von Microsoft Education 365 **gemeinsam Verantwortliche** iSd Art 26 DSGVO.

Unbeschadet ihrer Rolle als Auftragsverarbeiterin für die bloße Bereitstellung einer technischen Lösung verarbeitet Microsoft personenbezogene Daten aus **Eigeninteresse** für bestimmte eigene Geschäftstätigkeiten. Da Microsoft maßgeblich an der Entwicklung von Microsoft 365 Education beteiligt ist und dadurch Einfluss auf die technischen und organisatorischen Spezifikationen nimmt, ist sie **Verantwortliche** iSd Art 4 Z 7 DSGVO.

Das Gymnasium bzw der BMBWF stellten der Schülerin **lediglich grundsätzliche Informationen** über den Einsatz von Microsoft 365 Education zur Verfügung, sodass von einer **unvollständigen Auskunft** ausgegangen werden kann. Das Gymnasium und der BMBWF können sich nicht auf fehlenden Datenzugang berufen, weil Microsoft gemäß Art 26 Abs 1 DSGVO verpflichtet ist, sie bei der Erfüllung der Betroffenenrechte zu unterstützen. Selbst unter der Annahme, dass es sich bei Microsoft um eine Auftragsverarbeiterin handelt, ergibt sich eine **Unterstützungspflicht** aus Art 28 Abs 3 lit e DSGVO. Die Unvollständigkeit betrifft jedoch ausschließlich den Umstand, dass nicht dargelegt wurde, in welchem Umfang personenbezogene Daten im Rahmen des Einsatzes von Microsoft 365 Education an Microsoft übermittelt wurden. Die Verantwortlichkeit der Schulleitung und des BMBWF erstreckt sich hingegen nicht auf jene Datenverarbeitungen, die Microsoft nach Erhalt der Daten für eigene Zwecke vornimmt.

Auch die durch Microsoft erteilte Auskunft war unvollständig, weil unklar blieb, welche Daten aufgrund welcher Rechtsgrundlage an Microsoft übermittelt wurden, weshalb in den Protokolldaten Drittanbieter aufschienen, und was unter Begriffen wie "interne Berichterstattung", "Geschäftsmodellierung", "Betrugsbekämpfung" etc zu verstehen ist. Da bei einer **Minderjährigen** die **sprachlichen Anforderungen höher**

anzusetzen sind, genügt der Abstraktionsgrad den Anforderungen nach Art 12 Abs 1 DSGVO an sprachliche Klarheit und inhaltliche Präzision nicht.

Die bloße **Bereitstellung von Microsoft 365 Education** zu schulischen Zwecken ist datenschutzrechtlich **nicht zu beanstanden**. Rechtswidrig ist jedoch der Einsatz nicht notwendiger **Tracking-Cookies ohne Einwilligung**, sodass die Löschung nach Art 17 Abs 1 lit d DSGVO geboten ist.

DSB 11.11.2025, 2025-0.758.101

### **Bewerberdaten, Strafregisterauszug, Löschung**

- Im Rahmen eines Bewerbungsprozesses übermittelte eine Bewerberin einen Strafregisterauszug an ein Unternehmen, um dieses zu informieren, dass ein Eintrag wegen schweren Betrugs besteht. Die HR-Spezialistin des Unternehmens informierte das Management per E-Mail über den Strafregisterauszug und bat um Entscheidung, ob die Einstellung wie geplant erfolgen soll oder nicht. Nachdem die Bewerberin eine Absage hinsichtlich des anvisierten Anstellungsverhältnisses erhielt, forderte sie die Löschung ihrer personenbezogenen Daten. Das Unternehmen löschte die mit der Bewerbung in Verbindung stehenden Daten mit Ausnahme der E-Mail an das Management. Die Bewerberin erachtete sich in ihrem Recht auf Löschung und Geheimhaltung verletzt und erhob Datenschutzbeschwerde bei der DSB. Diese stellte eine Verletzung im Recht auf Löschung fest und trug dem Unternehmen die Löschung der E-Mail auf, verneinte aber eine Verletzung im Recht auf Geheimhaltung.

Die DSB hat erwogen: Gemäß Art 17 Abs 3 lit e DSGVO sind personenbezogene Daten nicht zu löschen, wenn die Verarbeitung zur **Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen** erforderlich ist. In **zeitlicher Hinsicht** greift dieser Ausnahmetatbestand erst, wenn die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen bereits **stattfindet** oder **sicher bevorsteht**. Die bloße **abstrakte Möglichkeit** rechtlicher Auseinandersetzungen reicht nicht aus. Da der Verantwortliche nicht dargelegt hat, welche konkreten zukünftigen Verfahren auf welcher Grundlage anhängig gemacht werden könnten und inwiefern durch derartige Verfahren eine Notwendigkeit zur weiteren Speicherung der personenbezogenen Daten begründet wird, liegen die Voraussetzungen des Art 17 Abs 3 lit e DSGVO nicht vor.

Aufgrund der **Öffnungsklausel** des Art 10 DSGVO übernahm der österreichische Gesetzgeber in **§ 4 Abs 3 DSG** eine Regelung zur Verarbeitung **strafrechtlich**

**relevanter Daten durch Private.** Diese Bestimmung erlaubt die Verarbeitung solcher Daten, wenn dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten nach Art 6 Abs 1 lit f DSGVO erforderlich ist und die Interessen der betroffenen Person gewahrt bleiben. Das Unternehmen hatte ein **berechtigtes Interesse** daran zu prüfen, ob die Verurteilung der Bewerberin wegen schweren Betrugs ein Einstellungshindernis ist und diese Information an die zuständigen Entscheidungsträger weiterzuleiten. Die Datenverarbeitung war für die Prüfung und interne Diskussion **erforderlich**. Da die Bewerberin den Eintrag im Strafregister selbst mitgeteilt hatte, war die Datenverarbeitung auch **vorhersehbar**. Die Interessenabwägung fällt zugunsten des Unternehmens aus, sodass keine Verletzung im Recht auf Geheimhaltung vorliegt.

Aus der weiteren Rechtsprechung der DSB:

- Bei einer **Wahrunterstellung** wird das Sachverhaltsvorbringen einer Partei nicht als tatsächlich gegeben festgestellt, sondern geprüft, ob der behauptete Rechtsanspruch bei **hypothetischer Richtigkeit** begründet wäre. Wenn nicht, entfällt die Ermittlung und Feststellung der Richtigkeit des Sachverhalts, weil die Tatsachen rechtlich nicht maßgeblich iSd § 37 AVG sind. Die Datenschutzbeschwerde einer **juristischen Person** wegen Verletzung im Recht auf Information ist zurückzuweisen, da diese nicht in den **Schutzbereich** der DSGVO fällt und **§ 1 Abs 3 DSG keine Art 13 DSGVO entsprechenden Informationsrechte** vorsieht. Obwohl juristische Personen dem Schutzbereich des **§ 1 DSG** unterliegen und nach § 24 DSG **beschwerdelegitimiert** sein können, ist eine Verletzung ihres Geheimhaltungsrechts durch **Videoüberwachung** mangels tatsächlicher Erfassungs- und damit Datenverarbeitungsmöglichkeit **denkunmöglich**. Daten natürlicher Personen, die der juristischen Person zugerechnet werden, sind nicht *ipso facto* Daten der juristischen Person, da die Rechte nach der DSGVO und dem DSG höchstpersönlich sind ([DSB 17.09.2025, 2025-0.746.087](#)).
- Im Rahmen eines **vorvertraglichen Verhältnisses** gemäß Art 6 Abs 1 lit b DSGVO im **geschäftlichen Verkehr zwischen Unternehmen** ist das Erforderlichkeitskriterium für die Datenverarbeitung erfüllt, wenn unter Beachtung der Grundsätze des Art 5 DSGVO eine **Handlungsoption** gewählt wird, die bei **objektiver Betrachtung** für keinen der am vorvertraglichen Verhältnis Beteiligten **unüblich und überraschend** sein musste. Die **Weiterleitung einer Produkthanfrage samt**

**Kontaktdaten** an ein lieferberechtigtes Vertriebsunternehmen ist eine **zulässige vorvertragliche Maßnahme**, wenn der Zweck des vorvertraglichen Verhältnisses die Erwirkung der Lieferung eines Produkts ist und die Weiterleitung weder den Grundsatz der Rechtmäßigkeit noch jenen der Zweckbindung oder der Datenminimierung verletzt ([DSB 22.09.2025, 2025-0.742.062](#)).

### EU-Rechtsakte

- Am **19.11.2025** wurden die Vorschläge der **Europäischen Kommission** für (i) einen **"Digital Omnibus"**, [COM\(2025\) 837 final](#), (ii) einen **"Digital Omnibus on AI"**, [COM\(2025\) 836 final](#) und (iii) die Schaffung eines **"European Business Wallets"**, [COM\(2025\) 838 final](#), veröffentlicht. Die Verordnungsentwürfe sollen ua die Einhaltung der **DSGVO**, der **KI-VO** und des **Data Acts** vereinfachen. **Anm: Nähere Informationen finden Sie in unserem Legal Insight [European Commission presents "Digital Omnibus" package](#).**

### Nationale Rechtsakte

- Am **20.11.2025** ist die **Regierungsvorlage** zum Netz- und Informationssystemssicherheitsgesetz 2026 ([NISG 2026](#)) im Nationalrat eingelangt. Mit dem NISG 2026 wird die [NIS-2-RL \(EU\) 2022/2555](#) ins innerstaatliche Recht umgesetzt. Als zuständige Behörde wird das Bundesamt für Cybersicherheit (**Cybersicherheitsbehörde**) benannt. **Anm: Nähere Informationen finden Sie in unserem Legal Insight [Österreich: NISG 2026 – Alles, was Sie wissen müssen](#).**

to the point

# Datenschutzmonitor. 48/2025 vom 03.12.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das **Datenschutzrecht**, das **Digitalisierungsrecht** sowie das **IFG** schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Wir freuen uns Ihnen die **hundertste Ausgabe** des Schönherr Datenschutzmonitors in ebenso vielen Wochen zuschicken zu dürfen. Diese Gelegenheit wollen wir auch nutzen, um uns bei unseren rund **350 Abonnenten** herzlich zu **bedanken!**

Abonnieren Sie auch unsere anderen periodischen Newsletter, **Digital Law Monitor**, **Technology & Digitalisation**, **Financial Regulation**, **Healthcare & Life Sciences** sowie **White Collar Crime** für regelmäßige, prägnante Updates [hier](#).

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH SA 27.11.2025, C-421/24, *AGCOM* (Glücksspiel, Werbung, E-Commerce-RL, Video Sharing)

- **Rechtsprechung des VwGH**

VwGH 22.10.2025, Ra 2023/04/0075 (Videoüberwachung, § 12 DSG, berechnete Interessen, Datenminimierung, Verhältnismäßigkeit)

- **Rechtsprechung der Justiz**

OLG Wien 25.09.2025, 7Ra17/25h (betriebliche Echtzeit-Videoüberwachung, Screenshots)

OLG Wien 07.10.2025, 20Bs245/25p; OLG Innsbruck 07.10.2025, 7Bs232/25p (Beschlagnahme von Datenträgern)

OLG Wien 21.03.2024, 13R3/24t (DSGVO, Verwaltungsverfahrenskosten, Rettungsaufwand)

OLG Innsbruck 05.06.2025, 2R65/25p (Akteneinsicht, rechtliches Interesse, Rechtsanspruch)

- **Rechtsprechung des BVwG**

BVwG 03.09.2025, W292 2248134-1 (Exzess, Auslandsbezug, hohe Anzahl)

BVwG 29.09.2025, W292 2273455-1 (Exzess, Missbrauchsabsicht, Sorgerecht)

BVwG 24.09.2025, W295 2297643-1 (unerbetene Werbeanrufe, Einwilligung, wirksames Kontrollsystem, Verschulden)

- **Rechtsprechung des LVwG**

LVwG Wien 04.11.2025, VGW-113/032/16206/2025 (IFG, ORF, Zuständigkeit)

LVwG Wien 16.10.2025, VGW-113/027/15142/2025 (IFG, Fristverlängerung, Anhörungsrecht)

- **Rechtsprechung der DSB**

DSB 17.09.2025, 2025-0.677.482 (Plattform, Auskunft, Namensidentität)

DSB 11.09.2025, 2023-0.643.180 (Rollenverteilung, Übermaßverbot, behördeninterne Datenweitergabe, Förderung)

DSB 12.09.2025, 2024-0.739.833 (Videoüberwachung, öffentliche Fläche, Besitzstörung)

DSB 17.09.2025, 2025-0.502.649 (Auskunft, Umfang, Negativauskunft, Löschprotokoll)

## To the Point:

### Rechtsprechung des EuGH

Aus der Rechtsprechung des EuGH:

- Die Regulierung des **Glücksspiels** ist in der Union nicht harmonisiert. Das Herkunftslandprinzip der **E-Commerce-RL 2000/31/EG** gilt deshalb nicht für das Angebot von Glücksspielen. Daran hat auch das Gesetz über digitale Dienste ("**DSA**") nichts geändert. Die Beschränkung von **Werbung** kann Teil der Politik eines Mitgliedstaats zur Regulierung von Glücksspiel sein. Die Tätigkeit einer **Video-Sharing-Plattform** ist aber weder das Angebot von Glücksspiel noch Werbung dafür. Eine **Video-Sharing-Plattform** fällt auch dann unter die **Haftungsbefreiung für Hosting-Anbieter**, wenn über die Plattform Glücksspielwerbung verbreitet wird, sofern sie nicht in die hochgeladenen Inhalte eingreift. Eine **Vergütung** für die Dienstleistung oder eine **Anzeigeoptimierung** schadet nicht ([EuGH SA 27.11.2025, C-421/24, AGCOM](#)).

### Rechtsprechung des VwGH

VwGH 22.10.2025, Ra 2023/04/0075

#### **Videoüberwachung, § 12 DSG, berechnigte Interessen, Datenminimierung, Verhältnismäßigkeit**

- Auf einer Liegenschaft in der Nähe einer Straßenbahnstation kam es vor, dass Passanten ihre Notdurft im Hauseingang, im Hof oder auf den Stiegen verrichteten. Es kam auch zu Sachbeschädigungen und einer Brandstiftung. Die Liegenschaftseigentümerin installierte daher ua eine **funktionsstüchtige Videokamera**. Die Kamera war **gekennzeichnet** und wurde noch unter dem alten DSG 2000 **registriert**. Nach der Registrierung wurde der Aufnahmebereich jedoch geändert. Ein Mieter fühlte sich in seinem Geheimhaltungsrecht verletzt und brachte eine erfolgreiche Datenschutzbeschwerde ein. Das BVwG wies die Bescheidbeschwerde der Liegenschaftseigentümerin ab und führte ua aus, dass § 12 DSG mit der DSGVO unvereinbar sei und daher nicht zur Anwendung gelange. Über außerordentliche Revision der Liegenschaftseigentümerin hob der VwGH infolge Verletzung von Verfahrensvorschriften das Erkenntnis des BVwG auf.

Der VwGH hat erwogen: Die DSGVO ist eine EU-Verordnung (**VO**). Innerstaatliche Vorschriften, die die Tragweite einer VO beeinträchtigen, sind unionsrechtswidrig. Dennoch können Ordnungsbestimmungen für ihre **Durchführung** den Erlass von Maßnahmen durch die Mitgliedstaaten erfordern. Solche **Durchführungsmaßnahmen** sind zulässig, wenn sie die unmittelbare Anwendbarkeit der VO nicht vereiteln, deren

unionsrechtliche Natur nicht verbergen und nur die Ausübung des durch die VO verliehenen **Ermessens** konkretisieren.

Grundsätzlich bestehen keine Bedenken dagegen, dass in **innerstaatlichen Vorschriften** bestimmte Interessen als **berechnigte Interessen** iSd Art 6 Abs 1 lit f DSGVO normiert werden. Es spricht auch nichts dagegen, den Schutz des Eigentums oder von Personen an bestimmten besonders gefährdeten Orten als (**zulässiges**) **berechnigtes Interesse** anzuerkennen. Mit der Regelung des **§ 12 Abs 2 Z 4 iVm Abs 3 Z 2 DSG** (Videoüberwachung an bestimmten besonders gefährdeten Orten) hat der Gesetzgeber jedoch die Interessenabwägung auf gesetzlicher Ebene zugunsten einer zulässigen Bildverarbeitung vorweggenommen. Dadurch wird die Berücksichtigung der **konkreten Umstände des Einzelfalls** durch die DSB und das BVwG verhindert, weshalb diese Bestimmungen mit dem Unionsrecht **unvereinbar** sind und unangewendet zu bleiben haben.

Es fehlt allerdings eine nachvollziehbare Begründung des BVwG, weshalb es die Erforderlichkeit der Videoüberwachung zwar bejaht, aber gleichzeitig von einer Unverhältnismäßigkeit der Videoüberwachung ausgeht. Mit dem Grundsatz der **Datenminimierung** wird der Grundsatz der **Verhältnismäßigkeit** zum Ausdruck gebracht. Dieser ist gemeinsam mit der Voraussetzung der **Erforderlichkeit** der Datenverarbeitung zu prüfen. Diese Voraussetzung verlangt eine Abwägung der jeweiligen einander gegenüberstehenden Rechte und Interessen, welche unter **Berücksichtigung der spezifischen Umstände des Einzelfalls** vorzunehmen ist.

Bei der Abwägung der jeweiligen einander gegenüberstehenden Rechte und Interessen sind insb die **vernünftigen Erwartungen** der Betroffenen sowie der Umfang der fraglichen Verarbeitung und deren Auswirkungen auf diese Person zu berücksichtigen. Zu den konkreten Umständen der Videoüberwachung, die im Rahmen der **Interessenabwägung** zu berücksichtigen sind, zählen weiters der räumliche und zeitliche Umfang der Videoüberwachung, ob die Videoüberwachung auf bestimmte Bereiche begrenzt ist, die Form der Beobachtung, die Zugriffsbeschränkungen sowie die Speicherdauer.

Eine **fortdauernde Videoüberwachung** ist ein erheblicher Eingriff in das Geheimhaltungsrecht. Auch bei einer "fortdauernden Videoüberwachung" hat jedoch eine Auseinandersetzung mit den jeweiligen Umständen des Einzelfalls, ua mit dem Umfang der fraglichen Verarbeitung und deren Auswirkungen auf die Betroffenen, zu erfolgen. Zu beachten ist, dass die Videoaufnahmen nach drei Tagen automatisch gelöscht

wurden. Zu prüfen wäre zudem gewesen, ob die überwiegende Mehrzahl der Mieter der Videoüberwachung zugestimmt hätte, was sie bei einer anderen Videokamera betreffend dieselbe Liegenschaft getan hat. **Anm: Der VwGH hat § 12 Abs 2 Z 4 iVm Abs 3 Z 2 DSGVO für unionsrechtswidrig erklärt. Gleichzeitig sprach er erstmals aus, dass der nationale Gesetzgeber berechnete Interessen iSd Art 6 Abs 1 lit f DSGVO festlegen darf, solange eine einzelfallbezogene Überprüfung möglich bleibt. Bemerkenswert ist die Klarstellung des VwGH, dass der Datenminimierungsgrundsatz den Verhältnismäßigkeitsgrundsatz zum Ausdruck bringt und gemeinsam mit der Erforderlichkeit zu prüfen ist. Zudem skizziert der VwGH einen Leitfaden für die Zulässigkeitsprüfung von Videoüberwachungen.**

### **Rechtsprechung der Justiz**

Aus der Rechtsprechung der Justiz:

- Die **betriebliche Echtzeit-Videoüberwachung** einer **Verkaufsfläche** und die gezielte Anfertigung einzelner **Screenshots** vom Livestream zur **Beweissicherung** der Pflichtverletzung einer Arbeitnehmerin sind bei vorheriger schriftlicher Information/Einwilligung und überwiegend berechtigten Interesse nach Art 6 Abs 1 lit f DSGVO iVm **§ 12 DSGVO** verhältnismäßig und zulässig. Mangels Verbreitung der Screenshots liegt auch keine Verletzung des Rechts am eigenen Bild nach § 78 UrhG vor ([OLG Wien 25.09.2025, 7Ra17/25h](#)).
- Gemäß § 115f StPO ist die **Beschlagnahme von Datenträgern** und Daten zulässig, wenn sie aus **Beweisgründen** erforderlich erscheint und bestimmte Tatsachen die Annahme rechtfertigen, dass dadurch wesentliche Informationen zur Aufklärung einer Straftat ermittelt werden können. Eine Beschlagnahme darf daher nicht bloß zur Sicherheit oder zur Vorsicht erfolgen und nicht dazu dienen, erst einen Verdacht zu begründen. Ein solcher Eingriff berührt sowohl Art 8 EMRK als auch § 1 DSGVO und unterliegt daher einer **strengen Verhältnismäßigkeitsprüfung**. Entscheidend sind insbesondere die Schwere und Art der Straftat, die Intensität des Tatverdachts, die Art der betroffenen Daten, der Speicherort sowie der voraussichtliche Zeitraum der Auswertung. Die Beschlagnahme darf jeweils nur für jenen **Zeitraum** angeordnet und bewilligt werden, der zur Erreichung ihres Zwecks erforderlich ist. Liegen die Voraussetzungen für die Beschlagnahme nicht mehr vor, ist diese gemäß § 115f Abs 9 StPO gerichtlich aufzuheben ([OLG Wien 07.10.2025, 20Bs245/25p](#); [OLG Innsbruck 07.10.2025, 7Bs232/25p](#)).

- Hinsichtlich der **Kosten** der Beteiligten eines **Verwaltungsverfahrens** gilt, dass ein Kostenersatz zwischen den Beteiligten nur dann stattfindet, wenn die Verwaltungsvorschriften ausnahmsweise eine entsprechende Regelung enthalten (§ 74 AVG). Einen solchen Kostenersatz für Verfahrenskosten (insb Rechtsanwaltskosten) sehen weder die **DSGVO** noch das **DSG** vor. Unter bestimmten Voraussetzungen können die Kosten des Verwaltungsverfahrens jedoch als **Schadenersatz** im Zivilrechtsweg geltend gemacht werden. Der Einwand der **Unzulässigkeit des Rechtswegs** trifft daher nicht zu. Dies gilt etwa bei der Übertretung einer privatrechtlichen Vereinbarung oder wenn Kosten als **Rettungsaufwand** angefallen sind, um eine Gefahr abzuwenden. Ein Rettungsaufwand kann nur unvermeidbare Verfahrenshandlungen umfassen ([OLG Wien 21.03.2024, 13R3/24t](#)).
- Ohne Zustimmung aller Parteien ist einem **Dritten Akteneinsicht** nur zu gewähren, soweit der Antragsteller ein **rechtliches Interesse** glaubhaft macht und keine überwiegenden Interessen (berechtigte Interessen eines anderen oder öffentliche Interessen nach **Art 23 Abs 1 DSGVO**) entgegenstehen. Ein **rechtliches Interesse** muss in der Rechtsordnung begründet und von ihr gebilligt sein. Es kann insb durch die Verfolgung von Ansprüchen begründet sein. Das ist gegeben, wenn die Rechtsposition des Antragstellers durch Kenntnis eines Sachverständigengutachtens günstig beeinflusst werden kann ([OLG Innsbruck 05.06.2025, 2R65/25p](#)).

### **Rechtsprechung des BVwG**

[BVwG 03.09.2025, W292 2248134-1](#)

#### **Exzess, Auslandsbezug, hohe Anzahl**

- Ein Student nutzte verschiedene Online-Dienste, legte dort zahlreiche Nutzerkonten an und gab dort seine personenbezogenen Daten bekannt. Anschließend stellte er zwischen Februar und August 2021 sechzehn Auskunfts- und Löschersuchen an verschiedene, überwiegend im Ausland ansässige Verantwortliche. Er begründete die Vielzahl seiner Ersuchen damit, wissen zu wollen, welche personenbezogenen Daten bei den unterschiedlichen Online-Diensten vorhanden sind. Die Online-Dienste beantworteten seine Auskunfts- oder Löschersuchen häufig erst nach Ablauf der Monatsfrist des Art 12 Abs 3 DSGVO. Der Student erhob ua bereits einen Tag nach Fristablauf Datenschutzbeschwerden an die DSB. Die DSB lehnte die Behandlung der Datenschutzbeschwerden gemäß Art 57 Abs 4 DSGVO ab. Der Student erhob dagegen erfolglos Beschwerde an das BVwG. Der VwGH setzte das Verfahren bis zur Entscheidung des

EuGH 09.01.2025, C-416/23 (*Österreichische Datenschutzbehörde*) aus und hob in weiterer Folge das Erkenntnis des BVwG wegen inhaltlicher Rechtswidrigkeit auf. Das BVwG wies die Bescheidbeschwerde des Studenten im zweiten Rechtsgang ab.

Das BVwG hat erwogen: Bei der Beurteilung, ob eine **Unverhältnismäßigkeit** bei der Antragstellung durch den Studenten vorliegt, spielt die **Anzahl der gestellten Anträge** eine gewichtige Rolle. Das Einbringen von sechzehn Datenschutzbeschwerden während eines Betrachtungszeitraums von nur rund sieben Monaten in ähnlich gelagerten Fällen mit Auslandsbezug kann als erhebliche Anzahl an anhängig gemachten Verfahren vor der DSB angesehen werden. Darüber hinaus kommen bei Verfahren, in welchen die datenschutzrechtlich Verantwortlichen **außerhalb Österreichs ihre Hauptniederlassung** haben, der DSB komplexe Aufgaben im Zuge des **Kooperationsmechanismus** nach Art 56 ff DSGVO zu. Dies erfordert einen weit überdurchschnittlichen Einsatz von zeitlichen und personellen Ressourcen auf Seiten der DSB.

Die Verfahrensführung des Studenten erfolgte, ohne dass dies **objektiv erforderlich** gewesen wäre, um seine aus der DSGVO erwachsenden Rechte zu schützen. Die **Nichteinhaltung der Frist** zur Beantwortung der Online-Dienste **berührt** den Studenten in **verhältnismäßig geringem Ausmaß** in seinen subjektiven Rechten. Dementsprechend ermöglicht § 24 Abs 6 DSG der DSB in Fallkonstellationen, in denen der Verantwortliche – wenn auch nach Verstreichen der Frist des Art 12 Abs 3 DSGVO – etwa einem Auskunfts- oder Löschersuchen entspricht, das behördliche Verfahren formlos einzustellen. Weiters hat der Student trotz entsprechender behördlicher Aufforderungen nicht mehr am Verfahren mitgewirkt.

Folglich war in Bezug auf die Datenschutzbeschwerden des Studenten **Missbrauchsabsicht nach Art 57 Abs 4 DSGVO** anzunehmen. Im Unionsrecht gilt der **allgemeine Rechtsgrundsatz**, dass Bürger sich nicht in betrügerischer oder missbräuchlicher Weise auf unionsrechtliche Normen berufen dürfen.

Da der Student von einem gewissen Maß an **Aktivismus** zur Gewinnung von Rsp bei der Führung von Datenschutzverfahren getrieben scheint, ist davon auszugehen, dass er auch einen allfälligen **Kostenbescheid** rechtlich bekämpfen würde. Vor diesem Hintergrund ist zunächst keine angemessene Gebühr für die Bearbeitung der exzessiven Datenschutzbeschwerden des Studenten zu verlangen, sondern die Behandlung dieser Datenschutzbeschwerden abzulehnen.

#### Aus der weiteren Rechtsprechung des BVwG:

- Bei **offenkundig unbegründeten** oder **exzessiven** Datenschutzbeschwerden darf die DSB eine Gebühr verlangen oder sich weigern, tätig zu werden (Art 57 Abs 4 DSGVO). Die Aufsichtsbehörde trägt die **Beweislast** für den offenkundig unbegründeten oder exzessiven Charakter der Datenschutzbeschwerde. Der EuGH legt Art 57 Abs 4 DSGVO dahingehend aus, dass Anfragen nicht allein aufgrund ihrer Zahl als exzessiv eingestuft werden können. Die DSB muss unter Berücksichtigung der einzelfallbezogenen Umstände eine **Missbrauchsabsicht** des Betroffenen nachweisen. Eine Missbrauchsabsicht liegt vor, wenn jemand Datenschutzbeschwerden einreicht, ohne dass dies objektiv erforderlich ist, um die Rechte aus der DSGVO zu schützen. Eine Missbrauchsabsicht kann auch darin liegen, dass der Betroffene die **Unrichtigkeit seines Rechtsstandpunkts** kennen musste, weil er dieselbe Datenschutzbeschwerde bereits erfolglos erhoben hatte. Dem Betroffenen war bekannt, dass ihm hinsichtlich seines Sohnes kein **Sorgerecht** zukommt, ein Kontaktverbot besteht und bereits über eine Vielzahl seiner ähnlich gelagerten Datenschutzbeschwerden gegen ihn entschieden wurde. Der Betroffene musste sich der Unrichtigkeit seines Rechtsstandpunkts daher bewusst sein, weshalb die DSB die Behandlung der Datenschutzbeschwerde wegen rechtsmissbräuchlicher und exzessiver Ausübung des Beschwerderechts zu Recht abgelehnt hat ([BVwG 29.09.2025, W292 2273455-1](#)).
- **Anrufe zu Werbezwecken** sind ohne vorherige Einwilligung des Nutzers unzulässig. Es gibt **keine Ausnahme**. Ein Nutzer kann eine **Einwilligung** durch **ausdrückliche oder konkludente Willenserklärung** erteilen. Eine **konkludente Einwilligung** setzt ein Verhalten voraus, das zweifelsfrei als Einwilligung zum Erhalt von Werbeanrufen verstanden werden kann. Ersucht ein Nutzer, der seine Einwilligung erteilt hat, um Unterlassung weiterer Anrufe, so ist dies als **Widerruf** der Einwilligung zu werten. Spätere Anrufe erfolgen ohne Einwilligung. Da die Strafdrohung für unerbetene Anrufe zu Werbezwecken EUR 50.000 übersteigt (§ 174 Abs 1 iVm § 188 Abs 6 Z 9 TKG), gilt die **Fahrlässigkeitsvermutung** des § 5 Abs 1 VStG nicht. Das Verschulden ist nachzuweisen. Der Beschuldigte hat jedoch ein **wirksames Kontrollsystem** einzurichten und **Vorkehrungen** für den Fall **nichtregelkonformen Verhaltens der Mitarbeiter** zu treffen ([BVwG 24.09.2025, W295 2297643-1](#)).



## Rechtsprechung der LVwG

LVwG Wien 04.11.2025, VGW-113/032/16206/2025

### **IFG, ORF, Zuständigkeit**

- Ein Informationswerber beantragte beim Österreichischen Rundfunk (**ORF**) Informationen über Protokolle des Stiftungsrats aus September 2024 und die dort vorgelegten Dokumente. Zusätzlich fragte er, ob diese Informationen aus Sicht des ORF aus einer Verwaltungstätigkeit oder aus einer unternehmerischen Tätigkeit stammen und welche Verfahrensregeln aus Sicht des ORF zur Anwendung kommen. Der ORF verweigerte die Auskunft unter Hinweis auf Verschwiegenheitspflichten sowie Geschäfts- und Betriebsgeheimnisse. Daraufhin stellte der Informationswerber beim LVwG Wien den Antrag, gemäß § 14 Abs 8 IFG auszusprechen, dass ihm der ORF Zugang zu den begehrten Informationen gewähren muss.

Das LVwG hat erwogen: Bei **Nichterteilung der Information durch eine Stiftung** ist für den **Rechtsschutz** entweder das BVwG oder ein LVwG zuständig (§ 14 Abs 1 IFG). Gemäß § 14 Abs 1 Z 1 IFG ist das BVwG zuständig, wenn eine Stiftung unmittelbar von **Bundesorganen** oder von Personen geleitet wird, die von Bundesorganen bestellt werden. Der Gesetzeswortlaut lässt offen, ob eine mehrheitliche oder ausschließliche Bestellung durch Bundesorgane erforderlich ist oder ob jede Beteiligung an der Verwaltung durch von Bundesorganen bestellte Personen(gemeinschaften) ausreicht.

Die Geschäfte des ORF werden gemäß § 19 Abs 1 ORF-G vom **Stiftungsrat, Generaldirektor** und **Publikumsrat** besorgt. Die **gesetzlichen Bestellungsmodalitäten** der §§ 20 ff ORF-G zeigen, dass der ORF nicht ausschließlich oder mehrheitlich von durch Bundesorgane bestellten Personen(gemeinschaften) verwaltet wird, diese jedoch eine maßgebliche Rolle spielen.

Weder die Erläuterungen noch der Wortlaut des § 14 Abs 1 Z 1 IFG verlangen für die Zuständigkeit des BVwG eine qualifizierte Mehrheit von durch Bundesorgane bestellten Personen. Vielmehr ist allgemein von einer Verwaltung durch von Bundesorganen bestellte Personen(gemeinschaften) die Rede, die auch gegeben ist, wenn eine Stiftung nicht mehrheitlich von durch Bundesorgane bestellten Personen(gemeinschaften) verwaltet wird. Dafür spricht auch die **systematische Unterscheidung** zwischen Stiftungen, Fonds oder Anstalten einerseits und Unternehmungen andererseits. Bei Unternehmungen ist die Zuständigkeit des BVwG ausdrücklich auf solche beschränkt, an denen der Bund eine Beherrschung in einem bestimmten qualifizierten Ausmaß ausübt, während für Stiftungen, Fonds oder

Anstalten keine solche Einschränkung vorgenommen wurde, sondern **allgemein** auf eine (nicht näher qualifizierte) Verwaltung durch von Bundesorganen bestellte Personen(gemeinschaften) abgestellt wird.

Es wird daher davon ausgegangen, dass § 14 Abs 1 Z 1 IFG jegliche Stiftungen erfasst, in denen die Verwaltung durch von Bundesorganen bestellte Personen(gemeinschaften) geführt wird, auch wenn diese die Stiftung nicht allein oder mehrheitlich verwalten. Nach diesem Verständnis ist das **BVwG** für die Entscheidung über die Nichterteilung von Informationen durch den ORF **zuständig**. **Anm: Nähere Informationen zu den Geheimhaltungsgründen des IFG insb iZm privaten Informationspflichtigen finden Sie in der RDB (Paywall): [Cudlik/Petschinka, Ausgewählte Fragen der Geheimhaltung im IFG, ecolex 2025, 847.](#)**

### Aus der weiteren Rechtsprechung der LVwG:

- Die **Fristverlängerung** ist zur Wahrung des Anhörungsrechts eines anderen iSd § 10 IFG zulässig. Dem klaren Wortlaut des § 8 Abs 2 IFG ist nicht zu entnehmen, dass zusätzlich zum Hinweis auf das Anhörungsrecht gemäß § 10 IFG weitere **besondere Gründe** für die Fristverlängerung anzuführen sind. Zweck der Bestimmung ist es, den Informationswerber darüber in Kenntnis zu setzen, aus welchen Gründen die Informationerteilung noch nicht erfolgt ist. Es genügt daher, den besonderen Grund kurz zu umreißen oder auf die erforderliche **Anhörung** gemäß § 10 IFG **hinzuweisen** ([LVwG Wien 16.10.2025, VGW-113/027/15142/2025](#)).

## Rechtsprechung der DSB

DSB 17.09.2025, 2025-0.677.482

### **Plattform, Auskunft, Namensidentität**

- Ein Nutzerprofil auf einer **Plattform für Kleinanzeigen** enthielt den Namen und die (frühere) Anschrift eines Nutzers. Ein namensgleicher Betroffener teilte der Plattform mit, dass er nicht registriert ist und ein Inserat mit seinen Daten missbräuchlich veröffentlicht wurde. Nach abweisender Antwort der Plattform stellte er ein Auskunftersuchen ua unter Angabe seiner Wohnanschrift, die mit der im Profil hinterlegten Adresse übereinstimmte. Die Plattform prüfte die Zuordnung des Inserats und der Nutzerdaten und erteilte dem Vertreter des Betroffenen Auskunft zum betreffenden Nutzerprofil. Der Nutzer erhob Datenschutzbeschwerde wegen Verletzung des Rechts auf Geheimhaltung, die von der DSB abgewiesen wurde.

Die DSB hat erwogen: Der Nutzer hat sein Profil 2020 angelegt. Seine hinterlegte Anschrift war seit Juni 2023 nicht mehr aktuell. Die im Profil hinterlegte Adresse war zum Zeitpunkt des Auskunftersuchens dem namensgleichen Betroffenen zuzuordnen.

Die **Datenverarbeitung zur Auskunftserteilung** beruht auf der **Erfüllung einer rechtlichen Verpflichtung** nach Art 6 Abs 1 lit c, 12 Abs 3 und Art 15 DSGVO, die den Verantwortlichen verpflichten, Auskunftersuchen fristgerecht zu bearbeiten. Es ist ein wirksames Auskunftersuchen gestellt worden. Die Identität des Betroffenen war durch Vorlage einer Ausweiskopie und Adressübereinstimmung hinreichend belegt. Daten, die im Zuge eines **Identitätsdiebstahls** erhoben wurden, verbleiben dennoch personenbezogene Daten des Opfers, was einschlägige EDSA-Leitlinien bestätigen (EDSA Leitlinien 01/2020, Rz 104, 107). Die Plattform durfte anhand der Aktenlage von der **rechtswidrigen Verwendung** der Daten des Betroffenen durch den Nutzer ausgehen und Auskunft erteilen. Eine vorherige Kontaktaufnahme mit dem Nutzer war nicht geboten. Die Auskunftserteilung war erforderlich und verhältnismäßig, eine zweckwidrige Weiterverwendung der Daten des Nutzers ist nicht erfolgt.

DSB 11.09.2025, 2023-0.643.180

### **Rollenverteilung, Übermaßverbot, behördeninterne Datenweitergabe, Förderung**

- Die Obfrau eines Tierschutzvereins beantragte beim Amt der Stmk Landesregierung eine Förderung für ein Projekt. Die zuständige Sachbearbeiterin fragte im Zuge der Amtshilfe gemäß Art 22 B-VG bei der zuständigen Bezirkshauptmannschaft (**BH**) nach, ob verwaltungsstrafrechtliche Verstöße nach dem Tierschutzgesetz von der Obfrau anhängig sind oder Strafen verhängt wurden. Die BH übermittelte daraufhin einen Auszug der verhängten Verwaltungsstrafen. Die Obfrau erachtete diese Datenübermittlung als unzulässig, zumal nicht sie Förderwerberin ist, sondern der von ihr vertretene Verein und die Förderrichtlinie, die der Datenübermittlung zugrunde lag, nicht veröffentlicht war. Sie brachte Datenschutzbeschwerde wegen der Verletzung ihres Rechts auf Geheimhaltung gegen zwei Mitarbeiter der BH bei der DSB ein. Die DSB wies die Datenschutzbeschwerde ab.

Die DSB hat erwogen: Die Verarbeitung personenbezogener Daten durch eine natürliche Person bei der Ausübung ihrer beruflichen Tätigkeit wird dem **Arbeitgeber als Verantwortlichen zugerechnet**. Einzelne Mitarbeiter sind nur für die Verarbeitung verantwortlich, wenn sie aus reinem

privaten Interesse oder persönlichen Motiven handeln.

Das **Übermaßverbot** beschränkt die Zuständigkeit der DSB auf die Prüfung der denkmöglichen Zulässigkeit von Datenermittlungen durch eine Verwaltungsbehörde im Verwaltungsverfahren.

Eine vorgesetzte Verwaltungsbehörde kann nach Art 20 Abs 1 B-VG **Weisungen** an untergeordnete Organe erteilen. Dafür braucht es keine gesonderte gesetzliche Grundlage. Die Weisung kann formfrei, somit auch mündlich, schriftlich oder schlüssig erfolgen. Eine **nicht veröffentlichte** Förderrichtlinie kann so eine **Weisung** sein. Untergeordnete Verwaltungsorgane haben sich an eine entsprechende Weisung zu halten. Die Förderrichtlinie stellt auf Förderwerber oder handlungsbefugte Organe von Förderwerbern ab. Somit ist auch die Obfrau des Tierschutzvereins umfasst. Eine **behördeninterne Datenweitergabe** ist zudem keine Offenlegung iSd DSGVO.

Die Information über **verwaltungsstrafrechtliche Vormerkungen** ist iZm der Vergabe von Förderungen nach dem TierschutzG von Relevanz. Nach der Förderrichtlinie darf keine Förderung ausbezahlt werden, wenn eine Verwaltungsübertretung nach § 38 TierschutzG vorliegt. Nach Art 6 Abs 1 lit e DSGVO ist die Verarbeitung von personenbezogenen Daten rechtmäßig, wenn diese für die Wahrnehmung einer Aufgabe, die im **öffentlichen Interesse** liegt, erforderlich ist. Die **Förderungsvergabe** ist eine Aufgabe im **öffentlichen Interesse**.

### Aus der weiteren Rechtsprechung der DSB:

- Bei einer **Videoüberwachung** zum Schutz des Eigentums im privaten Bereich ist eine Einbeziehung **öffentlicher Flächen** im Ausmaß von **maximal 50 cm** zulässig, wenn der Schutzzweck der Videoüberwachung sonst nicht erfüllt werden kann. Ist ein **Privatgrund** eindeutig als solcher **gekennzeichnet** und begibt sich der **Kfz-Fahrer zum Wenden** dennoch in diesen Bereich (**Besitzstörung**), ist die Videoüberwachung angemessen. Der Fahrer, der bewusst ein Verbot ignorierte, kann sich auch nicht darauf berufen, dass er sein Verhalten nicht gesetzt hätte, wenn er von der – gut sichtbaren – Videoüberwachung informiert worden wäre ([DSB 12.09.2025, 2024-0.739.833](#)).
- Das Schreiben des Betroffenen war ein **Auskunftersuchen**, gelangte in den **Machtbereich** des Verantwortlichen und wurde **verspätet** beantwortet. Unerheblich ist die unrichtige **interne Zuordnung** des Auskunftersuchens. Es gibt jedoch kein subjektives Recht auf Feststellung der verspäteten Erteilung einer Auskunft.

Verarbeitet der Verantwortliche zum Zeitpunkt des Einlangens des Auskunftersuchens keine personenbezogenen Daten zu einer Person, ist eine **Negativauskunft** zu erteilen. Die im Auskunftersuchen und im Identitätsnachweis erhaltenen Daten sind vom Auskunftsrecht (noch) nicht umfasst, weil sie zum maßgeblichen Zeitpunkt noch nicht verarbeitet wurden. Über bereits **gelöschte Daten** besteht keine inhaltliche Auskunftspflicht. Ebenso wenig besteht eine Verpflichtung zum Speichern von **Löschprotokollen**. Über **mündlich "vorhandene" Daten** ist keine Auskunft geschuldet. Das Auskunftsrecht ist auch **kein allgemeines Fragerecht** ([DSB 17.09.2025, 2025-0.502.649](#)).

to the point

# Datenschutzmonitor. 49/2025 vom 11.12.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das **Datenschutzrecht**, das **Digitalisierungsrecht** sowie das **IFG** schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

Abonnieren Sie auch unsere anderen periodischen Newsletter, **Digital Law Monitor**, **Technology & Digitalisation**, **Financial Regulation**, **Healthcare & Life Sciences** sowie **White Collar Crime** für regelmäßige, prägnante Updates [hier](#).

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH/EuG**

EuGH 02.12.2025, C-492/23, *Russmedia Digital* (DSA, Haftungsprivileg, Verantwortlicheneigenschaft)

EuG 03.12.2025, T-318/24, *WS/Kommission* (Auskunft, Mitarbeiter, Dokument, Empfänger, Protokollierung)

EuGH 02.12.2025, C-34/24, *Stichting Right to Consumer Justice* (Online-Plattform, Verbandsklage, Gerichtsstand)

- **Rechtsprechung der Justiz**

OGH 11.11.2025, 10b155/25p (Videoüberwachung, Servitut, Interessenabwägung)

- **Rechtsprechung des BVwG**

BVwG 23.10.2025, W101 2268654-1 (Auskunft, Beweislast, Geschäftsgeheimnis)

BVwG 07.10.2025, W292 2285608-1 (Auskunft, grenzüberschreitende Verarbeitung, Eizellenspende)

BVwG 23.10.2025, W176 2288880-1 (Firmendaten, öffentlich zugängliche Daten, Interessenabwägung)

BVwG 25.09.2025, W252 2289069-1 (Rechtsanwalt, Rechtsanspruch, Interessenabwägung)

BVwG 25.09.2025, W252 2292573-1 (Disziplinaranzeige, Rechtsgrundlage)

BVwG 14.10.2025, W137 2236019-1 (Datenrichtigkeit, Datenwillinge)

BVwG 06.10.2025, W256 2278150-1 (Gutachten, subjektive Meinung, Berichtigung)

BVwG 10.09.2025, W137 2297602-2 (Bundesheer, dienstliche Weisung)

BVwG 01.10.2025, W170 2314010-1 (Disziplinarerkenntnis, dienstliche Weisung, Datenbankzugriff)

BVwG 05.09.2025, W256 2255025-1 (Personenbezug, Impfstatus)

BVwG 04.09.2025, W252 2287329-1 (Mandatsbescheid, Gefahr im Verzug)

BVwG 16.09.2025, W292 2273455-1 (Mutwillensstrafe, Rechtsmissbrauch)

BVwG 07.10.2025, W137 2307782-1 (Akteneinsicht, Interessenabwägung)

BVwG 08.09.2025, W605 2309836-1 (Auskunftspflichtgesetz, Akteneinsicht)

- **Rechtsprechung des LVwG**

LVwG Vorarlberg 09.10.2025, LVwG-352-2/2025-R12 (Informationsbegehren, public watchdog, politische Meinung, Standort)

LVwG Kärnten 13.11.2025, KLVwG-1828/5/2025 (IFG, innergemeindlicher Instanzenzug, keine Aufzeichnung)

LVwG Kärnten 06.11.2025, KLVwG-1830/5/2025 (IFG, Wirkungsbereich, keine Aufzeichnung)

- **Rechtsprechung der DSB**

DSB 25.09.2025, 2025-0.355.103 (automatisierte Entscheidung, Scoring, Auskunft, Energieversorger)

DSB 18.11.2025, 2025-0.902.556 (Geldstrafe, Erforderlichkeit, Verschulden)

DSB 24.09.2025, 2025-0.533.437 (Rechtsanwalt, Rolle, Verarbeitungsvorgänge)

DSB 24.09.2025, 2025-0.757.118 (Videotürklingel, berechtigtes Interesse, digitaler Spion)

DSB 23.09.2025, 2025-0.746.088 (Typo, falsche E-Mail-Adresse)

DSB 19.09.2025, 2025-0.470.791 (Personenbezug, Identifizierbarkeit, Offenlegung)

DSB 31.07.2024, 2023-0.521.417 (irrtümliche Datenerhebung, Datenübermittlung)

- **EU-Rechtsakte**

Entwurf der DurchführungsVO zu KI-Reallaboren

Entwurf der DurchführungsVO zu europäische Briefschaften für die Digitale Identität

EDSA, draft Recommendations 2/2025 on e-commerce Websites

- **Nationale Rechtsakte**

Vbg: Novelle des Gesetzes über landesspezifische Regelungen zum Datenschutz

## To the Point:

### Rechtsprechung des EuGH

EuGH 02.12.2025, C-492/23, *Russmedia Digital*

#### **DSA, Haftungsprivileg, Verantwortlicheneigenschaft**

- Ein Nutzer veröffentlichte auf einer rumänischen Online-Plattform eine Anzeige, in der sensible personenbezogene Daten einer Betroffenen verarbeitet wurden. Die Betroffene klagte ua auf immateriellen Schadenersatz gemäß Art 82 DSGVO. Dem EuGH wurden Fragen zum Verhältnis des Haftungsprivilegs des DSA zur Verantwortlicheneigenschaft der DSGVO vorgelegt.

Der EuGH hat erwogen: Der Betreiber einer **Online-Plattform** unterliegt als **Vermittlungsdiensteanbieter** dem **DSA**. Legt er die Parameter für die Verbreitung der Anzeigen anhand des Zielpublikums und der Einzelheiten der Veröffentlichung fest (zB Darstellung, Dauer, Rubriken, Ranking), wirkt er an der Festlegung der wesentlichen **Mittel** der Verarbeitung mit. Dadurch nimmt er maßgeblich Einfluss auf die weltweite Verbreitung dieser Daten. Verarbeitet er die Daten zudem für eigene Zwecke (zB Werbung und andere kommerzielle Zwecke), legt er auch den Zweck der Verarbeitung fest und ist daher **(Mit-)Verantwortlicher** für diese Datenverarbeitung. Ihm obliegt daher die Einhaltung der Grundsätze des Art 5 und der Art 24 f DSGVO.

Der Vermittlungsdiensteanbieter hat mittels geeigneter **technischer und organisatorischer Maßnahmen** (i) sicherzustellen, dass Anzeigen, die **sensible Daten** iSd Art 9 DSGVO enthalten, identifiziert werden und (ii) zu prüfen, ob der inserierende Nutzer zugleich jene Person ist, deren sensible Daten in der Anzeige enthalten sind. Ist dies nicht der Fall und kann der inserierende Nutzer keine Einwilligung der Betroffenen oder eine andere Rechtsgrundlage nachweisen, hat der Vermittlungsdiensteanbieter die Veröffentlichung der Anzeige zu **verweigern**. Außerdem hat er alle nach dem **Stand der Technik** verfügbaren technischen Maßnahmen in Betracht zu ziehen, um die **Kopie und Replikation des Online-Inhalts** zu **blockieren**. In einer solchen Konstellation kann sich der Vermittlungsdiensteanbieter nicht auf das Haftungsprivileg des DSA berufen.

Aus der weiteren Rechtsprechung des EuGH/EuG:

- Das **Auskunftsrecht** bezieht sich nicht auf **Dokumente**, sondern nur auf Daten, die in einem Dokument enthalten sind. Die **Mitarbeiter** eines Verantwortlichen sind **keine Empfänger** iSd Datenschutzrechts. Selbst wenn eine Auskunft über konkrete

Mitarbeiter erforderlich ist, um dem Betroffenen die Ausübung seiner Datenschutzrechte zu ermöglichen, würde eine entsprechende Auskunft in die Rechte dieser Mitarbeiter eingreifen. Verantwortliche sind nicht verpflichtet, eine **Protokollierung** vorzusehen, die Informationen über die Identität der Mitarbeiter erfasst. Es gibt auch kein Betroffenenrecht auf die **Wiederherstellung** gelöschter Daten (EuG 03.12.2025, T-318/24, *WS/Kommission*).

- Ist der Markt eines Mitgliedstaats angeblich von der **Verwirklichung wettbewerbswidriger Verhaltensweisen** betroffen, die darin bestehen, dass der Betreiber einer **Online-Plattform**, die auf alle in diesem Mitgliedstaat wohnenden Nutzer ausgerichtet ist, eine überhöhte Provision auf den Preis der auf dieser Plattform zum Verkauf angebotenen **Apps** und der in diesen Apps integrierten **digitalen Produkte** erhebt, ist das **sachlich zuständige Gericht** dieses Mitgliedstaats für die Entscheidung über **Verbandsklagen** **zuständig** (EuGH 02.12.2025, C-34/24, *Stichting Right to Consumer Justice*).

### Rechtsprechung der Justiz

Aus der Rechtsprechung der Justiz:

- Eine **Videoüberwachung** des eigenen Grundstücks ist grundsätzlich zulässig, wenn keine Nutzungsrechte Dritter bestehen. Die Videoüberwachung des **Servitutsbereichs** kann nicht mit dem allgemeinen Interesse an der **Kontrolle des Eigentums** gerechtfertigt werden. Ein Eingriff in den **höchstpersönlichen Lebensbereich** ist einer Interessenabwägung regelmäßig nicht zugänglich. Dass der Servitutsberechtigte zur Kontrolle einer **schonenden Ausübung** der Dienstbarkeit mit Beobachtung durch den Eigentümer rechnen muss, kann eine Videoüberwachung aufgrund der unterschiedlichen **Beobachtungsintensität** nicht rechtfertigen und ist nicht unbedingt erforderlich. Ein berechtigtes Interesse an der Videoüberwachung zur **persönlichen Sicherheit** besteht nicht, wenn keine **konkrete Bedrohung** durch den Servitutsberechtigten vorliegt und verbale Konflikte vom Eigentümer ausgingen. Ein behauptetes Interesse an der Beobachtung von Wildtieren rechtfertigt die Videoüberwachung nicht, wenn der **tatsächliche Zweck** die Aufzeichnung des Servitutsberechtigten ist (OGH 11.11.2025, 10b155/25p).

### Rechtsprechung des BVwG

BVwG 23.10.2025, W101 2268654-1

#### **Auskunft, Beweislast, Geschäftsgeheimnis**

- Ein ehemaliger Mitarbeiter, der zugleich Kunde seines früheren Arbeitgebers war,

richtete an diesen ein Auskunftersuchen. Da die erteilte Auskunft kaum E-Mails, Termineinträge, Protokolle, Präsentationsunterlagen oder Organigramme enthielt, erachtete der ehemalige Mitarbeiter sie als unvollständig, sodass er Datenschutzbeschwerde bei der DSB erhob. Der ehemalige Arbeitgeber begründete die fehlenden Unterlagen mit dem Schutz von Betriebs- und Geschäftsgeheimnissen. Die DSB wies die Datenschutzbeschwerde ab. Dagegen erhob der ehemalige Mitarbeiter (erfolglos) Beschwerde an das BVwG.

Das BVwG hat erwogen: Gemäß Art 15 DSGVO hat jede betroffene Person das Recht zu erfahren, ob und welche personenbezogenen Daten verarbeitet werden. Die Auskunft bezieht sich auf den **Zeitpunkt der Antragstellung**, sodass bereits gelöschte Daten nicht zu beauskunften sind. Dem Betroffenen sind alle ihn direkt oder indirekt betreffenden personenbezogenen Daten mitzuteilen, unabhängig davon, ob und wie diese mit seinem Namen oder einem Kürzel verbunden sind.

Die **Beweislast** für die Verarbeitung personenbezogener Daten des Betroffenen durch den Verantwortlichen liegt beim Betroffenen. Wird die **Unvollständigkeit** der Auskunft eingewandt, muss im Beschwerdeverfahren **konkret vorgebracht** werden, warum dies so ist. Die **bloße Vermutung** oder **hypothetische Argumentation** einer unvollständigen Auskunft aufgrund eines unzureichenden Suchverfahrens genügt nicht. Bei der Beantwortung des Auskunftersuchens trägt der **Verantwortliche die Behauptungs- und Beweislast** für die **positive Erledigung**.

Berührt eine Auskunft die Interessen Dritter, ist eine **Interessenabwägung** iSd Art 6 Abs 1 lit f bzw lit g DSGVO durchzuführen. Die Auskunft darf nur dann erteilt werden, wenn die Gründe für die Beauskunftung jene für die Geheimhaltung überwiegen. Das Durchsuchen aller Mitarbeiter-Mail-Postfächer nach Nachrichten oder Termineinträgen eines Betroffenen widerspricht einerseits dem **Erforderlichkeitsgrundsatz** des Art 5 DSGVO, andererseits überwiegt das Recht auf Geheimhaltung der betroffenen Mitarbeiter. Darüber hinaus sieht Art 15 Abs 3 DSGVO kein eigenständiges Recht auf Übermittlung einer **Datenkopie** vor und darf der Verantwortliche dem Antrag des Betroffenen nur insoweit entsprechen, als die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden.

Ein **Geschäftsgeheimnis**, wie etwa Dokumente, die die **Berechnung der Wirtschaftlichkeit eines Investitionsvorhabens** beinhalten, ist eine Information, die geheim ist, weil sie weder allgemein bekannt noch ohne Weiteres zugänglich ist, von kommerziellem Wert ist und

Gegenstand angemessener Geheimhaltungsmaßnahmen und daher **nicht zu beauskunften** ist.

BVwG 07.10.2025, W292 2285608-1

### **Auskunft, grenzüberschreitende Verarbeitung, Eizellenspende**

- Eine Minderjährige, die in einer tschechischen Kinderwunschlinik mit dem Samen ihres Vaters und einer anonymen **Eizellenspende** gezeugt wurde, richtete ein Auskunftersuchen betreffend den Namen und die Anschrift der Eizellenspenderin an die Kinderwunschlinik. Die Kinderwunschlinik verweigerte die Offenlegung, woraufhin die Minderjährige – vertreten durch ihre Mutter – Datenschutzbeschwerde erhob. Die DSB leitete über das IMI-System ein Verfahren zur Bestimmung der federführenden Aufsichtsbehörde nach Art 56 DSGVO ein. Die tschechische Aufsichtsbehörde übermittelte der DSB einen abweisenden Beschlusssentwurf, weil tschechisches Recht einer Beauskunftung der Identität von Samenspendern entgegensteht. Auch die DSB wies die Datenschutzbeschwerde ab. Dagegen erhob die Minderjährige eine (erfolglose) Beschwerde an das BVwG.

Das BVwG hat erwogen: Es liegt eine **grenzüberschreitende Verarbeitung** iSd Art 4 Z 23 lit b DSGVO vor, weil die Kinderwunschlinik in der **EU niedergelassen** ist und die Verarbeitung **erhebliche Auswirkungen** auf Betroffene in mehr als einem Mitgliedstaat haben kann, da potenzielle Kunden und Spender aus mehreren Mitgliedstaaten stammen können. Die Kinderwunschlinik hat ihren Sitz nur in einem Mitgliedstaat, dies spricht jedoch nicht automatisch gegen eine grenzüberschreitende Verarbeitung.

Die **Zuständigkeit der federführenden Aufsichtsbehörde** richtet sich nach der **Hauptniederlassung des Verantwortlichen**, sodass sich die federführende Zuständigkeit der tschechischen Aufsichtsbehörde ergab. Da die DSB keinen **Einspruch** gegen den Beschluss der tschechischen Aufsichtsbehörde erhob, trat **Bindungswirkung** ein. Ein **effektiver Rechtsschutz** bleibt jedoch gewahrt, weil die Minderjährige der DSB ihr Vorbringen erstatten konnte und der Bescheid im Inland bekämpfbar ist.

Angaben zur Eizellenspenderin sind **keine personenbezogenen Daten** der Minderjährigen. Die unionsrechtlichen Vorgaben zum **Transplantationsrecht** erlauben eine Ausgestaltung mit **Anonymitätsprinzip**. Die tschechischen Rechtsvorschriften setzen diese Vorgaben um, sodass die **Anonymität der Eizellenspenderin** aufrechterhalten war. Auch der Hinweis auf genetische Nähe ändert daran nichts, weil keine

zwei Personen identische **genetische Daten** aufweisen können. Die Minderjährige kann sich daher nicht auf Art 15 DSGVO stützen, um Informationen über eine dritte Person zu erhalten.

BVwG 23.10.2025, W176 2288880-1

### **Firmendaten, öffentlich zugängliche Daten, Interessenabwägung**

- Im Rahmen eines **Inkassoverfahrens** gegen einen Betroffenen legte das beauftragte Inkassobüro die Firmendaten eines Einzelunternehmens offen, dessen Geschäftsanschrift seiner Privatadresse entsprach. Der Betroffene erachtete sich dadurch in seinem Recht auf Geheimhaltung verletzt und erhob Datenschutzbeschwerde bei der DSB, die dieser stattgab. Das Inkassobüro erhob (erfolgreich) Bescheidbeschwerde an das BVwG.

Das BVwG hat erwogen: Die **Firmenbezeichnung** eines eingetragenen Einzelunternehmens ist ein **personenbezogenes Datum**. Auch **öffentlich zugängliche Daten** fallen in den **Anwendungsbereich** der DSGVO. Einschränkungen des Geheimhaltungsanspruchs sind nur aufgrund einer **einzelfallbezogenen Interessenabwägung** möglich.

Eine Verarbeitung ist nach Art 6 Abs 1 lit f DSGVO zulässig, wenn sie zur Wahrung berechtigter Interessen erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Die **Forderungsbetreibung** ist ein solches berechtigtes Interesse. Da unklar war, ob ein **Privatgeschäft** vorlag oder nicht, lag es aufgrund der **Unterschiede** zwischen **einseitig und beidseitig unternehmensbezogenen Geschäften** im berechtigten Interesse des Gläubigers, zu erfahren, dass an der Adresse des Betroffenen ein Einzelunternehmen betrieben wird. Die Offenlegung der Firmenbezeichnung durch das Inkassobüro diente dieser rechtlichen Einordnung und war angemessen, erforderlich und auf das notwendige Maß beschränkt. Zudem musste der Betroffene damit rechnen, dass bei Zahlungsverzug ein Inkassobüro eingeschaltet wird und dieses offenlegt, dass an der Rechnungsadresse ein Einzelunternehmen geführt wird.

Die Beeinträchtigung war überdies gering, weil die Angaben im Firmenbuch und auf der Webseite des Einzelunternehmens **öffentlich zugänglich** waren und somit eine **geringere Schutzwürdigkeit** aufwiesen. Ein bloß **hypothetisches Risiko auf Rufschädigung** begründet kein überwiegendes Geheimhaltungsinteresse. Da nur die Firmenbezeichnung offengelegt wurde, wurde der Grundsatz der Datenminimierung

eingehalten. Die Verarbeitung war daher rechtmäßig.

Aus der weiteren Rechtsprechung des BVwG:

- Die Übermittlung personenbezogener Daten durch einen Rechtsanwalt im Rahmen einer **außerordentlichen Revision an den VwGH** ist nach Art 6 Abs 1 lit f DSGVO zulässig. Der **Rechtsanwalt** ist dabei **Verantwortlicher** iSd Art 4 Z 7 DSGVO. Die **Erforderlichkeit** ist **weit auszulegen**. Vorgebrachte Informationen sind nicht bereits deshalb überschießend, weil das Gericht sie für unerheblich erachtet oder sich auf andere Informationen stützt. Maßgeblich ist, dass der Verantwortliche vorab **abstrakt einschätzen** kann, ob die Daten dem **Gericht dienlich** sein können. Im Rahmen der gebotenen **Interessenabwägung** kommt dem **Recht auf ein faires Verfahren** und der **effektiven Rechtsdurchsetzung** besonderes Gewicht zu. Angesichts des hohen Gewichts des fairen Verfahrens und der **anwaltlichen Verschwiegenheitspflicht** überwiegt regelmäßig das Interesse an effektiver Rechtsdurchsetzung, sofern keine offensichtlich überschießende Datenübermittlung vorliegt ([BVwG 25.09.2025, W252 2289069-1](#)).
- Eine auf Art 9 Abs 2 DSGVO gestützte Verarbeitung sensibler Daten ist nur dann rechtmäßig, wenn sie **neben den Anforderungen des Art 9 Abs 2 DSGVO** auch mindestens eine der in **Art 6 Abs 1 DSGVO** genannten **Rechtmäßigkeitsvoraussetzungen** erfüllt. Die Verarbeitung besonderer Kategorien personenbezogener Daten zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen** ist rechtmäßig, wenn die Betroffene selbst eine **Disziplinaranzeige samt Beweisurkunden** bei der zuständigen Stelle einbringt und die Verarbeitung zur Beurteilung der Disziplinaranzeige **erforderlich** ist ([BVwG 25.09.2025, W252 2292573-1](#)).
- Der **Grundsatz der Datenrichtigkeit** (Art 5 Abs 1 lit d und Abs 2 DSGVO) verpflichtet Verantwortliche, personenbezogene Daten "*sachlich richtig und erforderlichenfalls auf dem neuesten Stand*" zu halten. Sachlich richtig sind Daten, wenn sie der Realität entsprechen, wobei der **Verarbeitungszweck** den **maßgeblichen Beurteilungsmaßstab** bildet. **Hinweisen** auf eine mögliche Unrichtigkeit – etwa aufgrund eines Löschersuchens – muss **nachgegangen** werden. Aus dem Grundsatz der Datenrichtigkeit ergibt sich daher auch die Pflicht, **angemessene technische und organisatorische Maßnahmen** zu treffen, um die Datenrichtigkeit sicherzustellen. Umfang und Intensität dieser Maßnahmen richten sich nach dem Grundsatz der **Verhältnismäßigkeit** unter Berücksichtigung

des Prüfungsaufwands, Verarbeitungszwecks und Verarbeitungsrisikos unrichtiger Daten für die Betroffene. Eine **jederzeitige Datenrichtigkeit** ist **nicht erforderlich**. Aus Gründen der praktischen Umsetzbarkeit sind **Aktualisierungsfrequenz** und **Aufwand** auf ein **zumutbares Maß** zu beschränken. Verarbeitet die Verantwortliche umfangreiche Datensätze zu (theoretisch) allen Einwohnern Österreichs, ist ihr die damit einhergehende Problematik von "**Datenzwilligen**" bekannt, sodass spätestens nach der erfolgten Anzeige der Betroffenen eine **erweiterte Überprüfung** hätte stattfinden müssen ([BVwG 14.10.2025, W137 2236019-1](#)).

- Auf Tatsachenangaben beruhende Schlussfolgerungen eines Sachverständigen im Rahmen eines Gutachtens sind die **subjektive Meinung** eines Gutachters, deren Richtigkeit oder Unrichtigkeit sich einer **Tatsachenüberprüfung entzieht** und somit **keiner Berichtigung** iSd Art 16 DSGVO **zugänglich** ist. Die "Richtigstellung" einer gutachterlichen Meinung im Sinne einer Anpassung an eine andere, ebenso subjektive Meinung kann nicht Gegenstand einer auf Art 16 DSGVO gestützten Datenschutzbeschwerde sein ([BVwG 06.10.2025, W256 2278150-1](#)).
- Das Speichern und Ordnen von E-Mails eines vom Dienst enthobenen Bundesheerobersts aufgrund einer **dienstlichen Weisung** fällt nicht in den Bereich der **Wahrung der nationalen Sicherheit** und unterliegt daher der **DSGVO**. Ein Beamter, der vorübergehend einer anderen Dienststelle zugeteilt ist, wird gemäß § 39 BDG nicht automatisch von seinen für die vorige Dienststelle ausgeführten Aufgaben entbunden. Dienstliche Aufgaben können mit einer Weisung nach § 43 BDG konkretisiert werden. Handelt ein Beamter auf Grundlage einer solchen Weisung, liegt **keine rechtswidrige Offenlegung** bzw **kein rechtswidriger Zugriff** vor und war die Datenverarbeitung **rechtmäßig** ([BVwG 10.09.2025, W137 2297602-2](#)).
- Eine **dienstlich veranlasste Datenschutzbelehrung** ist als **Weisung** zu verstehen. Verbietet das in der Datenschutzbelehrung normierte "**need-to-know-Prinzip**" den Zugriff auf personenbezogene Daten in dienstlichen Datenbanken (wie PERSIS), rechtfertigt die **Beweissicherung** für eine vom Beamten selbst eingebrachte Beschwerde nicht den Zugriff, weil deren Bearbeitung nicht seine **dienstliche Aufgabe** war. Ein **Rechtsirrtum** ist nur dann rechtfertigend oder entschuldigend, wenn der Betreffende die Richtigkeit seiner Rechtsmeinung durch **Nachfrage** bei der Behörde überprüft hat. Unterlässt der Beamte diese Nachfrage trotz **eindeutigen Wortlauts** der Weisung, liegt **grobe**

**Fahrlässigkeit** vor. Generalpräventiv ist eine strenge Bestrafung geboten, um allen Beamten vor Augen zu führen, dass der **Zugriff auf dienstliche Datenbanken** nicht für private Anliegen genutzt werden darf, auch nicht mit dem **Einverständnis** des von der Abfrage Betroffenen ([BVwG 01.10.2025, W170 2314010-1](#)).

- Der **Personenbezug** setzt ein **materielles Element** voraus, also dass Angaben über einen Betroffenen gemacht werden. Die Tatsache, dass ein Arbeitnehmer anstelle eines Impfnachweises täglich einen negativen PCR-Test als Nachweis einer geringen epidemiologischen Gefahr vorlegt, lässt **keine zwingenden Rückschlüsse** auf dessen **Impfstatus** zu, wenn die Rechtsvorschriften die Bekanntgabe einer Impfung nicht zwingend vorschreiben, sondern als **gleichwertige Möglichkeit** eines Nachweises vorsehen. Eine (indirekte) Offenlegung und damit eine Verletzung im Recht auf Geheimhaltung liegt nicht vor ([BVwG 05.09.2025, W256 2255025-1](#)).
- Die Erlassung eines **Mandatsbescheids** gemäß § 22 Abs 4 DSG iVm § 57 Abs 1 AVG zur Untersagung der Weiterführung einer Datenverarbeitung setzt eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen voraus (**Gefahr im Verzug**). Eine solche liegt nicht vor, wenn die behaupteten Datenschutzverletzungen zum **Zeitpunkt der Antragstellung** bereits **mehrere Monate zurückliegen** und **keine konkreten Anhaltspunkte** für eine gegenwärtige oder künftige Gefährdung bestehen. Das Vorliegen der Gefahr im Verzug muss mit **einzel-fallbezogenen Tatsachen** begründet werden. Reine **Spekulationen, hypothetische Erwägungen, allgemeine Besorgnis** hinsichtlich zukünftiger oder lediglich auf Alltagserfahrung gestützte, fallunabhängige Vermutungen **genügen nicht** ([BVwG 04.09.2025, W252 2287329-1](#)).
- Dem Beschwerdeführer wurde eine **Mutwillensstrafe** von EUR 700 auferlegt, weil er seit 2018 insgesamt **341 Datenschutzbeschwerden** bei der DSB eingereicht hatte und im konkreten Verfahren eine **137-seitige Datenschutzbeschwerde** sowie im Rahmen seiner Bescheidbeschwerde **76 Schriftsätze samt Beilagen** vorlegte. Durch diese überwiegend **unstrukturierten, grund- und aussichtslosen Eingaben** wurde das BVwG **wiederholt** belastet. Sein Antrag, das BVwG möge die DSB verpflichten, ihm eine **detaillierte Aufstellung aller protokollierten Verfahren** zu übermitteln, zeigt, dass der Beschwerdeführer aus bloßer **Freude an der Behelligung** des Gerichts und damit **mutwillig** handelt, zumal die Aussichtslosigkeit weiterer Eingaben für jedermann erkennbar ist. Sein Verhalten ist daher als **offenkundig**



**rechtsmissbräuchlich** zu werten ([BVwG 16.09.2025, W292 2273455-1](#)).

- Ein Antrag, medizinische Gutachten und Dokumente vollständig von der **Akteneinsicht** auszunehmen, ist überschießend, wenn diese das **zentrale Element des Ordnungsstrafverfahrens** bilden. **Datenschutzrechtlich sensible, aber** für den Verfahrensgegenstand **irrelevante Passagen** (zB Vorgeschichte oder Anamnese) sind im Rahmen einer **Interessenabwägung** ohnehin durch das Gericht von der Akteneinsicht auszunehmen ([BVwG 07.10.2025, W137 2307782-1](#)).
- Die Erlassung eines **antragsbedürftigen Bescheids** nach § 4 AuskunftspflichtG von Amts wegen **ohne** einen eindeutigen diesbezüglichen **Antrag** belastet den Bescheid mit **Rechtswidrigkeit**. Das AuskunftspflichtG ist nicht geeignet, um eine **Akteneinsicht** nach § 17 AVG durchzusetzen, weil die Auskunftserteilung nach dem Auskunftspflichtgesetz nicht die Gewährung der im AVG geregelten Akteneinsicht bedeutet ([BVwG 08.09.2025, W605 2309836-1](#)).

### Rechtsprechung der LVwG

LVwG Vorarlberg 09.10.2025, LVwG-352-2/2025-R12

#### **Informationsbegehren, public watchdog, politische Meinung, Standort**

- Ein Journalist beantragte per E-Mail die Übermittlung der gemäß § 1c Abs 2 Parteienförderungsgesetz (PFG) zu führenden PDF-Dateien mit den genauen Standorten der Wahlplakate für die Vorarlberger Landtagswahl 2024. Die Landespressestelle Vorarlberg lehnte dies aus Datenschutzgründen ab. Nach dem Antrag des Journalisten auf bescheidmäßige Erledigung lehnte die Vorarlberger Landesregierung das Auskunftsbegehren mittels Bescheid ab. Der Journalist erhob (erfolglos) Bescheidbeschwerde an das LVwG Vorarlberg und berief sich auf Art 10 EMRK sowie seine Rolle als public watchdog. Die Vorarlberger Landesregierung hielt dem entgegen, dass die Standortdaten personenbezogen seien und Rückschlüsse auf politische Meinungen der Grundstückseigentümer zuließen, womit besondere Kategorien personenbezogener Daten gemäß Art 9 Abs 1 DSGVO betroffen seien.

Das LVwG hat erwogen: Die **Standorte von Wahlplakaten** und die darin enthaltenen **Adressen** sind **personenbezogene Daten**. Sie fallen zudem unter **besondere Kategorien personenbezogener Daten** iSd Art 9 DSGVO, weil sich daraus **politische Meinungen** der Grundstückseigentümer ableiten lassen. Bereits die Möglichkeit einer ableitbaren politischen Meinung genügt für diese Einstufung. Die Lebenserfahrung

spricht für eine Zustimmung zur Plakataufstellung nur bei zumindest positiver politischer Affinität.

Eine Weitergabe dieser Daten bedarf einer **Rechtfertigung**. Die in Art 9 Abs 2 DSGVO normierten Ausnahmen greifen jedoch nicht. Die Daten sind **nicht offensichtlich öffentlich gemacht** iSd Art 9 Abs 2 lit e DSGVO, weil die Grundstückseigentümer weder die Plakate selbst aufgestellt noch die PDF-Dateien iSd § 1c Abs 2 PFG erstellt und an die Landesregierung übermittelt haben. Bloße Sichtbarkeit im öffentlichen Raum begründet keine Öffentlichmachung iSd DSGVO. Auch ein **erhebliches öffentliches Interesse** iSd Art 9 Abs 2 lit g DSGVO liegt nicht vor, weil das Auskunftsgesetz **keine hinreichend bestimmte gesetzliche Grundlage** für die Verarbeitung besonderer Kategorien bietet.

Für den Zugang zu Informationen nach Art 10 EMRK sind der Zweck der Anfrage, die Art der begehrten Information, die Rolle des Antragstellers sowie die Verfügbarkeit der Information maßgeblich. Zwar erfüllt der Journalist die Rolle eines **public watchdog**. Das öffentliche Interesse an den konkreten Standortdaten überwiegt aber nicht das Datenschutzinteresse der Grundstückseigentümer. Die bestehenden **Kontrollmechanismen** nach dem PFG sichern das öffentliche Interesse bereits ausreichend ab.

Auch eine **Teilbeantwortung** scheidet aus, weil der Behörde die Zuordnung der gemeldeten 2.700 Adressen zu natürlichen oder juristischen Personen nicht vorliegt und eine entsprechende **Erhebung** die Erfüllung übriger Aufgaben **wesentlich beeinträchtigen** würde.

#### Aus der weiteren Rechtsprechung der LVwG:

- Die **Bürgermeisterin** einer Gemeinde ist sowohl im **eigenen** als auch im **übertragenen Wirkungsbereich** ein **informationspflichtiges Organ** iSd IFG. Der **innergemeindliche Instanzenzug** im eigenen Wirkungsbereich der Gemeinde ist im Anwendungsbereich des IFG **ausgeschlossen**. Eine Information iSd IFG ist jedoch nur eine **Aufzeichnung**, die in irgendeiner (beliebigen) Form gespeichert wird. In **mündlicher Form** durch persönliche Gespräche oder Telefonate eingeholte Rechtsauskünfte sind **keine Informationen** iSd IFG ([LVwG Kärnten 13.11.2025, KLVwG-1828/5/2025](#)). **Anm: Nähere Informationen zu den Geheimhaltungsgründen des IFG insb iZm privaten Informationspflichtigen finden Sie in der RDB (Paywall): [Cudlik/Petschinka, Ausgewählte Fragen der Geheimhaltung im IFG, ecolex 2025, 847](#).**
- Eine E-Mail betreffend eine Studie über bestimmte **Altlasten** fällt in den **Wirkungsbereich der Bürgermeisterin** der

Gemeinde. Eine solche E-Mail ist grundsätzlich eine **Information** iSd **IFG**. Ist die E-Mail jedoch **nicht mehr vorhanden**, weil sie gelöscht wurde, kann die Information dennoch nicht erteilt werden ([LVwG Kärnten 06.11.2025, KLVwG-1830/5/2025](#)). **Anm: Ist eine Information nicht (mehr) vorhanden, ist im Datenschutzrecht eine Negativauskunft zu erteilen.**

### **Rechtsprechung der DSB**

[DSB 25.09.2025, 2025-0.355.103](#)

#### **Automatisierte Entscheidung, Scoring, Auskunft, Energieversorger**

- Ein Energieversorger lehnte einen Online-Antrag auf Energielieferung wenige Minuten nach einer automatisierten Bonitätsabfrage bei einer Auskunft ab. Grundlage der Entscheidung war ein von der Auskunft automatisiert berechneter Score. Der Betroffene erhob daraufhin Datenschutzbeschwerde, ua wegen einer unzulässigen automatisierten Entscheidung nach Art 22 DSGVO, unzureichender Informationen nach Art 13 und 14 DSGVO sowie mangelhafter Auskünfte nach Art 15 DSGVO. Die DSB gab der Datenschutzbeschwerde gegen die Auskunft überwiegend statt, gegen das Energieunternehmen hingegen nur teilweise.

Die DSB hat erwogen: Der Score wurde von der Auskunft **vollständig automatisiert** berechnet und war **maßgebliche Grundlage** für die Ablehnungsentscheidung des Energieversorgers. Der gesamte **Ablehnungsprozess** beim Energieversorger erfolgte **ohne menschliches Zutun**. Art 22 Abs 1 DSGVO ist daher sowohl auf die Score-Erstellung durch die Auskunft als auch auf die darauf gestützte Entscheidung des Energieversorgers anwendbar.

Die Datenverarbeitung durch den Energieversorger war gemäß Art 22 Abs 2 lit a DSGVO rechtmäßig, weil die **Bonitätsprüfung** zur Entscheidung über den Vertragsabschluss **angesichts monatlich tausender Anträge erforderlich** ist. Zudem standen dem Betroffenen die nach Art 22 Abs 3 DSGVO vorgesehenen Garantien (menschliche Überprüfung, eigene Stellungnahme) faktisch offen. Eine Verletzung des Art 22 DSGVO durch den Energieversorger lag daher nicht vor. Bei der Auskunft hingegen lag kein **Ausnahmetatbestand** des Art 22 Abs 2 DSGVO vor. Die automatisierte Berechnung und Übermittlung des Score-Wertes war daher eine unzulässige automatisierte Entscheidung.

Beide Unternehmen verletzen die erforderlichen **Informationspflichten**. Weder die Auskunft noch der Energieversorger informierten den Betroffenen in ihren Datenschutzerklärungen über das Bestehen einer automatisierten Entscheidungsfindung

sowie über die involvierte Logik, Tragweite und angestrebten Auswirkungen.

#### Aus der weiteren Rechtsprechung der DSB:

- Werden personenbezogene Daten zur Wahrung berechtigter Interessen veröffentlicht, ist auch dann, wenn das berechnete Interesse vorliegt, zu prüfen, ob die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses **erforderlich** ist. Der Beschuldigte hat die gegen ihn eingebrachte Privatanklage eines **Bürgermeisters** veröffentlicht. Der Bürgermeister einer Gemeinde ist eine Person des **öffentlichen Lebens**, weshalb ihm gegenüber ein höheres Maß an (sachlicher) Kritik erlaubt ist. Die Veröffentlichung der **privaten Wohnadresse** sowie des **Geburtsdatums** des Bürgermeisters war dennoch **objektiv** nicht erforderlich. Ein **Ver schulden** liegt bereits dann vor, wenn der Beschuldigte sich über die Rechtswidrigkeit seines Verhaltens **nicht im Unklaren sein konnte**. Dem Beschuldigten musste klar sein, dass es einschlägige Datenschutzvorschriften gibt, denn über die DSGVO wurde bei deren Wirksamwerden im Jahr 2018 breit in der Öffentlichkeit informiert und diskutiert. Die verhängte Geldstrafe iHv EUR 80 erscheint im Lichte des verwirklichten Tatunwerts iVm dem Einkommen und Vermögen des Beschuldigten tat- und schuldangemessen ([DSB 18.11.2025, 2025-0.902.556](#)).
- **Rechtsanwälte** sind **Verantwortliche** iSd DSGVO. Das Erheben personenbezogener Daten des Mandanten beim **Betreiber einer Website** und die anschließende **Offenlegung** dieser Daten in einem **zivilgerichtlichen Verfahren** ist eine **Aneinanderreihung** von Verarbeitungsvorgängen. Diese **Verarbeitungsvorgänge** sind **separat** zu prüfen. Die Datenerhebung ist zur Überprüfung der konkret verarbeiteten Daten auch dann berechtigt, wenn sich herausstellt, dass die vermeintlich widerrechtliche Verwendung des Namens und der Adresse des Mandanten tatsächlich durch eine Person erfolgte, die denselben Namen wie der Mandant hat. Im zivilgerichtlichen Verfahren durften die Daten zur **Geltendmachung von Rechtsansprüchen** des Mandanten offengelegt werden ([DSB 24.09.2025, 2025-0.533.437](#)).
- Zum Schutz des Eigentums, der Gesundheit und des Lebens einer unter Erwachsenenschutz gestellten Person wurde eine **Video Türklingel** mit Aufnahme- und Speicherfunktion installiert. Der Schutz der genannten Rechtsgüter ist ein **berechtigtes Interesse** iSd Art 6 Abs 1 lit f DSGVO. Die Datenverarbeitung war aber nicht in dem Umfang erforderlich, dass der **Zugangsbe reich** zum Haus und somit sämtliche

Nachbarn sowie die Wohnungstür der Betroffenen mitaufgezeichnet werden mussten. Als **gelinderes Mittel** hätte ein "**digitaler Spion**" mit Echtzeitüberwachung ohne Aufnahme und Speicherung von Bild- und Audiodaten angebracht werden dürfen ([DSB 24.09.2025, 2025-0.757.118](#)).

- Das Versenden einer E-Mail infolge eines **Typos** an die **falsche E-Mail-Adresse** ist eine Verletzung des Grundrechts auf Geheimhaltung, weil die Daten des Betroffenen unrechtmäßig offengelegt werden. Auf ein etwaiges Verschulden kommt es nicht an ([DSB 23.09.2025, 2025-0.746.088](#)).
- Kann eine **Person** anhand ihres Vornamens und Benutzernamens von Teilnehmern eines Livestreams **identifiziert** werden, sind diese Informationen als **personenbezogene Daten** zu qualifizieren. Durch die Veröffentlichung im Livestream werden diese Daten **offengelegt** ([DSB 19.09.2025, 2025-0.470.791](#)).
- Erhebt ein Verantwortlicher **irrtümlich** personenbezogene Daten für den Zweck eines **Newsletter-Versands**, ist die Datenverarbeitung rechtswidrig. Aus der Rechtswidrigkeit der **innereuropäischen Verarbeitung** resultiert auch die Rechtswidrigkeit der Übermittlung der personenbezogenen Daten ins **Drittland (USA)** ([DSB 31.07.2024, 2023-0.521.417](#)).

### EU-Rechtsakte

- Am **02.12.2025** wurde der Entwurf der "*Commission Implementing Regulation laying down rules for the application of Regulation (EU) 2024/1689 of the European Parliament and of the Council as regards the establishment, development, implementation, operation and supervision of **AI regulatory sandboxes***", [Ares\(2025\)10569703](#), veröffentlicht. Mit dieser DurchführungsVO wird der Einsatz von **KI-Reallaboren** iSd der [KI-VO](#) näher geregelt.
- Am **02.12.2025** wurde der Entwurf der "*Commission Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards onboarding of users to the **European Digital Identity Wallets** by electronic identification means conforming to assurance level high or by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures where the combination meets the requirements of assurance level high*", [Ares\(2025\)10575642](#), veröffentlicht. Mit dieser DurchführungsVO werden Referenzstandards für die Einbindung der Nutzer in die **europäische Brieftasche für**

**die Digitale Identität** iSd eIDAS-VO festgelegt.

- Am **03.12.2025** nahm der EDSA den Entwurf der "[Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites](#)" an. Der EDSA empfiehlt, die Benutzung von **e-commerce Websites** als "**Gast**" mit wenigen Ausnahmen zu ermöglichen.

### Nationale Rechtsakte

- Am **04.12.2025** wurde das **vorarlbergerische** "*Gesetz über eine Änderung des Gesetzes über **landesspezifische Regelungen zum Datenschutz***", [LGBI 2025/73](#), kundgemacht. Mit dieser Novelle wird die Veröffentlichung von **Förderdaten** und ihre Abfrage in der **Transparenzdatenbank** geregelt.

to the point

# Datenschutzmonitor. 50/2025 vom 17.12.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das **Datenschutzrecht**, das **Digitalisierungsrecht** sowie das **IFG** schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

**Aktuell:** Unser **IFG-Musterpaket** stellen wir Ihnen auf Anfrage gerne zur Verfügung.

Abonnieren Sie auch unsere anderen periodischen Newsletter, **Digital Law Monitor**, **Technology & Digitalisation**, **Financial Regulation**, **Healthcare & Life Sciences** sowie **White Collar Crime** für regelmäßige, prägnante Updates [hier](#).

Wir laden Sie herzlich zum nächsten Termin unserer **Schönherr Tech&Law Academy** über **Incident Response & Cybersecurity** am **21.01.2026** ein. Melden Sie sich [hier](#) an.

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EuGH**

EuGH SA 11.12.2025, C-684/24, *Across Fiduciaria* (AML/CFT, wirtschaftliche Eigentümer, Register)

EuGH SA 11.12.2025, C-468/24, *Netz Niederösterreich* (Smart Meter, Stromnetz, elektronisches Kommunikationsnetz)

- **Rechtsprechung des VwGH**

VwGH 13.11.2025, Ra 2023/04/0271 (vergleichbarer Fall, automatisierte Entscheidung)

VwGH 13.11.2025, Ra 2022/04/0115 (Revisionspunkt, subjektives Recht, Zurückweisung)

- **Rechtsprechung der Justiz**

OLG Innsbruck 18.06.2025, 114Ds1/23f (Disziplinarverfahren, IKT-NV, Ansehen des öffentlichen Dienstes)

- **Rechtsprechung des BVwG**

BVwG 29.07.2025, W605 2251236-1 (Besitzstörung, Tonaufnahme, Beweisnotstand, Haushaltsausnahme)

BVwG 22.10.2025, W254 2316529-1 (SIS, Ausschreibung, erhebliches öffentliches Interesse)

BVwG 20.10.2025, W258 2246973-1 (Mitarbeiter, Gesundheitsdaten, breite Öffentlichkeit)

BVwG 28.08.2025, W298 2280052-1 (Besitzstörung, elektronischer Wachhund, Überwachungsdruck)

BVwG 23.10.2025, W274 2309030-2 (Verfahrenshilfeantrag, Verbesserungsauftrag)

- **Rechtsprechung der DSB**

DSB 29.09.2025, 2025-0.682.666 (Geldstrafe, Dashcam, Kennzeichnung, Verschulden)

DSB 26.09.2025, 2025-0.117.456 (Insolvenzverwalter, justizielle Tätigkeit, Unzuständigkeit)

DSB 25.09.2025, 2025-0.432.701 (Rechtsanwalt, Rolle, Beschwerdegegner)

DSB 29.09.2025, 2025-0.754.485 (SIS, Rückkehrentscheidung, Löschung)

DSB 29.09.2025, 2024-0.501.636 (Verwirkung eines Rechts, Gläubigerschutz, Zuständigkeit)

DSB 01.10.2025, 2025-0.765.344 (Vollmacht, Missbrauch, kein Auskunftersuchen)

- **EU-Rechtsakte**

VO 2025/2518 zur Festlegung zusätzlicher Verfahrensregeln für die DSGVO

- **Nationale Rechtsakte**

Zweites EU-Informationssysteme-Anpassungsgesetz

AVG-Novelle (Großverfahren)

## To the Point:

### Rechtsprechung des EuGH

EuGH SA 11.12.2025, C-684/24, *Across Fiduciaria*

#### **AML/CFT, wirtschaftliche Eigentümer, Register**

- Mehrere italienische Treuhandgesellschaften klagten gegen Maßnahmen, die **AML/CFT-Registerpflichten** zu **wirtschaftlichen Eigentümern** sowie Zugangsrechte zu den Daten im Register für Personen mit "berechtigtem Interesse" auslösten. Der italienische Staatsrat legte dem EuGH Fragen zur Auslegung und Gültigkeit von Art 31 RL 2015/849 (idF RL 2018/843) vor. Diese betrafen insb (i) die Reichweite der Begriffe, die zu Registerpflichten führen, (ii) die Zulässigkeit einer nationalen Definition des "berechtigten Interesses" zum Datenzugang im Hinblick auf Art 7 und 8 GRC, welche das Recht auf Achtung des Privat- und Familienlebens sowie den Schutz personenbezogener Daten gewährleisten, und (iii) den Rechtsschutz bei Ausnahmen vom Zugang.

Der Generalanwalt hat erwogen: Der Unionsgesetzgeber darf zur Sicherung der praktischen Wirksamkeit der **Geldwäscheprävention** einen **offenen Begriff** ("ähnliche Rechtsvereinbarungen") verwenden. Treuhandaufträge können ähnliche Rechtsvereinbarungen sein, wenn ihre Struktur oder Funktion dazu dient, Vermögenswerte im Namen einer anderen Person anzulegen und die wirtschaftliche Eigentümerstellung nach außen zu verdecken. Der Zugang für natürliche oder juristische Personen mit "berechtigtem Interesse" nach Art 31 Abs 4 lit c ist mit Art 7 und 8 GRC vereinbar. Die Richtlinie enthält eine abschließende Liste der offenzulegenden Mindestdaten (Name, Geburtsjahr und -monat, Wohnsitzland, Staatsangehörigkeit des wirtschaftlichen Eigentümers) und erlaubt eine grundrechtskonforme, am Ziel der AML/CFT ausgerichtete Auslegung. "**Berechtigtes Interesse**" kommt insb Presse, Zivilgesellschaft und wirtschaftlich Betroffenen zu. **Nationale Präzisierungen sind grundsätzlich zulässig**, verlangen aber eine einzelfallbezogene Abwägung unter Einbeziehung der Risiken für den wirtschaftlichen Eigentümer und die Wahrung der Verhältnismäßigkeit. Eine **nichtgerichtliche Stelle** darf Ausnahmen vom Zugang bei außergewöhnlichen Umständen prüfen, sofern ein wirksamer gerichtlicher Rechtsschutz einschließlich einstweiliger Anordnungen gewährleistet ist.

### Aus der weiteren Rechtsprechung des EuGH:

- Die Digitalisierung des Energiesektors rechtfertigt die Einführung **intelligenter Messsysteme**. Die Verarbeitung personenbezogener Daten muss aber weiterhin unter Beachtung der DSGVO erfolgen. Die Bestimmung des Art 5 Abs 3 der ePrivacy-RL 2002/58 ist auf eine Smart-Meter-Datenübertragung nicht anzuwenden, wenn das **Stromnetz** nicht öffentlich ist und der Zähler nicht im Eigentum des Verbrauchers steht. Ein Stromnetz dient primär der Stromlieferung und ist kein **elektronisches Kommunikationsnetz**. Die Bestimmungen des Art 13 DSGVO sowie Art 7 und 8 GRC stehen der österreichischen Regelung (§ 84a Abs 1 EIWOG, § 1 Abs 6 IMEVO) zu Smart-Metern nicht entgegen, wonach für Endkunden lediglich die Konfiguration des Ablesintervalls ersichtlich sein muss und Netzbetreiber in begründeten Einzelfällen auch ohne Einwilligung auslesen dürfen, sofern der Verbraucher auch über diesen besonderen Zweck im Voraus informiert wird und die Daten nach Zweckerfüllung unverzüglich gelöscht werden ([EuGH SA 11.12.2025, C-468/24, \*Netz Niederösterreich\*](#)).

### Rechtsprechung des VwGH

#### Aus der Rechtsprechung des VwGH:

- Für eine **Vergleichbarkeit** der zugrunde liegenden Fallkonstellationen kommt es nicht darauf an, ob die Verantwortlichen dem Grunde nach vergleichbare Tätigkeiten ausüben, sondern darauf, ob die **jeweiligen Datenverarbeitungen** vergleichbar sind (manuelle Eingabe eines Ausgangswertes gegenüber einer Berechnung mit **automatisierter Entscheidungsfindung**). Mit dem bloßen Hinweis auf fehlende Rechtsprechung des VwGH zu einer näher bezeichneten Verwaltungsvorschrift wird nicht dargelegt, welche konkret auf die Revisionssache bezogene grundsätzliche Rechtsfrage der VwGH erstmals zu lösen hätte. Mit einem nicht näher konkretisierten Zulässigkeitsvorbringen zu den **Transparenzvorschriften** des Art 12 DSGVO wird **keine grundsätzliche Rechtsfrage** aufgezeigt ([VwGH 13.11.2025, Ra 2023/04/0271](#)).
- In einer Revision ist jenes **subjektive Recht** zu bezeichnen, in dem sich der Revisionswerber als verletzt erachtet (**Revisionspunkt**). Die verfehlte Bezeichnung der Revisionspunkte als Beschwerdepunkte schadet nicht. Wird jedoch nicht dargetan, in welchen subjektiven Rechten der Revisionswerber sich als verletzt erachtet, ist die Revision mangels tauglichen Revisionspunkts **zurückzuweisen** ([VwGH 13.11.2025, Ra 2022/04/0115](#)).

## Rechtsprechung der Justiz

OLG Innsbruck 18.06.2025, 114Ds1/23f

### **Disziplinarverfahren, IKT-NV, Ansehen des öffentlichen Dienstes**

- Ein Richter betrachtete während seiner Dienstzeit mehrfach erotische Bilder und Videos auf seinem Dienst-PC und Laptop. Zusätzlich lud er über diese Geräte erotische Bilder auf einen privaten USB-Stick herunter. Da er die Bilder auch bei offener Zimmertür betrachtete, nahmen Gerichtspersonen und Rechtspraktikanten davon Kenntnis, worauf ein **Disziplinarverfahren** gegen den Richter beim OLG eingeleitet wurde. Das OLG Innsbruck sprach den Richter wegen der Verletzung seiner Dienstpflichten nach § 57 Abs 2 und 3 RStDG und eines Dienstvergehens nach § 101 Abs 1 RStDG schuldig. Es verhängte eine Geldstrafe von 150% des Brutto-Monatsbezugs (EUR 11.727,90) sowie EUR 500 Verfahrenskosten.

Das OLG Innsbruck hat erwogen: Die **private Nutzung** von Dienst-PC und Laptop ist nach der IKT-Nutzungsverordnung (**IKT-NV**) nur in **eingeschränktem** Ausmaß zulässig. Für private Zwecke dürfen vom Dienstgeber bereitgestellte Internetdienste nur dann verwendet werden, wenn damit eine Beeinträchtigung des **Ansehens** des öffentlichen Dienstes, eine **negative Rechtsfolge** beim Dienstgeber oder eine **Verletzung** eigener oder fremder **Dienstpflichten** ausgeschlossen ist.

Das Aufrufen und Abspeichern von pornografischen Inhalten ist geeignet, das Ansehen der Justiz zu gefährden. Es ist auch dann unzulässig, wenn die Inhalte auf nicht gesperrten Internetseiten verfügbar sind. **Fremde Speichermedien** – zB USB-Sticks – dürfen nur angeschlossen werden, wenn dies **dienstlich erforderlich** ist. Herunterladen, Betrachten und Speichern von Bildern mit erotischem und pornografischem Inhalt auf einem privaten USB-Stick hat nichts mit der Dienstverrichtung eines Richters zu tun.

Das Abspeichern einschlägiger Internetadressen (etwa in Favoriten/Ordern) auf dem Dienstlaptop und das Speichern erotischer und pornografischer Bild- und Videodateien auf einem privaten USB-Stick verstößt gegen die IKT-NV sowie gegen die **ressortspezifischen IKT/IT-Benutzungs- und Sicherheitsvorgaben** und damit gegen **dienstliche Anordnungen**.

## Rechtsprechung des BVwG

BVwG 29.07.2025, W605 2251236-1

### **Besitzstörung, Tonaufnahme, Beweisnotstand, Haushaltsausnahme**

- Ein Grundstückseigentümer installierte wegen langjähriger **Nachbarschaftsstreitigkeiten** Überwachungskameras mit Bewegungsmeldern auf seinem Grundstück. Die Videoaufzeichnung war auf das eigene Grundstück beschränkt, die Tonaufzeichnung erfasste jedoch auch den angrenzenden Bereich. Als die Nachbarin Laub auf sein Grundstück warf, kam es zu einem Streitgespräch, das mit Ton aufgezeichnet wurde, obwohl sich alle Beteiligten jeweils auf ihrem eigenen Grundstück aufhielten. Die Tonaufnahme wurde später in einem **Besitzstörungsverfahren** vor Gericht verwendet. Die Nachbarin erhob daraufhin Datenschutzbeschwerde bei der DSB, die dieser stattgab und feststellte, dass der Grundstückseigentümer die Nachbarin rechtswidrig **akustisch überwacht** habe, sowohl beim Streitgespräch als auch generell durch die Tonaufnahmen auf ihrem eigenen Grundstück. Dagegen erhob der Grundstückseigentümer (erfolglos) Beschwerde an das BVwG.

Das BVwG hat erwogen: Heimliche Tonaufnahmen ohne Einwilligung verletzen das aus § 16 ABGB abgeleitete "**Recht am eigenen Wort**" auch außerhalb der Grenzen des § 120 StGB. Bei einem kamerabasierten Videoüberwachungssystem mit Mikrofon und Bewegungsmelder liegt während des gesamten Betriebs ein automatisierter Verarbeitungsvorgang vor, unabhängig davon, wie oft tatsächlich aufgezeichnet wird.

Die Verwendung von Tonaufnahmen in einem **Rechtsstreit** aufgrund berechtigter Interessen iSd Art 6 Abs 1 lit f DSGVO ist nur in engen Ausnahmefällen zulässig, etwa bei Notwehr, Notstand oder zur Verfolgung **überragender berechtigter Interessen**. Ein rechtfertigender Beweisnotstand liegt nicht schon vor, weil eine Partei über ein besonders beweiskräftiges Beweismittel verfügen möchte. Vielmehr muss der Beweisführer nachweisen, dass sein Anspruch ohne die Tonaufnahme nicht durchsetzbar wäre und seine verfolgten Interessen höherwertig sind als die verletzte Privatsphäre des Gegners.

Es lag **kein Beweisnotstand** vor, weil sich das Besitzstörungsverfahren auf die Erörterung des letzten ruhigen Besitzstands und dessen Störung beschränkt. Dem Grundstückseigentümer standen andere Beweismittel zur Verfügung, insb seine eigene Aussage und die seiner Ehegattin als Zeugin. Dem stand lediglich das Bestreiten der Nachbarin gegenüber, die früher bereits ähnliche Störungen begangen hatte. Die Entscheidungsgründe zeigen zudem, dass

die Besitzstörung wesentlich auf die glaubwürdigen Aussagen des Grundstückseigentümers und seiner Ehegattin gestützt werden konnte. Das bloße Bestreiten der Nachbarin begründete daher keinen Beweisnotstand. Eine bloß denkmögliche künftige Notstandssituation rechtfertigt die Überwachung nicht. Die **Interessenabwägung** muss *ex ante* erfolgen und darf nur die geringstmögliche Verletzung fremder Interessen zulassen. Die vom Grundstückseigentümer angeführten Vorfälle mögen zwar Videokameras erklären, rechtfertigen jedoch keine Tonaufnahmen von Gesprächen außerhalb seines Grundstücks.

Nach der Rechtsprechung des EuGH ist der Betrieb einer Videoüberwachungsanlage an einem Einfamilienhaus keine ausschließlich **persönliche** oder **familiäre Tätigkeit**, wenn auch Bereiche außerhalb des eigenen Grundstücks erfasst werden. Dies gilt auch für Anlagen mit Tonaufnahmefunktion. Entscheidend ist nicht, wo die Aufzeichnung ausgelöst wird, sondern dass der Aufnahmebereich über das eigene Grundstück hinausreicht und damit Gespräche auf dem Nachbargrundstück erfasst werden können. Ein berechtigtes Interesse, solche Gespräche aufzuzeichnen, ist nicht erkennbar. Die Datenverarbeitung geht über das erforderliche Maß hinaus. Das Geheimhaltungsinteresse der Nachbarin wiegt höher als das Interesse des Grundstückseigentümers.

#### Aus der weiteren Rechtsprechung des BVwG:

- Die Mitgliedstaaten sind nach Art 3 Abs 1 VO-SIS-Rückkehr dazu verpflichtet, eine erlassene Rückkehrentscheidung in das Schengener Informationssystem (**SIS**) einzutragen. **Art 3 VO-SIS-Rückkehr** legt einen **klaren Zweck der Ausschreibung** – nämlich die Unterstützung bei der Durchsetzung von gegen illegal aufhältigen Drittstaatsangehörigen erlassenen Rückkehrentscheidungen – fest. ISd **Art 6 Abs 3 DSGVO** bildet die VO-SIS-Rückkehr die Rechtsgrundlage für die Verarbeitung. Die **Datenverarbeitung** ist zur Erreichung dieses Zwecks in Hinblick auf die **Identifizierung** der Betroffenen im Raum der **Schengener Mitgliedstaaten** jedenfalls erforderlich. An der normierten Unterstützung zur Effektivierung erlassener Rückkehrentscheidungen gegen illegal aufhältige Drittstaatsangehörige besteht ein **erhebliches öffentliches Interesse** ([BVwG 22.10.2025, W254 2316529-1](#)).
- Eine Datenübermittlung durch eine **leitende Mitarbeiterin** des Verantwortlichen zum Zweck der Personalverwaltung ist dem Verantwortlichen **zuzurechnen**. Für die Übermittlung von **Gesundheitsdaten** ist eine **ausdrückliche Einwilligung** erforderlich. Eine konkludente Einwilligung

genügt nicht. Das Aushängen eines Laborbefunds im öffentlich zugänglichen Gang eines Amtshauses erfüllt nicht den Ausnahmetatbestand des Art 9 Abs 2 lit e DSGVO, wonach sensible Daten, die von der Betroffenen offensichtlich öffentlich gemacht wurden, verarbeitet werden dürfen. Denn die vom EuGH geforderte **breite Öffentlichkeit** liegt nicht vor ([BVwG 20.10.2025, W258 2246973-1](#)).

- In einem gegen den Betroffenen geführten **Besitzstörungsverfahren** wurden als Beweismittel Lichtbilder vorgelegt. Die Lichtbilder wurden mit einer Handkamera angefertigt, nachdem ein "**elektronischer Wachhund**" durch einen Signalton über die Besitzstörung informierte. Bilddaten, die das KFZ des Betroffenen vor dem Schuppen an der betreffenden Liegenschaft zeigen, sind personenbezogene Daten des Betroffenen. Das **anlassbezogene Erheben** von Bilddaten, zB Fotografieren mit einem Handy zur Geltendmachung von gerichtlichen Rechtsbehelfen, ist jedoch zulässig. Ein die Persönlichkeitsrechte des ABGB einschränkender **Überwachungsdruck** kann im verwaltungsgerichtlichen Verfahren nicht geltend gemacht werden ([BVwG 28.08.2025, W298 2280052-1](#)).
- Das BVwG wies die Bescheidbeschwerde des Betroffenen gegen den Bescheid der DSB mit Erkenntnis ab. Der Betroffene stellte fristgerecht einen Antrag auf **Verfahrenshilfe** zur Erhebung einer Revision an den VwGH. Auf einen **Verbesserungsauftrag** des BVwG reagierte er jedoch nicht. Der Verfahrenshilfeantrag wird daher **zurückgewiesen** ([BVwG 23.10.2025, W274 2309030-2](#)).

#### Rechtsprechung der DSB

##### Aus der Rechtsprechung der DSB:

- Der **Beschuldigte** hat gegen die DSGVO verstoßen, indem er über eine **Dashcam** ohne entsprechende **Kennzeichnung** samt vorheriger **Mitteilung** Aufzeichnungen angefertigt und gespeichert hat. Der Schutz des **geparkten Fahrzeugs** sowie die **Dokumentation** von Unfallhergängen sind zwar **berechtigte Interessen**, die Videoaufzeichnungen können aber schon deshalb nicht auf berechtigte Interessen gestützt werden, weil der Beschuldigte die Videoüberwachung nicht gekennzeichnet hat und somit die Betroffenen darüber nicht informierte. Ein **Verschulden** liegt bereits vor, wenn der Beschuldigte sich über die Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte. Die verhängte **Geldstrafe** iHv EUR 600 ist tat- und schuldangemessen ([DSB 29.09.2025, 2025-0.682.666](#)).
- Die Verarbeitung personenbezogener Daten durch einen bestellten

**Insolvenzverwalter** ist als **justizielle Tätigkeit** anzusehen. Die DSB ist zur Beurteilung solcher Datenverarbeitungen **unzuständig** ([DSB 26.09.2025, 2025-0.117.456](#)).

- **Rechtsanwälte** sind datenschutzrechtliche **Verantwortliche**. Verfasst ein Rechtsanwalt einen Schriftsatz oder legt er Urkunden in einem Gerichtsverfahren vor, in denen personenbezogene Daten verarbeitet werden, ist der Rechtsanwalt – und nicht sein Mandant – als Verantwortlicher anzusehen. Wird der Mandant in der Datenschutzbeschwerde als **Beschwerdegegner** bezeichnet, darf die DSB den Beschwerdegegner von Amts wegen nicht austauschen ([DSB 25.09.2025, 2025-0.432.701](#)).
- Eine **Löschung von Ausschreibungen** im Schengener Informationssystem (**SIS**) ist nur unter bestimmten Voraussetzungen geboten, ua wenn die zuständige Behörde die Entscheidung, aufgrund deren die Ausschreibung eingegeben wurde, zurückgenommen oder für nichtig erklärt hat. Erwächst die der Ausschreibung zugrundeliegende **Rückkehrentscheidung** in Rechtskraft und ist sie aufrecht, kommt keine Löschung in Betracht ([DSB 29.09.2025, 2025-0.754.485](#)).
- Die österreichische Rechtsordnung anerkennt das Rechtsinstitut der "**Verwirkung eines Rechts**" nicht. Solange eine Forderung besteht, ist die zugrundeliegende Datenverarbeitung für den **Gläubigerschutz** sowie zur **Risikominimierung** gerechtfertigt. Für das Verhängen einer Strafe gemäß § 63 DSG ist die DSB **nicht zuständig** ([DSB 29.09.2025, 2024-0.501.636](#)).
- Schreitet ein Rechtsanwalt für einen Auskunftswerber ein, genügt die **Berufung** auf die ihm erteilte **Vollmacht** (auch) gegenüber einem Verantwortlichen des **privaten Bereichs**. Die Vorlage der Vollmacht ist nicht erforderlich. Es ist kein **Missbrauch** des Auskunftsrechts, wenn ein Auskunftersuchen nur deshalb gestellt wird, weil im Anschluss (möglicherweise) ein **Gerichtsverfahren** angestrebt werden wird. Das Auskunftsrecht ist ein antragsbedürftiges Recht. Stellt der Auskunftswerber **kein Auskunftersuchen** an den Verantwortlichen, kann er in seinem **Auskunftsrecht nicht verletzt sein** ([DSB 01.10.2025, 2025-0.765.344](#)). **Anm:** Die Oberlandesgerichte verlangen die Vorlage einer Vollmacht, sofern der Rechtsanwalt gegenüber einem Verantwortlichen des privaten Bereichs einschreitet. Somit entsteht zwischen den Rechtsprechungen der OLGs und der DSB eine Judikaturdivergenz.



## EU-Rechtsakte

- Am **12.12.2025** wurde die "*Verordnung (EU) 2025/2518 des Europäischen Parlaments und des Rates vom 26. November 2025 zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679*", [ABL L 2025/2518](#), kundgemacht. In dieser VO werden Verfahrensvorschriften für die Durchführung von **grenzüberschreitenden Verfahren** festgelegt.

## Nationale Rechtsakte

- Am **12.12.2025** wurde das **Zweite EU-Informationssysteme-Anpassungsgesetz**, [BGBl I 2025/87](#), kundgemacht. Mit dieser Sammelnovelle wird die Interoperabilität zwischen **EU-Informationssystemen** hergestellt und das Europäische Reiseinformationssystem (**ETIAS**) eingerichtet.
- Am **12.12.2025** wurde die "*Änderung des Allgemeinen Verwaltungsverfahrensgesetzes 1991*", [BGBl I 2025/82](#), kundgemacht. Mit diesem Gesetz wird das **AVG-Großverfahren** novelliert. Ua soll das Rechtsinformationssystem des Bundes (**RIS**) als **einheitliche elektronische Kundmachungsplattform** etabliert werden.

# Datenschutzmonitor. 51/2025 vom 29.12.2025

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das **Datenschutzrecht**, das **Digitalisierungsrecht** sowie das **IFG** schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

**Aktuell:** Unser **IFG-Musterpaket** stellen wir Ihnen auf Anfrage gerne zur Verfügung.

Abonnieren Sie auch unsere anderen periodischen Newsletter, **Digital Law Monitor**, **Technology & Digitalisation**, **Financial Regulation**, **Healthcare & Life Sciences** sowie **White Collar Crime** für regelmäßige, prägnante Updates [hier](#).

Wir laden Sie herzlich zum nächsten Termin unserer **Schönherr Tech&Law Academy** über **Incident Response & Cybersecurity** am **21.01.2026** ein. Melden Sie sich [hier](#) an.

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des EGMR**

EGMR 18.12.2025, 37514/20, *Černý/Tschiechen* (Anwaltskorrespondenz, Datenextraktion)

- **Rechtsprechung des EuGH**

EuGH 18.12.2025, C-422/24, *Storstockholms Lokaltrafik* (Körperkamera, Informationspflicht, gestuftes Informationsverfahren)

EuGH SA, 18.12.2025, C-604/24, *Farmakeio YZ & Sia* (Apotheke, Online-Shop, Arzneimittel)

- **Rechtsprechung des VfGH**

VfGH 27.11.2025, G99/2025 (Kartellrecht, Auswertung elektronischer Datenträger)

VfGH 09.12.2025, E335/2025 (Geldbuße, Strafkompetenz der DSB)

- **Rechtsprechung der Justiz**

OGH 26.11.2025, 6Ob141/24i (Google Fonts, Aufforderungsschreiben, Aussetzung)

OGH 26.11.2025, 6Ob189/24y (Bestimmtheit des Klagebegehrens, Feststellungsklage, Vertragserfüllung, Auskunft)

OLG Wien 18.07.2025, 15R16/25w (Kontenregisterauskunft, Verlassenschaft)

- **Rechtsprechung des BVwG**

BVwG 24.07.2025, W129 2310165-1 (Studierendendaten, private E-Mail-Adressen)

- **Rechtsprechung der LVwG**

LVwG Tirol 11.12.2025, LVwG-2025/21/2529-8 (IFG, dienst- und disziplinarrechtliche Informationen, Datenschutz)

LVwG Vorarlberg 24.10.2025, LVwG-488-1/2025-R22 (IFG, Informationspflicht, börsennotierte Gesellschaft)

- **Rechtsprechung der DSB**

DSB 08.10.2025, 2025-0.794.213 (Zuständigkeit, Rechtsschutz)

DSB 30.09.2025, 2025-0.757.551 (Auskunft, Tracking-Pixel, Auftragsexzess)

DSB 03.10.2025, 2025-0.677.597 (Referenzdatenbank, Zweckbindung)

DSB 01.10.2025, 2025-0.757.155 (Unternehmensserviceportal, veröffentlichte Daten, social watchdog)

DSB 05.12.2025, 2025-0.874.918 (Datenspeicherung, bonitätsrelevante Daten)

- **EU-Rechtsakte**

Vier DurchführungsVOs zur eIDAS

- **Nationale Rechtsakte**

Bundesrat beschließt NISG 2026

Zweite Transparenzdatenbank-Abfrageverordnung 2025

- **Vorschau EuGH-Rechtsprechung**

## To the Point:

### Rechtsprechung des EGMR

EGMR 18.12.2025, 37514/20, Černý/Tschiechien

#### **Anwaltskorrespondenz, Datenextraktion**

- Fünf Anwälte vertraten einen Mandanten in mehreren Strafverfahren. Bei einer Hausdurchsuchung stellte die Polizei das Smartphone und ein Tablet des Mandanten sicher. Die Geräte enthielten umfangreiche Kommunikation zwischen Mandant und Anwälten, darunter Schriftsatzentwürfe, Notizen zur Verteidigungsstrategie und weitere durch das **Anwaltsgeheimnis** geschützte Inhalte. Nachdem ein tschechisches Gericht die vollständige Auswertung der Geräte angeordnet hatte, nahmen die Behörden sämtliche extrahierten Daten in den Strafakt auf und machten sie den Mitbeschuldigten sowie der Staatsanwaltschaft zugänglich. Nach erfolglosem Ausschöpfen des Rechtswegs erhoben die Anwälte (erfolgreich) Beschwerde an den EGMR.

Der EGMR hat erwogen: Die aus den Geräten des Mandanten extrahierten und zur Gerichtsakte genommenen Daten enthielten **privilegierte Kommunikation** zwischen den Anwälten und ihrem Mandanten. Ein solcher Austausch genießt **besonderen Schutz** nach Art 8 EMRK. Die Anwälte durften **berechtigterweise die Wahrung der Vertraulichkeit** ihrer Kommunikation erwarten. Der **Schutz der Anwaltskorrespondenz** erstreckt sich auch auf **elektronische Kommunikation** auf den Geräten der Anwälte sowie des Mandanten. Die Aufnahme dieser Kommunikation in die Gerichtsakte ist ein Eingriff in das Recht der Anwälte auf Achtung ihres Privatlebens und ihrer Korrespondenz.

Die Vorschriften zur **Extraktion von Daten** aus beschlagnahmten elektronischen Geräten waren weder hinreichend klar noch vorhersehbar und enthielten **keine ausreichenden Schutzmechanismen** zum Schutz der Anwaltskorrespondenz. Das Gesetz erfüllt daher nicht die Anforderungen an einen "gesetzlich vorgesehenen" Eingriff iSd Art 8 Abs 2 EMRK.

Ein **wirksamer Rechtsbehelf** hätte eine Überprüfung der Rechtmäßigkeit sowie eine Anordnung zur Entfernung oder Vernichtung des geschützten Materials ermöglichen müssen. Da den Anwälten ein solcher Rechtsbehelf nicht zur Verfügung stand, lag auch eine Verletzung von Art 13 EMRK vor.

### Rechtsprechung des EuGH

EuGH 18.12.2025, C-422/24, Storstockholms Lokaltrafik

#### **Körperkamera, Informationspflicht, gestuftes Informationsverfahren**

- Ein öffentlicher Personenverkehrsdienstleister stattete seine **Fahrkartenkontrolleure** zur Verhinderung und Dokumentation von Drohungen und Gewalt gegen die Kontrolleure sowie zur Identitätsfeststellung der Fahrgäste mit **Körperkameras** aus. Die Kameras nahmen während der gesamten Schicht der Kontrolleure durchgehend Filme mit Bild und Ton auf. Das System löschte die Aufnahmen zwar nach zwei bzw. einer Minute, die Kontrolleure konnten die Löschung jedoch in Situationen, in denen sie eine Strafgebühr erhoben, sowie in Bedrohungssituationen per Knopfdruck unterbrechen. Die schwedische Aufsichtsbehörde verhängte eine Geldbuße von über EUR 1,4 Mio, wovon knapp EUR 400.000 auf die **mangelnde Information** der Betroffenen entfielen. Das vorliegende Gericht fragte den EuGH, ob der Verantwortliche die Betroffenen beim Tragen einer Körperkamera gemäß Art 13 oder 14 DSGVO informieren muss.

Der EuGH hat erwogen: Bei der Auslegung des Unionsrechts sind nicht nur dessen Wortlaut, sondern auch dessen **Kontext** und **Ziele** zu berücksichtigen.

Der Verantwortliche muss die Information nach Art 13 DSGVO erteilen, wenn er personenbezogene Daten **beim Betroffenen** erhebt. Werden personenbezogene Daten bei einer **anderen Person** – als dem Betroffenen – erhoben, gelangt Art 14 DSGVO zur Anwendung. Eine besondere Handlung des Betroffenen setzt Art 13 DSGVO nicht voraus. Entscheidend ist die Handlung des Verantwortlichen, sodass es keine Rolle spielt, in welchem Maß der Betroffene aktiv wird.

Auch wenn der Verantwortliche personenbezogene Daten **durch Beobachten**, zB mit einer Kamera, beim Betroffenen erhebt, muss er Art 13 DSGVO anwenden. Denn er **erlangt** die Daten unmittelbar vom Betroffenen selbst.

Der Verantwortliche muss die Information über die Datenerhebung daher zum **Zeitpunkt der Erhebung** erteilen. Dies kann, wenn er personenbezogene Daten bei einer anderen Person erhebt, erschwert oder unmöglich sein. Deshalb sieht Art 14 DSGVO eine spätere Erfüllung der Informationspflicht durch den Verantwortlichen vor.

Der Verantwortliche darf die geschuldete Information nach Art 13 DSGVO in einem **gestuften Verfahren** erteilen. Dabei kann er die **wichtigsten Informationen** auf

einem **Hinweisschild** anzeigen und die weiteren obligatorischen Informationen auf einer **zweiten Ebene** in geeigneter und vollständiger Weise an einem leicht zugänglichen Ort zur Verfügung stellen. Er kann die **berechtigten Interessen** des Verantwortlichen berücksichtigen. **Anm 1: Fraglich ist, ob diese Rechtsprechung auf die Datenerhebung im Online-Umfeld übertragen werden kann. Denn auch etwa die IP-Adresse wird vom Betroffenen selbst erlangt. Da Art 13 DSGVO keine Information über die Kategorien der verarbeiteten personenbezogenen Daten anordnet, könnte sohin die Informationspflicht über das Erheben von IP-Adressen nach der DSGVO entfallen. Unberührt bliebe allerdings die Informationspflicht des § 165 Abs 3 TKG 2021. Anm 2: Zu beachten ist der Hinweis des EuGH auf die mögliche Berücksichtigung der berechtigten Interessen des Verantwortlichen.**

Aus der weiteren Rechtsprechung des EuGH:

- Die Mitgliedstaaten müssen – unter den in der [RL 2001/83/EG](#) zur Schaffung eines **Gemeinschaftskodexes** für **Humanarzneimittel** vorgesehenen Bedingungen – den **Online-Shops** von **Apotheken** den Vertrieb **nicht verschreibungspflichtiger Arzneimittel** gestatten. Eine nationale Bestimmung, die den Online-Shops von Apotheken den Verkauf bestimmter nicht verschreibungspflichtiger Arzneimittel aus Gründen des **Schutzes der öffentlichen Gesundheit** verbietet, ist unionsrechtswidrig ([EuGH SA, 18.12.2025, C-604/24, Farmakeio YZ & Sia](#)).

### Rechtsprechung des VfGH

Aus der Rechtsprechung des VfGH:

- Der **Gesetzesprüfungsantrag** auf Aufhebung von Bestimmungen bzw Wortfolgen des Wettbewerbsgesetzes (WettbG) wegen unzureichenden Schutzes vor der **Sicherung und Auswertung** personenbezogener elektronisch gesicherter Daten bei **Hausdurchsuchungen** durch die Bundeswettbewerbsbehörde wird als zu eng gefasst zurückgewiesen ([VfGH 27.11.2025, G99/2025](#)).
- Die Zuständigkeit der **DSB** zum Verhängen von **Geldbußen** beruht auf Art 83 DSGVO. Für den **nationalen Gesetzgeber** besteht somit **kein Umsetzungsspielraum** ([VfGH 09.12.2025, E335/2025](#)).

### Rechtsprechung der Justiz

OGH 26.11.2025, 6Ob141/24i

#### **Google Fonts, Aufforderungsschreiben, Aussetzung**

- Eine Websitebesucherin rief nach Beratung durch ihren Anwalt mithilfe eines Programms, das im Hintergrund die Datenströme beim Surfen protokollierte, innerhalb kurzer Zeit tausende Websites auf, darunter auch die der betroffenen Websitebetreiberin. Aufgrund einer automatisierten Erkennung von Google Fonts richtete der Anwalt standardisierte Aufforderungsschreiben an die jeweiligen Websitebetreiber. Auch die betroffene Websitebetreiberin erhielt ein anwaltliches Schreiben, in dem der Anwalt die Übermittlung der IP-Adresse der Websitebesucherin an Google ohne deren Zustimmung als Datenschutzverstoß beanstandete und einen Vergleich über EUR 190 anbot. Insgesamt versandte der Anwalt rund 32.000 derartige Schreiben.

Der OGH hat erwogen: Da sich im Revisionsverfahren insbesondere Fragen zur Qualifikation **dynamischer IP-Adressen** als personenbezogene Daten iSd Art 4 Z 1 DSGVO sowie zum Einwand des Rechtsmissbrauchs iZm Ansprüchen auf immateriellen Schadenersatz gemäß Art 82 Abs 1 DSGVO und auf Auskunft gemäß Art 15 DSGVO stellen, wird das Verfahren bis zur Entscheidung des EuGH über mehrere Vorabentscheidungsersuchen ausgesetzt. Die Vorlagefragen betreffen insbesondere die Qualifikation dynamischer IP-Adressen als personenbezogene Daten, die mögliche Exzessivität von Auskunftersuchen nach Art 15 DSGVO, den Anspruch auf immateriellen Schadenersatz bei **bewusst und gezielt herbeigeführten Datenschutzverstößen** sowie den Rechtsmissbrauchseinwand bei **künstlicher Schaffung** der Voraussetzungen für DSGVO-Ansprüche.

Aus der weiteren Rechtsprechung der Justiz:

- Das Klagebegehren muss inhaltlich hinreichend **bestimmt** sein, damit es zur **Zwangsvollstreckung** geeignet ist. Das rechtliche Interesse an einer **Feststellungsklage** ist trotz Möglichkeit einer Leistungsklage zu bejahen, wenn sie Klarheit über die Rechtsbeziehungen zwischen den Parteien schaffen kann. Ein Verantwortlicher darf eine Datenverarbeitung nur auf den Rechtfertigungstatbestand der Vertragserfüllung stützen, wenn sie objektiv unerlässlich ist. Davon nicht umfasst ist eine Datenverarbeitung, die für die Finanzierung der vertraglich geschuldeten Dienstleistung erforderlich ist. Das **Auskunftsrecht** ist ein einheitlicher Anspruch. Der Verantwortliche hat auch über solche Daten Auskunft zu erteilen, die **aus einer Verarbeitung** personenbezogener Daten

**resultieren** ([OGH 26.11.2025, 6Ob189/24y](#)).

- Der Auskunftsanspruch nach **§ 4 Abs 4 KontRegG** ist ein höchstpersönliches Recht, das als spezialgesetzliche Ausformung des durch das Grundrecht auf Datenschutz garantierten Anspruchs auf Auskunft mit dem Tod der berechtigten Person erlischt und nicht auf die **Verlassenschaft** übergeht. Die rechtliche Unmöglichkeit der Einholung einer **Kontenregisterauskunft** für die Verstorbene durch die Verlassenschaft schließt jede Zumutbarkeit zusätzlicher Nachforschungen aus ([OLG Wien 18.07.2025, 15R16/25w](#)).

### **Rechtsprechung des BVwG**

[BVwG 24.07.2025, W129 2310165-1](#)

#### **Studierendendaten, private E-Mail-Adressen**

- Ein Referent der Studierendenvertretung der Universität für Weiterbildung Krems (ÖH-UWK) beantragte die Übermittlung aktueller Studierendendaten inkl privater E-Mail-Adressen. Die Universität übermittelte sämtliche Daten mit Ausnahme der privaten E-Mail-Adressen der Studierenden. Der Rektor wies den Antrag auf bescheidmäßige Erledigung der Nichtübermittlung ab, weil die Übermittlung der privaten E-Mail-Adressen nicht von § 13 Abs 4 HSG gedeckt sei und keine datenschutzrechtliche Rechtsgrundlage bestehe. Die ÖH-UWK erhob (erfolglos) Bescheidbeschwerde an das BVwG.  
Das BVwG hat erwogen: Die ÖH-UWK ist zwar ermächtigt, **elektronische Aussendungen** an Studierende vorzunehmen. Dies ist ihr jedoch im Wege der Aussendung an die **universitäre E-Mail-Adresse** möglich. Private E-Mail-Adressen der Studierenden sind hierfür nicht zusätzlich nötig. Ein Anspruch darauf, dass Studierende Aussendungen tatsächlich lesen, besteht nicht. Dies gilt auch für private E-Mail-Adressen, deren Aktualität und Nutzung ebenfalls nicht gewährleistet ist. Weder § 10 Abs 3 Z 4 lit b BildDokG noch § 13 Abs 4 HSG verpflichten zur Übermittlung privater E-Mail-Adressen. Die universitäre E-Mail-Adresse ist als "**studierenden-, studien- und studienbeitragsbezogenes Datum**" vorrangig zu verwenden, da sie der **Abwicklung aller studienrechtlichen Belange** dient. Außerdem unterscheidet der Gesetzgeber bewusst zwischen "privater E-Mail-Adresse" (§ 18 Abs 6 Z 8 BildDokG) und anderen E-Mail-Adressen.

Zwar ist § 13 Abs 4 HSG grundsätzlich eine taugliche Rechtsgrundlage iSd Art 6 Abs 1 lit e DSGVO, doch fehlt es an der **Erforderlichkeit** der Übermittlung privater E-Mail-Adressen. Die Studierendenvertretung kann ihre Aufgaben auch über universitäre E-

Mail-Adressen sowie andere Kommunikationswege (Plakate, Informationsmaterial, Online-Veröffentlichungen) erfüllen. Eine **bessere Erreichbarkeit** durch private E-Mail-Adressen ist **nicht gegeben**. Eine Übermittlung der privaten E-Mail-Adressen an die Studierendenvertretung würde daher gegen den **Grundsatz der Datenminimierung** gemäß Art 5 Abs 1 lit c DSGVO verstoßen.

### **Rechtsprechung der LVwG**

[LVwG Tirol 11.12.2025, LVwG-2025/21/2529-8](#)

#### **IFG, dienst- und disziplinarrechtliche Informationen, Datenschutz**

- Ein Informationswerber, der zuvor zwei Dienstaufsichtsbeschwerden gegen Bedienstete einer Bezirkshauptmannschaft beim Amt der Tiroler Landesregierung erhoben hatte, stellte einen Antrag auf Informationserteilung betreffend Verwaltungsmaßnahmen iZm diesen Beschwerden. Die Tiroler Landesregierung verweigerte die Informationserteilung aus datenschutzrechtlichen Gründen. Der Informationswerber erhob (erfolglos) Bescheidbeschwerde an das LVwG Tirol.

Das LVwG Tirol hat erwogen: Die begehrten Informationen sind personenbezogen, weil der Informationswerber mit seinem **Vorwissen** selbst bei geschwärzten Unterlagen Rückschlüsse auf die Betroffenen ziehen könnte. **Dienst- und disziplinarrechtliche Informationen** sind besonders schutzwürdig, weil ihre Veröffentlichung die berufliche Reputation und Privatsphäre der Bediensteten erheblich beeinträchtigen kann. Schon die Information über Einleitung oder Nichteinleitung von Disziplinarverfahren ist ein personenbezogenes Datum mit erhöhtem Vertraulichkeitsschutz.

Auch eine selektive oder teilweise Herausgabe unter Schwärzung vermag den Personenbezug aufgrund der detaillierten Sachkenntnis des Informationswerbers nicht zu neutralisieren. Zudem bilden disziplinar- und dienstrechtliche Unterlagen **eine sachliche und verfahrensrechtliche Einheit**. Eine **isolierte Offenlegung** würde Zusammenhänge verfälschen, interne Bewertungen offenbaren und die Funktionsfähigkeit sowie das Vertrauen in Aufsichts- und Disziplinarverfahren beeinträchtigen. Das Informationsfreiheitsrecht dient auch nicht dazu, eine **Parteistellung** in solchen Verfahren zu **ersetzen**. Eine Beteiligung Außenstehender ist gesetzlich nicht vorgesehen, weshalb kein subjektives Recht auf Einsicht in die Verfahrensführung besteht. Die landesrechtlichen Disziplinarvorschriften sehen überdies einen **strengen Vertraulichkeitsschutz** vor, der die Geheimhaltungsinteressen iSd § 6 Abs 1 Z 7 lit a IFG zusätzlich verstärkt.

Da das Geheimhaltungsinteresse der Bediensteten gegenüber dem Informationsinteresse des Informationswerbers überwiegt, war der Informationszugang zu verweigern.

#### Aus der Rechtsprechung der LVwG:

- Eine Gesellschaft unter beherrschendem Einfluss des Landes Vorarlberg, die der Kontrolle des Landes-Rechnungshofes unterliegt, fällt grundsätzlich in den Anwendungsbereich des IFG. Sie ist jedoch gemäß § 13 IFG von der Informationspflicht ausgenommen, wenn sie **Emittentin von an einem geregelten Markt notierten Wertpapieren** (zB Anleihen) ist. Ihre Aktien müssen nicht börsennotiert sein, um sie als **börsennotierte Gesellschaft** iSd § 13 Abs 3 IFG zu qualifizieren ([LVwG Vorarlberg 24.10.2025](#), [LVwG-488-1/2025-R22](#)).  
**Anm: Nähere Informationen zu den Geheimhaltungsgründen des IFG insbesondere iZm privaten Informationspflichtigen finden Sie in der RDB (Paywall): [Cudlik/Petschinka, Ausgewählte Fragen der Geheimhaltung im IFG, ecolx 2025, 847](#).**

#### Rechtsprechung der DSB

DSB 08.10.2025, 2025-0.794.213

##### **Zuständigkeit, Rechtsschutz**

- Ein deutscher Nutzer gab an, dass Unbefugte unter Verwendung seiner E-Mail-Adresse auf einer niederländischen Online-Medicines-Plattform mehrere weitere Kundenkonten angelegt und Bestellungen durchgeführt hätten. Trotz geforderter und von der Plattform zugesicherter Löschung erhielt er weiterhin E-Mails zu den "falschen" Konten. Erst nach erneuter Aufforderung entfernte die Plattform mehrere Konten. Der Nutzer erhob Datenschutzbeschwerde bei der österreichischen DSB. Die DSB wies die Datenschutzbeschwerde mangels Zuständigkeit zurück.

Die DSB hat erwogen: Die Regelung des Art 77 DSGVO eröffnet das **Beschwerderecht** insbesondere am gewöhnlichen Aufenthaltsort, am Arbeitsplatz des Betroffenen oder am Ort des mutmaßlichen Verstoßes. Da der Nutzer in Deutschland wohnt, liegt auch der behauptete Verstoß in Deutschland. Die Verantwortliche hat ihren Sitz in den Niederlanden. Das Online-Angebot der Plattform (auch) unter einer **österreichischen "at"-Top-Level-Domain** allein begründet **keinen ausreichenden Bezug zu Österreich**, und auch sonst fehlt ein **objektiver Konnex** zu Österreich.

Die DSGVO sieht weder eine freie Behördenwahl noch **Forum-Shopping** ohne objektiven Bezug vor. Ziel der DSGVO ist es, den Rechtsschutz dort zu erleichtern, wo ein

**räumliches oder sprachliches Naheverhältnis** besteht. Auch wenn die Datenschutzbeschwerde nicht bei einer Aufsichtsbehörde des Sitzes des Verantwortlichen eingebracht werden muss (wie unter der DS-RL 95/46/EG), ermöglicht Art 77 DSGVO nicht die Umgehung von Aufsichtsbehörden, zu denen ein objektiver Konnex besteht.

DSB 30.09.2025, 2025-0.757.551

##### **Auskunft, Tracking-Pixel, Auftragsexzess**

- Ein Auskunftswerber richtete ein Auskunftersuchen an ein Kurzzentrum. Das Kurzzentrum verarbeitete die Daten des Auskunftswerbers mit dessen Einwilligung zum Versand von Trainingsplänen. Für den Versand der Trainingspläne beauftragte das Kurzzentrum einen IT-Dienstleister als Auftragsverarbeiter. Über den Auftrag des Versands der Trainingspläne hinaus sendete der IT-Dienstleister auch Tracking-Pixel. Das Kurzzentrum erteilte eine Auskunft, informierte aber nicht über die Verarbeitung mittels Tracking-Pixel und verwies den Auskunftswerber an den IT-Dienstleister. Dieser wiederum verwies auf das Kurzzentrum. Der Auskunftswerber erachtete die Auskunft als unvollständig und erhob gegen das Kurzzentrum und den IT-Dienstleister Datenschutzbeschwerde bei der DSB. Die DSB wies die Beschwerde gegen das Kurzzentrum ab, gab der Beschwerde gegen den IT-Dienstleister jedoch statt und trug diesem auf, die Auskunft zu erteilen.

Die DSB hat erwogen: Die **datenschutzrechtliche Rollenverteilung** bestimmt, wer die Datenschutzbestimmungen einhalten muss. **Verantwortlicher** ist, wer allein oder gemeinsam mit anderen über **Zwecke und Mittel** der Verarbeitung personenbezogener Daten entscheidet. Wesentlich für die Rollenzuordnung ist die **Entscheidung**, personenbezogene Daten **für eigene Zwecke zu verarbeiten**. Ein **Auftragsverarbeiter** hingegen verarbeitet personenbezogene Daten **im Auftrag eines Verantwortlichen**. Die Einordnung hängt nicht vom Abschluss eines Auftragsverarbeitervertrags ab, sondern davon, ob die Begriffsdefinition des Art 4 Z 8 DSGVO erfüllt ist. Erteilt der Verantwortliche einem Auftragsverarbeiter nachträglich die **Weisung**, eine **bestimmte Verarbeitung zu unterlassen**, kann eine **eigenverantwortliche Verarbeitung durch den Auftragsverarbeiter** vorliegen. Das gilt insbesondere dann, wenn die **Verarbeitung außerhalb des Auftrags** liegt und der **Auftragsverarbeiter selbst über den Zweck entscheidet**.

Das **Auskunftersuchen** bestimmt den **Umfang** der zu erteilenden Information und ist nach dem Maßstab für **einseitige**

**privatrechtliche Willenserklärungen** auszulegen, also so, wie sie der Empfänger nach Wortlaut und Zweck objektiv verstehen konnte. Fragt ein Auskunftersuchen ausdrücklich nach einem Tracking-Pixel, erwartet der Antragsteller eine konkrete Auskunft zu dieser Verarbeitung.

Da das Kurzentrum für die Verarbeitung mittels Tracking-Pixel nicht verantwortlich war, musste es darüber keine Auskunft erteilen. Verantwortlich ist der IT-Dienstleister, der das Tool einsetzt, sodass dieser Auskunft erteilen muss.

DSB 03.10.2025, 2025-0.677.597

### Referenzdatenbank, Zweckbindung

- Ein Unternehmen betrieb eine Referenzdatenbank mit beruflichen Informationen über Angehörige der Gesundheitsberufe, Gesundheitsorganisationen und weitere Stakeholder der Gesundheitsbranche. Darin verarbeitete es ua personenbezogene Daten eines Nationalratsabgeordneten, der Jurist und Präsident eines parteinahen Vereins war, jedoch keine Tätigkeit im Gesundheitsbereich ausübte. Das Unternehmen gab die Daten zudem an Unternehmen der Pharma- und Gesundheitsbranche weiter. Da sich der Nationalratsabgeordnete in seinem Recht auf Geheimhaltung verletzt erachtete, erhob er (erfolgreich) Datenschutzbeschwerde bei der DSB.

Die DSB hat erwogen: Nach dem **Zweckbindungsgrundsatz** müssen personenbezogene Daten für klar definierte und rechtmäßige Zwecke erhoben werden, die zum Zeitpunkt der **Erhebung** feststehen. Diese **Zweckfestlegung** begrenzt die Eingriffsmöglichkeiten des Verantwortlichen. Folglich ist das Unternehmen, auch wenn es eine Gewerbeberechtigung für Adressverlage und Direktmarketingunternehmen gemäß § 151 GewO hält, dennoch an die von ihm selbst festgelegten Zwecke **gebunden**. Die Qualifikation des Nationalratsabgeordneten als Stakeholder im Gesundheitsbereich ist nicht nachvollziehbar. Auch seine berufliche Qualifikation als Jurist rechtfertigt dies nicht. Die gesetzgeberische Tätigkeit im Gesundheitsbereich begründet allein keine Zuordnung aller Nationalratsabgeordneten als Gesundheitsstakeholder. Folglich waren die Erhebung, Speicherung und Weitergabe der personenbezogenen Daten für die vom Unternehmen verfolgten Zwecke **nicht erforderlich** und somit **überschießend**.

DSB 01.10.2025, 2025-0.757.155

### Unternehmensserviceportal, veröffentlichte Daten, social watchdog

- Ein Bundesamt beschaffte für einen Mitarbeiter einen ergonomischen Schreibtisch und veröffentlichte den vergebenen Auftrag im Unternehmensserviceportal unter Nennung von Vor- und Nachname des Mitarbeiters. Zudem wurde der Datensatz von einem Transparenzverein auf einer Vergabeplattform sowie von einer Ausschreibungsplattformbetreiberin auf einer entsprechenden Plattform veröffentlicht. Der Mitarbeiter fühlte sich in seinem Recht auf Geheimhaltung verletzt und erhob gegen den Transparenzverein und die Ausschreibungsplattformbetreiberin (erfolgreich) Datenschutzbeschwerde bei der DSB.

Die DSB hat erwogen: Transparenzverein und Ausschreibungsplattformbetreiberin unterliegen, anders als das Bundesamt, nicht dem Bundesvergabegesetz 2018. Zwar ist das **Unternehmensserviceportal öffentlich**, die dort veröffentlichten Daten unterliegen jedoch grundsätzlich einem **Geheimhaltungsanspruch**. Aus der zulässigen **Veröffentlichung von Daten** kann nicht generell abgeleitet werden, dass keine schutzwürdigen Geheimhaltungsinteressen bestehen; dies wäre mit europarechtlichen Vorgaben unvereinbar.

Die Tätigkeit als **"social watchdog"** zur Förderung von Transparenz in Politik und Verwaltung sowie die Vernetzung von Auftraggebern und Auftragnehmern sind grundsätzlich **berechtigte Interessen**. Allerdings verbietet der **Grundsatz der Datenminimierung** gemäß Art 5 Abs 1 lit c DSGVO nicht nur die **Erhebung zweckfremder Daten**, sondern auch die Erhebung von Daten, die für den konkreten Zweck nicht erforderlich sind. Kann der verfolgte legitime Zweck mit einem geringeren Maß an Datenerhebung, -verarbeitung oder -nutzung genauso gut verwirklicht werden, ist der beabsichtigte Umfang nicht **auf das notwendige Maß beschränkt**. Da der verfolgte Zweck auch ohne die Nennung des Vor- und Nachnamens des Mitarbeiters erreicht werden konnte, war deren Veröffentlichung **nicht erforderlich**. Die Datenverarbeitung war somit **rechtswidrig**.

Aus der weiteren Rechtsprechung der DSB:

- Die Speicherung und Verarbeitung **bonitätsrelevanter Daten** in der **"Warnliste der Banken"** ist zum Zweck des **Gläubigerschutzes** und der **Risikominimierung** nach Art 6 Abs 1 lit f DSGVO iVm § 39 BWG rechtmäßig. Kreditinstitute sind dabei **Verantwortliche** iSd Art 4 Z 7 DSGVO. Auch nach einer im Jahr 2024 erfolgten bloß teilweisen **Tilgung** durfte die **Speicherung** fort dauern. Angesichts eines mehr als

zwölfjährigen Zahlungsverzugs der Betroffenen war die weitere Verarbeitung noch **erforderlich** und **verhältnismäßig**. Ein behaupteter **Verstoß gegen Informationspflichten** führt für sich genommen nicht zur Unrechtmäßigkeit der Verarbeitung und begründet keinen Lösungsanspruch ([DSB 05.12.2025, 2025-0.874.918](#)). **Anm: Die DSB ist in ihrer Rechtsprechung, ob ein Verstoß gegen Informationspflichten zur Unrechtmäßigkeit einer auf berechnete Interessen gestützten Datenverarbeitung führt, uneinheitlich. Im Straferkenntnis vom 29.09.2025, 2025-0.682.666, vermeinte die DSB, dass die Datenverarbeitung bereits mangels Information nicht auf berechnete Interessen gestützt werden kann ([Schönherr Datenschutzmonitor 50/2025 vom 17.12.2025](#)).**

### **EU-Rechtsakte**

- Am **17.12.2025** wurden die (i) "Durchführungsverordnung (EU) 2025/2527 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf **Referenzstandards** und **Spezifikationen** für qualifizierte Zertifikate für die **Website-Authentifizierung**", [ABI L 2025/2527](#); (ii) "Durchführungsverordnung (EU) 2025/2530 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Anforderungen an **qualifizierte Vertrauensdiensteanbieter**, die qualifizierte Vertrauensdienste erbringen", [ABI L 2025/2530](#); (iii) "Durchführungsverordnung (EU) 2025/2531 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf **Referenzstandards** und **Spezifikationen** für qualifizierte **elektronische Journale**", [ABI L 2025/2531](#); und (iv) "Durchführungsverordnung (EU) 2025/2532 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf **Referenzstandards** und **Spezifikationen** für qualifizierte **elektronische Archivierungsdienste**", [ABI L 2025/2532](#), kundgemacht. Mit diesen vier Durchführungs-VOs werden **Referenzstandards** und **Spezifikationen** sowie Anforderungen an **qualifizierte Vertrauensdiensteanbieter** unter der [eIDAS-VO](#) festgelegt.

### **Nationale Rechtsakte**

- Am **18.12.2025** ist der Entwurf des "Netz- und Informationssystemsicherheitsgesetzes 2026" ([NISG 2026](#)) auch im **Bundesrat** mit Zweidrittelmehrheit [beschlossen](#) worden. Mit dem NISG 2026 wird die [NIS-2-RL \(EU\) 2022/2555](#) ins innerstaatliche Recht umgesetzt. Als zuständige Behörde wird das Bundesamt für Cybersicherheit (**Cybersicherheitsbehörde**) benannt. **Anm: Nähere Informationen finden Sie in unserem Legal Insight Österreich: [NISG 2026 – Alles, was Sie wissen müssen](#).**
- Am **19.12.2025** wurde die **Zweite Transparenzdatenbank-Abfrageverordnung 2025**, [BGBl II 2025/313](#), kundgemacht. Die VO regelt **Leseberechtigungen** in Leistungsangebote mit **sensiblen Daten** in der **Transparenzdatenbank**.



# Datenschutzmonitor. 52/2025 vom 02.01.2026

**Willkommen zu unserem wöchentlichen Datenschutz-Update.** Mit diesem wöchentlichen Newsletter wollen wir eine kurze und aktuelle Rechtsprechungsübersicht für das **Datenschutzrecht**, das **Digitalisierungsrecht** sowie das **IFG** schaffen. Erfasst wird die relevante Rechtsprechung in Österreich und auf europäischer Ebene. Neben der kurzen Zusammenfassung der einzelnen Entscheidungen zeigt der Datenschutzmonitor die Entwicklung von Rechtsprechungslinien auf.

[Registrieren Sie sich, um wöchentliche Updates in Ihr E-Mail-Postfach zu erhalten!](#)

**Aktuell:** Unser **IFG-Musterpaket** stellen wir Ihnen auf Anfrage gerne zur Verfügung.

Abonnieren Sie auch unsere anderen periodischen Newsletter, **Digital Law Monitor**, **Technology & Digitalisation**, **Financial Regulation**, **Healthcare & Life Sciences** sowie **White Collar Crime** für regelmäßige, prägnante Updates [hier](#).

Wir laden Sie herzlich zum nächsten Termin unserer **Schönherr Tech&Law Academy** über **Incident Response & Cybersecurity** am **21.01.2026** ein. Melden Sie sich [hier](#) an.

Die **Datenschutzmonitor Jahresausgabe 2024** finden Sie [hier](#).

In der vergangenen Woche wurden die nachstehenden Entscheidungen und Rechtsakte veröffentlicht:

- **Rechtsprechung des VfGH**

VfGH 18.12.2025, G105/2025 (Arzneimittel-Großhandel, juristische Person, Wirtschaftsdaten)

- **Rechtsprechung des VwGH**

VwGH 11.11.2025, Ro 2025/11/0002 (Gesundheitsdiensteanbieter, eHVD, öffentliche Apotheke)

VwGH 26.11.2025, Ra 2022/04/0157 (Untergang der Rechtspersönlichkeit)

VwGH 25.11.2025, Ra 2023/04/0268 (Revisionspunkt, mündliche Verhandlung)

VwGH 19.11.2025, Ra 2025/04/0190 (Verantwortlicher, Beschwerdegegner, Ermittlungspflicht)

VwGH 26.11.2025, Ra 2023/04/0020 (Wiedereinsetzung, Unvorhergesehenheit, Zuständigkeit)

- **Rechtsprechung der Justiz**

OLG Wien 05.11.2025, 22Bs306/25y (Europäische Ermittlungsanordnung, Auswertung von Datenträgern und Daten)

- **Rechtsprechung des BVwG**

BVwG 17.10.2025, W252 2311432-1 (Berichtigung, objektiver Erklärungswert)

BVwG 04.11.2025, W605 2324043-1 (Abweisung, aufschiebende Wirkung)

BVwG 05.11.2025, W258 2292731-1 (Massenverfahren, Aussetzung)

- **Rechtsprechung der LVwG**

LVwG NÖ 16.12.2025, LVwG-AV-1158/001-2025 (IFG, informationspflichtige Gesellschaft, Geheimhaltungsgründe)

- **Rechtsprechung der DSB**

DSB 14.10.2025, 2025-0.823.962 (Auskunft, heimliche Audioaufnahmen, Zivilverfahren, Datenkopie)

DSB 06.08.2025, 2025-0.276.820 (Leistungsauftrag, aufschiebende Wirkung, Geldbuße)

DSB 08.10.2025, 2025-0.620.443 (Grundrecht auf Datenschutz, juristische Person)

DSB 30.09.2025, 2025-0.783.392 (Veterinärbereich, Nichtfeststellbarkeit, Erkundungsbeweis)

- **EU-Rechtsakte**

Durchführungsbeschlüsse (EU) 2025/2571 und (EU) 2025/2574 zum UK-Angemessenheitsbeschluss

Entwurf einer DurchführungsVO zur TTPW-VO

- **Nationale Rechtsakte**

NISG 2026

Änderung des Gesundheitstelematikgesetzes 2012

- **Vorschau EuGH-Rechtsprechung**

## To the Point:

### Rechtsprechung des VfGH

VfGH 18.12.2025, G105/2025

#### **Arzneimittel-Großhandel, juristische Person, Wirtschaftsdaten**

- Fünf Antragsteller, die als **Arzneimittel-Vollgroßhändler** täglich einen Großteil der österreichischen Apotheken beliefern, beantragten die Überprüfung der Verfassungsmäßigkeit des in §§ 4, 5 und § 6 Abs 3 Satz 2 MSVAG geregelten **Monitoringsystems**. Das neu eingeführte Monitoringsystem, das ab 01.01.2026 eine tägliche Übermittlung von **Lager- und Bewegungsdaten** zu Arzneispezialitäten und Wirkstoffen an den zuständigen Bundesminister, an das Bundesamt für Sicherheit im Gesundheitswesen (**BASG**) und den Dachverband der Sozialversicherungsträger (**DVSV**) vorsieht, würde ausschließlich die Antragsteller verpflichten. Damit würden die §§ 4 f MSVAG nachteilig in ihre Rechtssphäre, insb in die Grundrechte auf **Achtung des Privatlebens** gemäß Art 8 EMRK und auf **Datenschutz** gemäß § 1 DSGVO eingreifen. Die meldepflichtigen Daten würden zudem **Betriebs- und Geschäftsgeheimnisse** betreffen, weil sie die gesamte Organisation und Verwaltung der Lagerhaltung, der Wareneingänge und der Distribution offenlegen würden. Der VfGH wies den **Individualantrag** ab.

Der VfGH hat erwogen: Das Grundrecht auf Datenschutz nach **§ 1 DSGVO** schützt auch **Wirtschaftsdaten juristischer Personen**. Ein staatlicher Eingriff bedarf einer gesetzlichen Grundlage, die einem in Art 8 Abs 2 EMRK genannten Zweck dient, hinreichend determiniert ist, sich auf das Erforderliche beschränkt und verhältnismäßig ausgestaltet ist. Das Monitoringsystem verfolgt mit der Sicherung der Gesundheitsversorgung sowie der gesundheitspolitischen Steuerung ein **öffentliches Interesse** iSd Art 8 Abs 2 EMRK. Aus den gesetzlichen Bestimmungen ergibt sich klar, wer, wann, welche Daten an welche Stellen zu übermitteln hat. Die Modalitäten der Datenverarbeitung sind daher ausreichend präzisiert. Zudem werden nur jene Daten erhoben, die zur Erreichung der gesetzlichen Ziele erforderlich sind.

Da die Daten weder veröffentlicht noch an private Dritte weitergegeben werden und **strenge Geheimhaltungsverpflichtungen** bestehen, ist das Geheimhaltungsinteresse der Antragsteller gewahrt. Auch die Übermittlung an den DVSV erweist sich als erforderlich und sachgerecht, weil diesem zentrale koordinierende Aufgaben im System der Arzneimittelversorgung zukommen und die Datennutzung der Wahrnehmung **gesetzlicher Aufgaben** im Kernbereich

der Sozialversicherung dient. Im Ergebnis bestehen daher keine datenschutzrechtlichen Bedenken gegen das Monitoringsystem nach Art 8 EMRK und § 1 DSGVO.

### Rechtsprechung des VwGH

VwGH 11.11.2025, Ro 2025/11/0002

#### **Gesundheitsdiensteanbieter, eHVD, öffentliche Apotheke**

- Eine niederländische Gesellschaft mit Sitz in den Niederlanden, die dort eine Apotheke betreibt, beantragte die Eintragung in den österreichischen eHealth-Verzeichnisdienst (**eHVD**) als **Gesundheitsdiensteanbieterin** unter der Rolle einer "öffentlichen Apotheke". Die zuständige Bundesministerin wies den Antrag ab. Das BVwG wies die Beschwerde ab. Daraufhin erhob die Apotheke ordentliche Revision an den VwGH, der diese abwies.

Der VwGH hat erwogen: Der **eHVD** ist ein **zentrales Register** zur eindeutigen Identifikation von **Gesundheitsdiensteanbietern** und deren Rollen bei der elektronischen Verarbeitung von Gesundheitsdaten. Gesundheitsdiensteanbieter sind gemäß § 2 Z 2 GTeIG 2012 Verantwortliche oder Auftragsverarbeiter iSd DSGVO. Sie dürfen ihre Rolle nicht frei wählen, sondern nur jene Rollen verwenden, die in der GTeIV 2013 festgelegt sind. Diese Rollen orientieren sich an österreichischen Rechtsvorschriften. Eine Zuordnung ausländischer Berufsrollen zu inländischen Rollen ist rechtlich nicht vorgesehen, vielmehr können neue oder zusätzliche Rollen durch Verordnung geschaffen werden.

Die niederländische Apotheke ist zwar in den Niederlanden zum Apothekenbetrieb berechtigt, verfügt jedoch über keine österreichische Konzession nach dem Apothekengesetz. Sie ist daher nicht unter der Rolle "**öffentliche Apotheke**" in den eHVD einzutragen.

Diese Auslegung verstößt nicht gegen Unionsrecht und beeinträchtigt weder die **Niederlassungsfreiheit** noch den **grenzüberschreitenden Versandhandel**. Die Apotheke wird nicht generell vom eHVD ausgeschlossen, sondern lediglich nicht unter der beantragten Rolle eingetragen. Eine Eintragung unter einer neu zu schaffenden oder zusätzlichen Rolle bleibt möglich.

#### Aus der weiteren Rechtsprechung des VwGH:

- Wird eine Gesellschaft aus dem **Firmenbuch gelöscht**, kann sie noch über Vermögen verfügen oder es kann noch ein **Abwicklungsbedarf** bestehen, der die Rechtssubjektivität der Gesellschaft begründet. Ein offenes **datenschutzrechtliches Verfahren** führt jedoch zu **keinem**

**Abwicklungsbedarf.** Infolge des **Untergangs der Rechtspersönlichkeit** des Verantwortlichen als Revisionswerber ist die Revision für **gegenstandslos** zu erklären und das Verfahren einzustellen ([VwGH 26.11.2025, Ra 2022/04/0157](#)).

- Der **Revisionspunkt** muss hinreichend klar die Geltendmachung des **subjektiven Rechts** des Verantwortlichen auf Abweisung der Datenschutzbeschwerde und auf Nichtfeststellung der Datenschutzverletzung erkennen lassen. Beantragt der Verantwortliche eine **mündliche Verhandlung** und steht der entscheidungswesentliche Sachverhalt nicht fest, ist eine mündliche Verhandlung durchzuführen ([VwGH 25.11.2025, Ra 2023/04/0268](#)).
- Benennt der Betroffene in der Datenschutzbeschwerde unmissverständlich und unzweifelhaft eine bestimmte Person als **Verantwortlichen**, darf die DSB das Verfahren nicht gegen eine andere Person führen. Auch das BVwG darf die **Person des Beschwerdegegners** (= Verantwortlichen) **nicht austauschen**. Zur Bestimmung der Verantwortlichenstellung ist stets **zu ermitteln**, ob ein Handeln der Organisation oder den handelnden Bediensteten zuzuordnen ist ([VwGH 19.11.2025, Ra 2025/04/0190](#)).
- Die **Wiedereinsetzung in den vorigen Stand** ist nur möglich, wenn der Antragsteller die Frist wegen eines unvorhergesehenen oder unabwendbaren Ereignisses versäumt hat. Die "**Unvorhergesehenheit**" kann noch gewahrt sein, wenn der Partei in Ansehung der Wahrung der Frist nur ein milderer Grad der Versehung, dh eine **leichte Fahrlässigkeit**, unterläuft. Dies gilt, wenn ein Fehler begangen wurde, den gelegentlich auch ein sorgfältiger Mensch macht. Bei einer rechtskundigen Partei oder wenn ein rechtskundiger Parteienvertreter einschreitet, ist ein **strengerer Maßstab** anzulegen als bei einer rechtsunkundigen Partei. Die **Fristversäumnis** bei der Erhebung eines Rechtsmittels infolge unrichtiger Rechtsbelehrung ist mit einer Fristversäumnis bei einem verfahrenseinleitenden Antrag nicht vergleichbar. Versäumt der Antragsteller die Frist, weil er die Datenschutzbeschwerde bei der **unzuständigen** DSB statt gemäß Art 130 Abs 2a B-VG beim zuständigen **Präsidenten des BVwG** eingebracht hat, ist keine Wiedereinsetzung in den vorigen Stand möglich ([VwGH 26.11.2025, Ra 2023/04/0020](#)).

### Rechtsprechung der Justiz

Aus der Rechtsprechung der Justiz:

- Die Zulässigkeit der Vollstreckung einer **Europäischen Ermittlungsanordnung (EAA)** ist vom Gericht eigenständig zu prüfen und gegebenenfalls in sinngemäßer

Anwendung des § 105 StPO zu bewilligen. Die gerichtliche Bewilligung der **Beschlagnahme von Datenträgern und Daten** zur Auswertung durch deutsche Behörden war jedoch mit einem Begründungsmangel behaftet, weil konkrete Angaben zu Datenkategorien, Dateninhalten und zum erfassten Zeitraum nach § 115f Abs 3 StPO fehlten. Nach **§ 55e EU-JZG** hat die vollstreckende Behörde die nationalen Voraussetzungen der Ermittlungsmaßnahme einzuhalten, insb soweit diese dem Schutz von Grundrechten – hier dem Recht auf Achtung des Privat- und Familienlebens sowie dem Datenschutz – dienen. Die Bewilligung muss daher den Zugriff auf verdachtsrelevante Informationen durch eine **hinreichende Bestimmung** von Datenkategorien, Inhalten und Zeiträumen begrenzen. Der Beschluss wird im Umfang der gerichtlichen Bewilligung der Beschlagnahme der Datenträger und Daten zum Zweck der **Auswertung** durch die deutschen Behörden aufgehoben. Die Übermittlung von Datenträgern oder Originalsicherungen an den Ausstellungsstaat ist zulässig ([OLG Wien 05.11.2025, 22Bs306/25y](#)).

### Rechtsprechung des BVwG

Aus der Rechtsprechung des BVwG:

- Der aus einer E-Mail hervorgehende Wunsch eines Betroffenen, die Korrektur der in seinem Profil verwendeten Anrede zu erreichen, genügt zur Ausübung des Betroffenenrechts auf **Berichtigung**. Es kommt auf den **objektiven Erklärungswert** und nicht auf die Bezeichnung von Bestimmungen der DSGVO an ([BVwG 17.10.2025, W252 2311432-1](#)).
- Wird eine **Datenschutzbeschwerde**, mit der die Feststellung einer behaupteten Verletzung des Rechts auf Löschung geltend gemacht wird, **abgewiesen**, kann der Bescheidbeschwerde keine – ausdrücklich beantragte – **aufschiebende Wirkung** gewährt werden. Denn Beschwerden gegen Bescheide, deren Inhalt nicht in die Wirklichkeit umgesetzt werden kann, kommt keine aufschiebende Wirkung zu ([BVwG 04.11.2025, W605 2324043-1](#)). **Anm: Hier scheiterte die aufschiebende Wirkung bei der Bescheidbeschwerde, weil der Bescheid keine Wirkung entfaltete, die aufgeschoben hätte werden können.**
- Ein Verfahren kann ausgesetzt werden, wenn bei einem Verwaltungsgericht in einer erheblichen Zahl von anhängigen oder zu erwartenden Verfahren eine Rechtsfrage zu lösen ist, die in einem – gleichzeitig anhängigen – Verfahren vor dem VwGH zu lösen ist. Beim BVwG sind zum selben Themenkomplex etwa 100 Bescheidbeschwerden anhängig. Damit liegt eine **erhebliche**

**Anzahl an Verfahren** vor. Das gegenständliche Verfahren ist eines dieser Verfahren und daher **auszusetzen** ([BVwG 05.11.2025, W258 2292731-1](#)).

### **Rechtsprechung der LVwG**

[LVwG NÖ 16.12.2025, LVwG-AV-1158/001-2025](#)

### **IFG, informationspflichtige Gesellschaft, Geheimhaltungsgründe**

- Eine im mittelbaren Alleineigentum des Landes Niederösterreich stehende Gesellschaft schloss mit einem Unternehmen einen Vertrag über die Umsetzung eines Projekts. Der Vertrag enthielt wechselseitige, finanziell sanktionierte Geheimhaltungspflichten für im Zuge der Vertragsabwicklung erlangte Informationen. Ein Journalist richtete ein Informationsbegehren an die Gesellschaft, das ua auf den Vertrag, den Projektfortschritt, die Anzahl der Beschäftigten und die Gesellschafter des Unternehmens abstellte. Die Gesellschaft verweigerte die Informationsgewährung. Daraufhin beantragte der Journalist gemäß § 14 IFG die Entscheidung der Streitigkeit durch das LVwG NÖ. Das LVwG NÖ entschied, dass die begehrten Informationen nicht zu erteilen sind.

Das LVwG NÖ hat erwogen: Für die Berechnung der **Antragsfrist** ist auf den Ablauf der Frist zur Informationserteilung abzustellen und nicht auf die Mitteilung über die Nichtgewährung der Information. Dies vermeidet Beweisfragen über den Zugang dieser Mitteilung.

Die Gesellschaft fällt zwar nicht unter die Ausnahme für **börsennotierte Unternehmen**, doch können deren Informationspflichten zur Bestimmung der Reichweite des Informationsrechts herangezogen werden. Demnach besteht eine Veröffentlichungspflicht für einzelne Verträge nur nach § 108 Abs 3 Z 3 AktG, wenn die Hauptversammlung über die Zustimmung zu einem Vertrag zu entscheiden hat. Diese Pflicht gilt also grundsätzlich nur gegenüber den Eigentümern. Anstelle der Übermittlung eines Vertragsentwurfs genügt die Bereitstellung des **wesentlichen Inhalts**. Außenstehende haben daher grundsätzlich keinen Anspruch auf Information über einzelne Verträge oder konkrete Projekte durch private Informationspflichtige.

An der Aufklärung geschäftlicher Verbindungen staatlicher Unternehmen kann zwar ein **öffentliches Interesse** bestehen, das nach Geschäftsgegenstand und ggf nach außenpolitischen Bezügen zu beurteilen ist. Da das Informationsbegehren an einen privaten Informationspflichtigen gestellt wurde und der Gegenstand des Informationsbegehrens nicht die Erfüllung öffentlicher Aufgaben betraf, gelangt **Art 10**

**EMRK** jedoch nicht zur Anwendung. Das öffentliche Interesse ist daher mit **abgeschwächtem Gewicht** zu berücksichtigen. Die begehrte Information über die **Mitarbeiteranzahl** zu bestimmten Zeitpunkten an bestimmten Orten würde Rückschlüsse auf Personen ermöglichen und damit in deren **Datenschutzrechte** eingreifen. Zudem wären Rückschlüsse auf die Ressourcenzuordnung möglich, wodurch **Geschäfts- und Betriebsgeheimnisse** offengelegt und die **Wettbewerbsfähigkeit** beeinträchtigt würden. Gleiches gilt für Informationen zum **Projektfortschritt**.

Die Offenlegung des **Vertrags** würde die **vertragliche Geheimhaltung** verletzen, **finanzielle Nachteile** verursachen und **Geschäfts- und Betriebsgeheimnisse** offenbaren.

Informationen, die das Land NÖ betreffen, fallen nicht in den **Geschäftsbereich** der Gesellschaft. Ihre Offenlegung würde Geheimhaltungspflichten, Geschäftsgeheimnisse und personenbezogene Daten betreffen. Der Eingriff wiegt umso schwerer, als auch für die Berichterstattung nicht erforderliche Daten umfasst wären und dem Journalisten die wesentlichen Personen bereits bekannt sind.

Die begehrten Informationen über **Gesellschafter** und Hintergründe des Vertragspartners sind zwar grundsätzlich relevant für die Berichterstattung, unterliegen jedoch der **vertraglichen Geheimhaltung** und betreffen Geschäftsgeheimnisse sowie personenbezogene Daten. Da die gegen eine Informationserteilung sprechenden Interessen überwiegen, sind die begehrten Informationen nicht zu erteilen. **Anm 1: Zur Berechnung der Antragsfrist auf Entscheidung der Streitigkeit ist eine Judikaturdivergenz zwischen dem LVwG NÖ und dem BVwG entstanden, denn das BVwG erachtete in seinem Erkenntnis vom [11.11.2025, W274 2323801-1](#), die Mitteilung über die Informationsnichtgewährung als fristauslösend. Wir haben im [Schönherr Datenschutzmonitor 47/2025 vom 26.11.2025](#) berichtet.**

**Anm 2: Nähere Informationen zu den Geheimhaltungsgründen des IFG, insb iZm privaten Informationspflichtigen, finden Sie in der RDB (Paywall): [Cudlik/Petschinka, Ausgewählte Fragen der Geheimhaltung im IFG, ecolex 2025, 847](#).**

### **Rechtsprechung der DSB**

[DSB 14.10.2025, 2025-0.823.962](#)

### **Auskunft, heimliche Audioaufnahmen, Zivilverfahren, Datenkopie**

- Ein **Nachbar** verlangte im Zusammenhang mit einem zivilrechtlichen Verfahren betreffend **Lärmemissionen** Auskunft zu

heimlich erstellten Audioaufnahmen, auf denen er stimmlich erkennbar ist. Die Nachbarin verweigerte die Auskunft mit der Begründung, dass ihr Interesse an der Herstellung der Tonbandaufnahmen überwiege und das Auskunftsrecht bereits durch die Akteneinsicht im Zivilverfahren "konsumiert" worden sei. Die DSB gab der Datenschutzbeschwerde statt und stellte eine Verletzung des Auskunftsrechts fest.

Die DSB hat erwogen: **Stimmen- bzw Gesprächsaufnahmen** sind idR personenbezogene Daten. Der Nachbar ist im Kontext des Zivilverfahrens sowie aufgrund namentlicher Nennungen auf den Tonaufnahmen identifizierbar. Das Auskunftsrecht besteht jedoch nur hinsichtlich der eigenen personenbezogenen Daten des Nachbarn, nicht für Tonsegmente, die ausschließlich seine Ehegattin oder Kinder betreffen. Eine **Beschränkung des Auskunftsrechts** nach Art 23 Abs 1 lit j DSGVO zur Sicherstellung der **Durchsetzung zivilrechtlicher Ansprüche** kommt in Österreich mangels entsprechender gesetzlicher Grundlage nicht in Betracht, sodass die bloße Berufung auf das laufende Zivilverfahren die Verweigerung der Auskunft nicht rechtfertigt. Die Möglichkeit der Akteneinsicht im **Zivilverfahren** "konsumiert" das datenschutzrechtliche Auskunftsrecht nicht, weil beide Rechte unterschiedlichen Zwecken dienen und nebeneinander bestehen.

Heimliche Tonaufnahmen sind aufgrund ihrer **hohen Eingriffsintensität** regelmäßig unzulässig, außer es wird ein "**Beweisnotstand**" geltend gemacht. Dies bedeutet im datenschutzrechtlichen Verfahren, dass hohe Anforderungen in Bezug auf die Erforderlichkeit erfüllt werden müssen. Zur Beweisführung gegen behauptete Lärmbelästigungen wäre die auf das Fußballspielen der Kinder beschränkte Aufnahme als **gelminderes Mittel** ausreichend gewesen. Die stimmliche Aufnahme des Nachbarn war hingegen überschießend, weshalb dessen Interesse an einer Auskunft die Geheimhaltungsinteressen der Nachbarin überwiegt.

Die Beauskunftung der **Datenkopie** ist eine Modalität der Auskunft, deren Form (etwa Auszüge oder Transkripte) der Verantwortlichen überlassen bleibt, solange eine originalgetreue und verständliche Reproduktion erfolgt.

DSB 06.08.2025, 2025-0.276.820

### **Leistungsauftrag, aufschiebende Wirkung, Geldbuße**

- Die DSB trug einer Website-Betreiberin auf, ihren Cookie-Banner innerhalb einer Frist von zehn Wochen so zu ändern, dass auf der ersten Ebene neben "**Akzeptieren**" eine optisch gleichwertige Option zum Schließen des Banners ohne Einwilligung

angeboten wird. Die Betreiberin erhob Beschwerde an das BVwG, das diese abwies. Die Betreiberin wandte sich sowohl an den VfGH als auch den VwGH. Der VfGH lehnte die Behandlung ab und trat die Rechtssache an den VwGH ab. Der VwGH wies die erhobene Revision zurück. Die Betreiberin kam dem Leistungsauftrag der DSB zwar nach, aber erst zehn Wochen nach dem Beschluss des VwGH. Die DSB verhängte wegen der nicht fristgerechten Befolgung ihrer Anweisung im Rahmen eines Verwaltungsstrafverfahrens eine **Geldbuße** iHv EUR 6.200 sowie EUR 620 Verfahrenskosten (10%), somit insgesamt EUR 6.820.

Die DSB hat erwogen: Die Betreiberin missachtete eine vollziehbare, verbindliche **Anweisung** der Aufsichtsbehörde gemäß Art 58 Abs 2 lit d DSGVO, indem sie den Cookie-Banner nicht entsprechend dem Leistungsspruchpunkt des Bescheids umsetzte. Bei solchen Anweisungen handelt es sich um vollstreckbare Verwaltungsakte mit Handlungsbefehl, die neben oder anstatt weiterer Abhilfemaßnahmen verhängt werden können.

Der Bescheidbeschwerde an das BVwG kam **aufschiebende Wirkung** zu. Die Erkenntnisbeschwerde an den VfGH und die Revision an den VwGH haben hingegen keine aufschiebende Wirkung. Die Leistungsfrist war daher ab Zustellung des abweisenden Erkenntnisses des BVwG zu berechnen. Die **Nichtbefolgung des Leistungsauftrags** nach Verstreichen dieser **Leistungsfrist** erfüllte den Tatbestand des Art 83 Abs 1 und 6 DSGVO iVm Art 58 Abs 2 lit d DSGVO.

**Verschulden** liegt bei Verstößen gegen die DSGVO bereits vor, wenn der Beschuldigte sich über die Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte. Für die **Strafbemessung** waren die EDSA-Leitlinien für Geldbußen sowie die **wirtschaftliche Leistungsfähigkeit** der Website-Betreiberin zu berücksichtigen. **Achtung:** Aufschiebende Wirkung kommt nur Bescheidbeschwerden automatisch zu. Mit der Erkenntnisbeschwerde an den VfGH und der Revision an den VwGH kann die aufschiebende Wirkung beantragt werden. Wird die aufschiebende Wirkung nicht beantragt oder nicht gewährt, wird das Erkenntnis des BVwG mit Zustellung (!) rechtskräftig und beginnt daher mit der Zustellung auch die Leistungsfrist zu laufen.

Anm: Seit dem hier verfahrensgegenständlichen Beschluss des VwGH hat der EuGH der ePrivacyRL gegenüber der DSGVO den Vorrang eingeräumt. Es erscheint daher fraglich, ob die DSB für die Erlassung des Leistungsauftrags zuständig war.

Aus der weiteren Rechtsprechung der DSB:

- Das **Grundrecht auf Datenschutz** gemäß Art 8 GRG sowie Art 16 AEUV und nach der DSGVO ist auf den Schutz **natürlicher Personen** beschränkt. Eine Ausnahme für **juristische Personen** besteht nur, wenn der Name einer natürlichen Person in der Firma der juristischen Person aufscheint. Den Mitgliedstaaten steht es offen, den durch die DSGVO gewährten Schutz auf juristische Personen auszudehnen. Das DSG enthält jedoch keine entsprechende Bestimmung. Juristische Personen sind daher nur durch **§ 1 DSG** geschützt. Eine auf die DSGVO gestützte Datenschutzbeschwerde einer juristischen Person ist zurückzuweisen ([DSB 08.10.2025, 2025-0.620.443](#)).
- Die Verarbeitung personenbezogener Daten für den Vertrieb und den Verbrauch von Antibiotika im **Veterinärbereich** ist rechtmäßig. Die behauptete – von der gesetzlichen Ermächtigung nicht gedeckte – **Datenweitergabe** konnte nicht festgestellt werden. Bei der **Nichtfeststellbarkeit** einer Tatsache ist von ihrem Nichtvorliegen auszugehen. Ein allgemeines Vorbringen, das aus Mutmaßungen besteht, läuft zudem auf einen unzulässigen **Erkundungsbeweis** hinaus ([DSB 30.09.2025, 2025-0.783.392](#)).

#### **EU-Rechtsakte**

- Am **23.12.2025** wurden der (i) "*Durchführungsbeschluss (EU) 2025/2571 der Kommission vom 19. Dezember 2025 zur Änderung des Durchführungsbeschlusses (EU) 2021/1773 der Kommission gemäß der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich*", [ABI L 2025/2571](#); sowie (ii) "*Durchführungsbeschluss (EU) 2025/2574 der Kommission vom 19. Dezember 2025 zur Änderung des Durchführungsbeschlusses (EU) 2021/1772 der Kommission gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich*", [ABI L 2025/2574](#), veröffentlicht. Diese Durchführungsbeschlüsse verlängern die **Geltungsdauer** der für das Vereinigte Königreich geltenden **Angemessenheitsbeschlüsse** vom 27.12.2025 bis zum **27.12.2031**. **Anm: Zu begrüßen ist, dass die Geltungsdauer der Angemessenheitsbeschlüsse nicht erneut um sechs Monate, sondern um sechs Jahre verlängert wurde. Das stärkt die Rechtssicherheit.**
- Am **23.12.2025** wurde der **Entwurf** der "*Commission Implementing Regulation ... setting out detailed arrangements for the*

*provision of a common data structure, standardised metadata, standardised authentication and common application programming interface for the European repository for online political advertisements in accordance with Regulation (EU) 2024/900 of the European Parliament and of the Council*", [Ares\(2025\)11556145](#), veröffentlicht. Diese DurchführungsVO legt Standards fest, um die Aufnahme **politischer Anzeigen** iSd [TTPW-VO \(EU\) 2024/900](#) ins **europäische Archiv** zu erleichtern.

#### **Nationale Rechtsakte**

- Am **23.12.2025** wurde das "*Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsystemsicherheitsgesetz 2026 – NISG 2026) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden*", [BGBl I 2025/94](#), kundgemacht. Das neue NISG 2026 setzt die [NIS-2-RL \(EU\) 2022/2555](#) ins innerstaatliche Recht um und führt die [VO \(EU\) 2021/887](#) zum Europäischen Kompetenzzentrum im Bereich der Cybersicherheit durch. Das NISG 2026 wird am **01.10.2026** in Kraft treten. Das TKG 2021 und das GTelG 2012 wurden an das NISG 2026 angepasst. **Anm: Nähere Informationen zum NISG 2026 finden Sie im Legal Insight Österreich: NISG 2026 – Alles, was Sie wissen müssen.**
- Am **23.12.2025** wurde eine Änderung des **Gesundheitstelematikgesetzes** 2012, [BGBl L 2025/93](#), kundgemacht. Die Änderung betrifft eine **Aufbewahrungsfrist**, die von zehn auf **dreißig Jahre** verlängert wird.

#### **Vorschau EuGH-Rechtsprechung**

- Am **22.01.2026** wird vor dem **EuGH** die **mündliche Verhandlung** in der Rs [C-205/25, Bayerisches Landesamt für Datenschutzaufsicht](#), stattfinden. Gegenstand des Verfahrens ist, ob eine **Datenschutz-Aufsichtsbehörde** aus Akten von vor ihr geführten Datenschutzbeschwerdeverfahren gemäß Art 15 DSGVO Auskunft erteilen muss und bejahendenfalls, ob diese Auskunftspflicht durch nationales Recht beschränkt werden kann.

# Rechtsprechungslinien

Mit diesen Rechtsprechungslinien wird ein Versuch unternommen, die Rechtsprechung der unterschiedlichen Behörden und Gerichte zu Datenschutz und Digitalisierung zu systematisieren. Ein Anspruch auf Vollständigkeit besteht nicht. Die Rechtsprechungslinien werden ständig weiterentwickelt und ggf auch berichtigt.

## Grundrecht auf Datenschutz

- Die DSGVO gilt nur für die Verarbeitung der Daten **natürlicher Personen**. Die Daten von **Unternehmern** können umfasst sein, wenn aufgrund ihres Namens (Firma) eine oder mehrere natürliche Personen bestimmt werden (die Bestimmbarkeit natürlicher Personen genügt nicht; [EuGH 09.11.2010, C-92/09, Schecke](#); [17.12.2015, C-419/14, WebMindLicenses](#); [18.06.2020, C-78/18, Kommission/Ungarn](#); [10.12.2020, C-620/19, J & S Service](#); [OGH 13.08.2025, 6Ob173/24w](#); [DSB 17.09.2025, 2025-0.746.087](#); [08.10.2025, 2025-0.620.443](#)).
- **Juristische Personen** dürfen eine Verletzung im Recht auf Geheimhaltung iSd § 1 DSG bei der DSB geltend machen, denn ihre **Wirtschaftsdaten** sind personenbezogene Daten ([VfSlg 12.228/1989](#); [19.673/2012](#), [20.674/2024](#); [18.12.2025, G105/2025](#); [BVwG 30.07.2024, W287 2254678-1](#); [BVwG 27.10.2025, W137 2290323-1](#); [DSB 21.11.2022, 2022-0.792.182](#); [26.04.2023, 2023-0.072.284](#); [DSB 29.07.2025, 2024-0.368.729](#); [17.09.2025, 2025-0.746.087](#) [08.10.2025, 2025-0.620.443](#)).
- Eine Datenverarbeitung im Einklang mit den anzuwendenden **Verfahrensgesetzen** ist zulässig ([BVwG 23.01.2024, W108 2250843-1](#); [BFG 06.01.2024, RV/7100970/2023](#); [26.09.2024, RV/5101151/2020](#); [07.10.2024, W108 2277566-1](#)).

## Betroffenenrechte

- Es gibt **kein Recht auf Feststellung** einer in der **Vergangenheit** liegenden Verletzung des **Rechts auf Auskunft** ([VwGH 06.03.2024, Ro 2021/04/0027](#); [BVwG 05.12.2023, W211 2260885-1](#); [05.12.2023, W211 2260885-1](#); [11.12.2023, W137 2233746-1](#); [11.02.2025, W254 2295624-1](#); [06.05.2025, W256 2307865-1](#); [10.06.2025, W274 2307868-1](#); [23.06.2025, W211 2291530-1](#); [25.06.2025, W254 2307864-1](#); [30.06.2025, W211 2307833-1](#); [14.08.2025, W298 2309032-1](#)). Dasselbe gilt für die **Gewährung des Informationszugangs** nach dem **IFG** ([BVwG 10.11.2025, W176 2322793-1](#)).
- Das "**Recht auf Kopie**" ist kein eigenständiges Recht. Die Ausfolgung einer Kopie von Auszügen aus Dokumenten oder Datenbanken ist nur dann erforderlich, wenn dies zur wirksamen Ausübung der Betroffenenrechte unerlässlich ist ([EuGH 04.05.2023, C-487/21, Österreichische Datenschutzbehörde](#); [26.10.2023, C-307/22, FT](#); [27.05.2024, C-312/23, Addiko Bank](#); [VwGH 03.08.2023, Ro 2020/04/0035](#); [BVwG 05.12.2023, W211 2261719-1](#); [22.01.2024, W252 2246156-1](#); [22.01.2024, W252 2247042-1](#); [23.02.2024, W211 2262850-2](#); [19.03.2024, W287 2239852-1](#); [12.04.2024, W108 2255217-1](#); [09.09.2024, W176 2283061-1](#); [09.01.2025, W256 2244544-1](#); [10.02.2025, W176 2285593-1](#); [04.09.2025, W252 2312918-1](#); [23.10.2025, W101 2268654-1](#); [DSB 14.10.2025, 2025-0.823.962](#); [DSB 15.12.2025, 2025-0.395.497](#)).
- Schreitet ein bevollmächtigter Vertreter für einen Auskunftswerber ein, ist in einem **zweistufigen Prüfungsverfahren** neben der Identität des Auskunftswerbers auch die **Vollmacht** zu

prüfen. Auch wenn ein **Rechtsanwalt** für den Auskunftswerber einschreitet, ist von **Verantwortlichen des privaten Bereichs** der urkundliche Nachweis der Bevollmächtigung zu fordern. Mit der **bloßen Berufung eines Rechtsanwalts auf eine Vollmacht** gemäß § 8 Abs 1 RAO kann die Bevollmächtigung nur beim Einschreiten vor einer Behörde oder vor einem Gericht nachgewiesen werden ([OLG Innsbruck 29.01.2024, 10R87/24f](#); [OLG Wien 10.01.2025, 33R157/24m](#); [11.02.2025, 4R5/25x](#); [11.02.2025, 3R5/25i](#); [11.04.2025, 16R21/25p](#); [OLG Linz 15.01.2025, 2R174/24g](#); [15.01.2025, 2R172/24p](#); [06.02.2025, 6R10/25w](#); [05.03.2025, 2R32/25a](#); [OLG Graz 17.01.2025, 5R205/24t](#); [14.03.2025, 5R28/25i](#)). **AA:** [DSB 01.10.2025, 2025-0.765.344](#).

- Eine zunächst unvollständige **Auskunft** kann im Laufe des Verfahrens vor der DSB und auch noch vor dem BVwG **vervollständigt** werden ([VwGH 06.03.2024, Ro 2021/04/0027](#); [BVwG 05.12.2023, W211 2260885-1](#); [19.03.2024, W287 2249380-1](#); [12.04.2024, W108 2255217-1](#); [31.01.2025, W258 2247059-1](#); [06.05.2025, W256 2307865-1](#); [10.06.2025, W274 2307868-1](#); [30.06.2025, W211 2307833-1](#); [10.06.2025, W274 2307868-1](#)).
- **Kein Recht auf Feststellung** einer in der **Vergangenheit** liegenden Verletzung des **Rechts auf Löschung** (VwGH 10.12.2024, Ro 2021/04/0022; [BVwG 22.01.2024, W101 2134867-1](#); [19.04.2024, W287 2276988-1](#); [20.06.2024, W211 2225136-1](#); [31.01.2025, W258 2247059-1](#); [03.02.2025, W292 2285575-1](#)). Dasselbe gilt für das **Recht auf Berichtigung** ([BVwG 23.04.2024, W605 2283487-1](#)).
- Eine auf **Löschung** gerichtete **Revision** ist auch dann **wegen nachträglichen Wegfalls des rechtlichen Interesses** als gegenstandslos geworden zu erklären, wenn die Löschung erst nach Entscheidung durch das BVwG erfolgt ([VwGH 24.07.2024, Ro 2023/04/0001](#); [24.07.2024, Ra 2023/04/0270](#); [30.09.2024, Ro 2022/04/0033](#)).

## Schadenersatz

- Der Ersatz eines immateriellen Schadens hängt von keiner **Erheblichkeitsschwelle** ab. Der **bloße Verstoß** gegen die Bestimmungen der DSGVO **reicht jedoch nicht aus**, um einen Schadenersatzanspruch zu begründen. Ein solcher Verstoß führt **nicht automatisch** zu einem Schaden. Der Betroffene hat den entstandenen Schaden **nachzuweisen** ([EuGH 04.05.2023, C-300/21, Österreichische Post](#); [14.12.2023, C-340/21, Natsionalna agentsia](#); [14.12.2023, C-456/22, Gemeinde Ummendorf](#); [21.12.2023, C-667/21, Krankenversicherung Nordrhein](#); [25.01.2024, C-687/21, MediaMarktSaturn](#); [20.06.2024, C-182/22, Scalable Capital](#); [20.06.2024, C-590/22, PS \(Adresse erronée\)](#); [04.09.2025, C-655/23, Quirin Privatbank](#); [EuG 08.01.2025, T-354/22, Bindl/Kommission](#); [OGH 03.07.2025, 6Ob113/24x](#)).
- Die (objektiven) Voraussetzungen des immateriellen Schadenersatzes sind: (i) ein **Verstoß gegen die DSGVO**, (ii) der **Eintritt eines Schadens** und (iii) ein **Kausalzusammenhang zwischen dem Verstoß und den Schaden** ([EuGH 04.05.2023, C-300/21, Österreichische Post](#); [14.12.2023, C-340/21, Natsionalna agentsia](#); [14.12.2023, C-456/22, Gemeinde Ummendorf](#); [21.12.2023, C-667/21, Krankenversicherung Nordrhein](#); [25.01.2024, C-687/21, MediaMarktSaturn](#); [05.03.2024, C-755/21 P, Kočner/Europol](#); [11.04.2024, C-741/21, juris](#); [20.06.2024, C-182/22, Scalable Capital](#); [20.06.2024, C-590/22, PS \(Adresse erronée\)](#); [04.10.2024, C-507/23, Patērētāju tiesību aizsardzības centrs](#)).
- Das Haftungsregime des Art 82 DSGVO setzt weiters **Verschulden** voraus, das vermutet wird (**Beweislastumkehr**). Der **Grad des Verschuldens** ist bei der Bemessung der Höhe der Entschädigung nicht zu berücksichtigen ([EuGH 21.12.2023, C-667/21, Krankenversicherung](#)



[Nordrhein; 25.01.2024, C-687/21, MediaMarktSaturn; 20.06.2024, C-182/22, Scalable Capital; 04.09.2025, C-655/23, Quirin Privatbank](#)).

- Der Schadenersatz nach Art 82 Abs 1 DSGVO hat **keine Straf- oder Abschreckungsfunktion**, sondern ausschließlich eine **Ausgleichsfunktion** ([EuGH 04.05.2023, C-300/21, Österreichische Post; 21.12.2023, C-667/21, Krankenversicherung Nordrhein; 25.01.2024, C-687/21, MediaMarktSaturn; 11.04.2024, C-741/21, juris; 20.06.2024, C-182/22, Scalable Capital; 20.06.2024, C-590/22, PS \(Adresse erronée\); 04.10.2024, C-507/23, Patērētāju tiesību aizsardzības centrs; OGH 03.07.2025, 6Ob113/24x](#)).
- Die **Schwere des Verstoßes** gegen eine Bestimmung der DSGVO wirkt sich auf die **Höhe** des zu gewährenden Schadenersatzes **nicht** aus ([EuGH 04.10.2024, C-507/23, Patērētāju tiesību aizsardzības centrs; 04.09.2025, C-655/23, Quirin Privatbank](#)).
- Die **Haltung und die Beweggründe des Verantwortlichen** sind **nicht** zu berücksichtigen ([EuGH 04.10.2024, C-507/23, Patērētāju tiesību aizsardzības centrs; 04.09.2025, C-655/23, Quirin Privatbank](#)).

## Verwaltungsstrafrecht

- Das **Verschulden** ist **unionsautonom** auszulegen und liegt stets vor, wenn der Beschuldigte über die **Rechtswidrigkeit seines Verhaltens nicht im Unklaren** sein konnte (dies gilt für natürliche und juristische Personen). Auf ein **mangelndes Organisationsverschulden** kommt es nicht an ([BVwG 25.10.2024, W108 2285546-1; 17.10.2024, W176 2284816-1; 26.02.2025, W101 2284403-1; 20.06.2025, W291 2300813-1; DSB 07.12.2023, 2023-0.637.760; 07.12.2023, 2023-0.583.644; 11.12.2023, 2023-0.789.858; 12.12.2023, 2023-0.603.142; 16.08.2024, 2023-0.680.196; 07.10.2024, 2024-0.671.673; 03.06.2025, 2025-0.177.424; 06.08.2025, 2025-0.276.820; 04.09.2025, 2025-0.699.550; 29.09.2025, 2025-0.682.666; 18.11.2025, 2025-0.902.556](#)). Einzelne Senate des BVwG prüfen das Organisationsverschulden ([BVwG 26.03.2024, W137 2241630-1; 27.12.2024, W258 2227269-1; 25.07.2025, W258 2299744-1](#)).
- Die Regelungen des **§ 5 VStG (Verschulden)** gelangen aufgrund des Anwendungsvorrangs des Unionsrechts nicht zur Anwendung ([BVwG 27.03.2024, W214 2243436-1; 03.06.2024, W292 2282284-1; 15.07.2024, W298 2284627-1; 17.09.2024, W298 2295130-1; 27.03.2025, W298 2285480-1](#)).

## Verfahrensrecht

- Die **zuständige Behörde** für Beschwerden wegen Verstößen gegen das Datenschutzrecht ist die DSB ([BVwG 12.12.2023, W122 2270105-1; LVwG NÖ 01.12.2023, LVwG-M-55/001-2022; 23.09.2025, LVwG-M-32/001-2025; LVwG Burgenland 08.01.2024, E 263/07/2023.001/018; LVwG Wien 23.02.2024, VGW-101/032/11502/2023](#)).
- **Unterlässt** die DSB die Durchführung eines **ordnungsgemäßen Ermittlungsverfahrens**, setzt die DSB nur völlig ungeeignete Ermittlungsschritte oder ermittelt die DSB bloß ansatzweise, darf das BVwG die Angelegenheit zum Erlassen eines neuen Bescheids an die DSB **zurückverweisen** ([VwGH 21.12.2023, Ra 2023/04/0254; 19.04.2024, Ra 2022/04/0006; 06.06.2024, Ra 2023/04/0280; BVwG 15.11.2023, W292 2259252-1; 20.12.2023, W108 2254815-1; 25.09.2024, W108 2284790-1; 18.11.2024, W274 2291293-1](#)).
- In einem Verfahren zur Feststellung der **federführenden Aufsichtsbehörde** wird **keine Vorfrage iSd § 38 AVG** verbindlich beantwortet, weshalb für einen Aussetzungsbescheid

keine Rechtsgrundlage vorhanden ist ([VwGH 14.11.2023, Ro 2020/04/0009](#); [06.09.2024, Ro 2023/04/0006](#); [BVwG 13.12.2023, W287 2256142-1](#); [13.12.2023, W287 2256386-1](#); [04.01.2024, W298 2278490-1](#); [14.02.2024, W221 2280746-1](#); [04.04.2024, W211 2280745-1](#); [04.04.2024, W211 2278962-1](#); [17.04.2024, W298 2281864-1](#); [08.07.2024, W137 2280182-1](#)).

- Eine Datenschutzbeschwerde, die nach Ablauf der **subjektiven Präklusivfrist** von einem Jahr eingebracht wird, ist wegen Präklusion zurückzuweisen ([BVwG 15.12.2023, W108 2273800-1](#); [05.04.2024, W211 2274025-1](#); [17.04.2024, W298 2274023-1](#); [20.09.2024, W214 2291552-1](#); [25.09.2024, W108 2287986-1](#)).
- Wird eine zulässige und begründete **Säumenisbeschwerde** an das BVwG erhoben, darf das BVwG aufgrund seiner sog. "**kondemnatorischen**" **Entscheidungsbefugnis** die DSB zum Erlass eines Bescheids "verurteilen". Damit wird der DSB eine "**dritte Chance**" zur Bescheiderlassung eingeräumt ([BVwG 13.02.2024, W256 2280818-1](#); [13.06.2024, W292 2281684-1](#); [18.11.2024, W137 2297602-1](#)).
- Weist die DSB eine Datenschutzbeschwerde zurück, spricht das BVwG nur über die **Rechtmäßigkeit der Zurückweisung** ab ([BVwG 22.01.2024, W101 2277417-1](#); [30.04.2024, W252 2272830-1](#); [03.06.2024, W211 2273051-1](#); [18.06.2024, W214 2222613-2](#); [22.07.2024, W211 2286882-1](#)).
- Die **Zurückziehung der Datenschutzbeschwerde**, während das Verfahren beim BVwG anhängig ist, führt zur (**rückwirkenden**) **Unzuständigkeit** der DSB. Dadurch wird der Bescheid der DSB (**nachträglich**) **rechtswidrig** und ist vom BVwG zu beheben ([BVwG 16.01.2024, W211 2280187-1](#); [16.01.2024, W292 2248304-1](#); [27.02.2024, W221 2265528-2](#); [19.03.2024, W252 2271599-1](#); [06.06.2024, W287 2268623-1](#); [12.06.2024, W108 2280177-1](#); [21.08.2024, W214 2257555-1](#); [06.09.2024, W292 2247490-1](#); [16.09.2024, W287 2248646-1](#); [16.09.2024, W137 2262841-1](#); [16.09.2024, W137 2263387-1](#); [16.09.2024, W137 2257622-1](#); [30.09.2024, W211 2271492-1](#); [04.10.2024, W211 2272474-1](#); [05.09.2025, W256 2294340-1](#)).

## Strafgerichte

- Gelangt der Inhalt einer **verschlüsselten Kommunikation** im **Rechtshilfeweg** in das Ermittlungsverfahren der Staatsanwaltschaft, unterliegen die von ausländischen Behörden übermittelten Kommunikationsdaten **keinem Beweisverwertungsverbot** ([OGH 17.07.2024, 11Os55/24h](#); [05.11.2024, 14Os14/24a](#); [05.11.2024, 14Os100/24y](#); [OGH 18.02.2025, 14Os11/25m](#); [16.12.2025, 11Os43/25w](#)). Beachte aber [OGH 05.11.2024, 14Os107/24b](#).

# Rechtsprechungsübersicht 2024

Die Reihung der Entscheidungen richtet sich nach dem Erscheinungsdatum, weil die Entscheidungen in dieser Reihenfolge für den Schönherr Datenschutzmonitor 2024 erfasst wurden.

## EGMR

| Entscheidung  | Stichworte  |
|---|---|
| EGMR 11.01.2024, 42541/18, <i>Tena Arregui/Spanien</i>            | Überwachung der E-Mail-Korrespondenz                            |
| EGMR 13.02.2024, 33696/19, <i>Podchasov/Russland</i>              | Telegram, Vorratsdatenspeicherung, Ende-zu-Ende Verschlüsselung |
| EGMR 22.02.2024, 16974/14, <i>Kaczma-rek/Polen</i>                | Telefonüberwachung  |
| EGMR 28.05.2024, 72038/17, <i>Pietrzak/Polen</i>                  | Geheime Überwachung, Vorratsdatenspeicherung                    |
| EGMR 23.05.2024, 2507/19, <i>Contrada/Italien</i>                 | Telefonüberwachung, Mafia                                       |
| EGMR 06.06.2024, 36559/19, <i>Bershe-da/Monaco</i>                | Mobiltelefon, Anwaltsgeheimnis                                  |
| EGMR 20.06.2024, 8826/20, <i>Namaz-li/Azerbaidzhan</i>            | Überwachung, Anwaltsgeheimnis                                   |
| EGMR 25.06.2024, 23215/21, <i>Vlaisavljevskj/Nordmazedonien</i>   | Energieversorgung, öffentliche Daten                            |
| EGMR 28.11.2024, 31091/16, <i>Csikos/Ungarn</i>                   | Telefonüberwachung, Journalismus                                |
| EGMR 03.12.2024, 28935/21, <i>MSD/Rumänien</i>                    | Online-Gewalt, Schadenersatz                                    |
| EGMR 19.12.2024, 29550/17, <i>Grande Oriente D'italia/Italien</i> | Durchsuchung und Beschlagnahme, juristische Person              |

## EuGH (Urteile und Schlussanträge)

| Entscheidung  | Stichworte   |
|---|--|
| EuGH 11.01.2024, C-231/22, <i>Belgischer Staat</i>                  | Rollenverteilung, öffentliche Stelle                           |
| EuGH 16.01.2024, C-33/22, <i>Österreichische Datenschutzbehörde</i> | BVT-Untersuchungsausschuss, Anwendungsbereich, Gewaltenteilung |

|   |  |
|---|--|
| EuGH 25.01.2024, C-687/21, <i>MediaMarktSaturn</i>                                      | Immaterieller Schaden, hypothetisches Risiko   |
| EuGH Schlussanträge 25.01.2024, C-757/22, <i>Meta Platforms</i>                         | Verbraucherschutzeinrichtung   |
| EuGH 30.01.2024, C-118/22, <i>Direktor na Glavna direksia „Natsionalna politsia“</i>    | DSRL-PJ 2016/680   |
| EuGH Schlussanträge vom 22.02.2024, C-693/22, I. ( <i>Vente d'une base de données</i> ) | Verkauf einer Datenbank mit personenbezogenen Daten                                      |
| EuGH 07.03.2024, C-604/22, <i>IAB Europe</i>  | Personenbezug, Rollenverteilung, Cookies   |
| EuGH 05.03.2024, C-755/21P, <i>Kočner/Europol</i>                                       | Schadenersatz, Data Breach   |
| EuGH 07.03.2024, C-740/22, <i>Endemol Shine Finland</i>                                 | Mündliche Verarbeitung, Dateisystem, Wahrnehmung einer Aufgabe im öffentlichen Interesse |
| EuGH 07.03.2024, C-479/22P, <i>OC/Kommission</i>  | Personenbezug, Identifizierung   |
| EuGH 14.03.2024, C-46/23, <i>Újpesti Polgármesteri Hivatal</i>                          | Amtswegige Löschungsbefugnis   |
| EuGH 21.03.2024, C-61/22, <i>Landeshauptstadt Wiesbaden</i>                             | Fingerabdruck, Rechtmäßigkeitsprüfung, Primärrechtswidrigkeit                            |
| EuGH Schlussanträge 11.04.2024, C-768/21, <i>Land Hessen</i>                            | Abhilfebefugnisse der Aufsichtsbehörden  |
| EuGH 11.04.2024, C-741/21, <i>juris</i>   | Immaterieller Schadenersatz  |
| EuGH Schlussanträge 25.04.2024, C-446/21, <i>Schrems/Meta</i>                           | Verhaltensorientierte Werbung, Datenminimierung, veröffentlichte sensible Daten          |
| EuGH Schlussanträge 25.04.2024, C-21/23, <i>Lindenapotheke</i>                          | Unlauterer Wettbewerb, sensible Daten  |
| EuGH 30.04.2024, C-470/21, <i>La Quadrature du Net II</i>                               | Urheberrechtsverletzung, IP-Adresse  |
| EuGH 30.04.2024, C-178/22, <i>Procura della Repubblica</i>                              | Staatsanwaltschaft, Telekomdaten, schwere Straftat                                       |
| EuGH 30.04.2024, C-670/22, <i>M.N. (EncroChat)</i>                                      | Überwachung, Europäische Ermittlungsanordnung  |

|   |  |
|---|--|
| EuGH 07.05.2024, C-115/22, <i>NADA</i>  | Anti-Doping-Behörde, kein "Gericht" iSd Art 267 AEUV                                     |
| EuGH 27.05.2024, C-312/23, <i>Addiko Bank</i>                                       | Datenkopie, Anfragezweck, Auskunftsumfang  |
| EuGH Schlussanträge 30.05.2024, C-200/23, <i>Agentsia po vpisvaniyata</i>           | Handelsregister, Rollenverteilung, Löschung  |
| EuGH Schlussanträge 06.06.2024, C-169/23, <i>Masdi</i>                              | Informationspflicht, generierte Daten  |
| EuGH 13.06.2024, C-229/23, <i>HYA ua II</i>   | Überwachung, Begründungspflicht  |
| EuGH Schlussanträge 13.06.2024, C-80/23, <i>Ministerstvo na vatreshnite raboti</i>  | Polizeiakte, biometrische und genetische Daten   |
| EuGH 20.06.2024, C-182/22 und C-189/22, <i>Scalable Capital</i>                     | Schadenersatz, Data Breach   |
| EuGH 20.06.2024, C-590/22, <i>PS (Adresse erronée)</i>                              | Schadenersatz, Fehlzustellung  |
| EuGH 11.07.2024, C-757/22, <i>Meta</i>  | Informationspflicht, Verbraucherschutz-einrichtung                                       |
| EuGH 11.07.2024, C-461/22, <i>MK</i>  | Erwachsenenvertretung, Anwendungsbereich, Verantwortlicher                               |
| EuGH Schlussanträge 11.07.2024, C-394/23, <i>Mousse</i>                             | Anredatedaten, berechtigtes Interesse, Widerspruchsrecht                                 |
| EuGH 29.07.2024, C-623/22, <i>Belgian Association of Tax Lawyers</i>                | DAC 6, Steuergestaltung, Meldepflicht  |
| EuGH Schlussanträge 05.09.2024, C-416/23, <i>Österreichische Datenschutzbehörde</i> | Exzess, Rechtsmissbrauch, Ermessen   |
| EuGH 12.09.2024, C-17/22 ua, <i>HTB Neunte Immobilien</i>                           | Gesellschaftsrecht, Rechtsgrundlagen, vertragliche Verpflichtung, berechnigte Interessen |
| EuGH Schlussanträge 12.09.2024, C-203/22, <i>Dun &amp; Bradstreet</i>               | automatisierte Entscheidung, Bonität, Auskunft   |
| EuGH Schlussanträge 12.09.2024, C-383/23, <i>ILVA</i>                               | Geldbuße, Unternehmensbegriff, Verhältnismäßigkeit                                       |
| EuGH Schlussanträge 12.09.2024, C-247/23, <i>Deldits</i>                            | Transgender, Berichtigung, Register  |

|   |  |
|---|--|
| EuGH 26.09.2024, C-768/21, <i>Land Hessen</i>   | Aufsichtsbehörde, Aufsichtsbefugnisse, Ermessen, subjektives Recht, Geldbuße           |
| EuGH 04.10.2024, C-446/21, <i>Schrems III</i>   | Personalisierte Online-Werbung, Datenminimierung, sensible Daten                       |
| EuGH 04.10.2024, C-507/23, <i>Patērētāju tiesību aizsardzības centrs</i>  | Immaterieller Schaden, Entschuldigung  |
| EuGH 04.10.2024, C-21/23, <i>Lindenapotheke</i>   | Apotheke, Mitbewerber, Unterlassungsklage, Gesundheitsdaten                            |
| EuGH 04.10.2024, C-621/22, <i>Koninklijke Nederlandse Lawn Tennisbond</i>   | Interessenabwägung, wirtschaftliche Interessen   |
| EuGH 04.10.2024, C-200/23, <i>Agentsia po vpisvanyata</i>   | Handelsregister, Rollenverteilung, immaterieller Schaden                               |
| EuGH 04.10.2024, C-548/21, <i>Bezirkshauptmannschaft Landeck</i>  | StPO, Mobiltelefon, Auswertung   |
| EuGH 17.10.2024, C-302/23, <i>Jarocki</i>   | eIDAS-Verordnung   |
| EuGH 21.11.2024, C-336/23, <i>Hrvatska pošta</i>  | PSI 2-RL, Dokumentenzugang   |
| EuGH 28.11.2024, C-169/23, <i>Masdi</i>   | Informationspflicht, Ausnahme, Datenquelle, Datengenerierung                           |
| EuGH 28.11.2024, C-80/23, <i>Ministerstvo</i>   | DSRL-PJ 2016/680, biometrische und genetische Daten                                    |
| EuGH 12.12.2024, C-587/21P, <i>DD/FRA</i> ; 12.12.2024, C-130/22P, <i>DD/FRA</i> ; 12.12.2024, C-680/22P, <i>DD/FRA</i> | EU-Beamte  |
| EuGH 19.12.2024, C-65/23, <i>K GmbH</i>   | Kollektivvereinbarung, Betriebsvereinbarung, gerichtliche Kontrolle, Anwendungsvorrang |

## EuG

| Entscheidung   | Stichworte                                       |
|--|--|
| EuG 24.04.2024, T-205/22, <i>Naass und Sea-Watch/Frontex</i> | Zugang zu amtlichen Dokumenten                   |
| EuG 08.05.2024, T-375/22, <i>Izuzquiza</i>                   | Zugang zu Dokumenten des Europäischen Parlaments |

|   |   |
|---|---|
| EuG 17.07.2024, T-1077/23, <i>Bytedance</i> | DMA, Torwächter                           |
| EuG 17.07.2024, T-761/21, <i>Courtois</i>   | COVID, Dokumentenzugang                   |
| EuG 17.06.2024, T-546/23, <i>WS/EDSB</i>    | Auskunft, Logfiles, immaterieller Schaden |

#### VfGH

| Entscheidung                | Stichworte  |
|-----------------------------|---|
| VfGH 12.03.2024, E3436/2023 | Juristische Person, Investorenwarnung, Zuständigkeit                            |
| VfGH 03.10.2024, E4003/2023 | Videoüberwachung, Verschleierungsverbot   |
| VfGH 24.09.2024, UA17/2024  | COFAG-Untersuchungsausschuss, Informationsordnungsgesetz, Persönlichkeitsrechte |

#### VwGH

| Entscheidung   | Stichworte   |
|--|--|
| VwGH 27.11.2023, Ra 2023/04/0221; Ra 2023/04/0224; Ra 2023/04/0248 | Vorfrage iSd § 38 AVG  |
| VwGH 30.11.2023, Ro 2023/04/0043                                   | Zurückweisung, federführende Aufsichtsbehörde  |
| VwGH 11.12.2023, Ra 2021/04/0095                                   | Zulässigkeitsgründe, Parteienerklärung   |
| VwGH 14.12.2023, Ra 2023/13/0054                                   | Kontenregister, Rechtswidrigkeit infolge Unzuständigkeit   |
| VwGH 21.12.2023, Ra 2023/04/0254                                   | Materielle Wahrheit, Zurückverweisung  |
| VwGH 21.12.2023, Ro 2021/04/0010                                   | Arbeitsmarktchancen-Assistenzsystem, Privatwirtschaftsverwaltung, Gesetzesqualität, Profiling, automatisierte Entscheidung |
| VwGH 01.02.2024, Ro 2020/04/0031                                   | Insolvenzdaten, Speicherfrist, Bankenwarnliste   |
| VwGH 01.02.2024, Ra 2021/04/0088                                   | Justizielle Tätigkeit, Gerichtsvollzieher, Kassation   |
| VwGH 01.02.2024, Ro 2020/04/0016                                   | Staatsanwaltschaft, Zuständigkeit  |
| VwGH 01.02.2024, Ro 2021/04/0006                                   | BVT-Untersuchungsausschuss, Zuständigkeit  |

|  |  |
|--|--|
| VwGH 01.02.2024, Ro 2021/04/0016                                 | Immobilienentwicklung, Werbung, Einwilligung   |
| VwGH 01.02.2024, Ra 2020/04/0187                                 | Geldbuße, juristische Person   |
| VwGH 01.02.2024, Ro 2021/04/0013                                 | Rufdatenerhebung, Verständigung der "Betroffenen"                                      |
| VwGH 28.02.2024, Ro 2024/04/0001;<br>28.02.2024, Ro 2023/04/0032 | Scoring, Aussetzung  |
| VwGH 06.03.2024, Ro 2021/04/0030                                 | Kreditauskunftei, Feststellungskompetenz, Beschwerderecht, Informationspflicht         |
| VwGH 02.04.2024, Ro 2021/04/0008                                 | Kreditauskunftei, Scoring, Profiling   |
| VwGH 06.03.2024, Ro 2021/04/0037                                 | Zeitlicher Anwendungsbereich, Auskunft   |
| VwGH 06.03.2024, Ro 2021/04/0027                                 | Feststellungskompetenz, Auskunft   |
| VwGH 08.04.2024, Ra 2022/04/0056                                 | Sozialversicherungsrechtliches Geburtsdatum, Beschränkung des Berichtigungsrechts      |
| VwGH 02.04.2024, Ro 2021/04/0018                                 | Unzulässigkeit der Revision  |
| VwGH 04.03.2024, Ra 2024/04/0010                                 | Aufschiebende Wirkung  |
| VwGH 19.04.2024, Ra 2022/04/0006                                 | Materielle Wahrheit, ergänzungsbedürftiger Sachverhalt                                 |
| VwGH 19.04.2024, Ra 2024/04/0303                                 | Staatsanwaltschaft, Strafgericht, Akteneinsicht  |
| VwGH 22.04.2024, Ro 2022/04/0038                                 | Bonitätsdaten, Speicherfrist   |
| VwGH 17.05.2024, Ro 2022/04/0026                                 | Bewertungsplattform, Hotelbetreiber  |
| VwGH 28.05.2024, Ro 2021/04/0034                                 | Kreditauskunftei, Geschäftsführer, Bonität   |
| VwGH 17.05.2024, Ra 2023/04/0005                                 | Sinus-Geo-Milieus, statistische Wahrscheinlichkeitswerte, weltanschauliche Überzeugung |
| VwGH 06.06.2024, Ra 2022/04/0008                                 | Ermittlungspflicht, Zurückverweisung   |
| VwGH 06.06.2024, Ra 2023/04/0280                                 | Voller Beweis, Zurückverweisung  |
| VwGH 06.06.2024, Ra 2023/04/0004;<br>Ra 2023/04/0006             | Zurückziehung der Datenschutzbeschwerde im Verfahren vor dem VwGH nicht möglich        |
| VwGH 13.06.2024, Ra 2023/04/0259                                 | Zurückverweisung   |



|   |  |
|---|--|
| VwGH 17.05.2024, Ra 2021/04/0009                    | Vorlagefrage, Identität des Streitgegenstandes                       |
| VwGH 25.06.2024, Ra 2022/04/0167                    | Staatsanwaltschaft, funktionelle Unzuständigkeit, Kognitionsbefugnis |
| VwGH 24.07.2024, Ro 2023/04/0001; Ra 2023/04/0270   | Kreditauskunftei, Löschung, Einstellung                              |
| VwGH 24.07.2024, Ra 2024/04/0376                    | Einzelfallbezogene Interessenabwägung                                |
| VwGH 02.08.2024, Ra 2022/04/0161                    | Auskunft, Klaglosstellung, kein Aufwandersatz                        |
| VwGH 03.09.2024, Ro 2022/04/0031                    | Schule, Art 6 Abs 1 lit e DSGVO, Interessenabwägung                  |
| VwGH 03.09.2024, Ra 2023/04/0042                    | AMS, Speicherbegrenzung, Rechtsansprüche                             |
| VwGH 03.09.2024, Ra 2023/04/0092; Ra 2023/04/0107ua | Beschwerdegegner   |
| VwGH 06.09.2024, Ro 2023/04/0006                    | Aussetzung, Kohärenzverfahren  |
| VwGH 30.09.2024, Ro 2022/04/0033                    | Löschungersuchen, Klaglosstellung, kein Kostenzuspruch               |
| VwGH 16.10.2024, Ra 2022/04/0151                    | Bewerbungsdaten, Löschung  |
| VwGH 16.10.2024, Ra 2022/04/0140                    | Behörde, Veröffentlichung einer Stellungnahme                        |
| VwGH 09.10.2024, Ra 2024/06/0161                    | Mitwirkungspflicht im Verwaltungsstrafverfahren                      |
| VwGH 31.10.2024, Ra 2022/04/0145                    | Mandatsbescheid, Vorstellungsbescheid, Revision                      |
| VwGH 24.10.2024, Ra 2023/05/0006                    | AuskunftspflichtG, Verschwiegenheit, social watchdog                 |
| VwGH 15.11.2024, Ro 2022/04/0028                    | Beschwerdevorentscheidung, Vorlageantrag, Aussetzungsbescheid        |
| VwGH 19.11.2024, Ro 2022/04/0016                    | Exzess, Aussetzung   |

## OGH

| Entscheidung               | Stichworte                            |
|----------------------------|---------------------------------------|
| OGH 20.12.2023, 6Ob206/23x | Immaterieller Schaden, Medienprivileg |

|   |   |
|---|---|
| OGH 20.12.2023, 6Ob205/23z                            | Koppelungsverbot, Transparenzgebot                                  |
| OGH 11.01.2024, 12Os127/23b                           | Erneuerungsverfahren, private Beweismittel                          |
| OGH 19.12.2023, 5Ob34/23w                             | Kleinkreditevidenz, Bankenwarnliste                                 |
| OGH 20.12.2023, 6Ob29/23t                             | Offenlegungspflichten, UGB  |
| OGH 17.01.2024, 6Ob143/23g                            | Doppelgleisigkeit, DSB  |
| OGH 17.01.2024, 6Ob38/23s                             | Verbandsklage, Scoring  |
| OGH 05.02.2024, 8Bs33/24z                             | Sicherstellung und Auswertung eines Mobiltelefons                   |
| OGH 15.02.2024, 8ObA72/23f                            | Dienstpflichtverletzung   |
| OGH 21.02.2024, 6Ob236/23h                            | Medienprivileg, Gerichtszuständigkeit                               |
| OGH 26.04.2024, 6Ob210/23k                            | Schadenersatz, "Shitstorm", Bildnisschutz                           |
| OGH 15.05.2024, 6Ob20/24w                             | GOG, Präzisierungspflicht   |
| OGH 15.05.2024, 6Ob43/24b                             | Schadenersatz   |
| OGH 15.05.2024, 6Ob70/24y                             | Schadenersatz, Versicherung   |
| OGH 25.06.2024, 4Ob102/23p                            | Bonus Club, Daten als Entgelt                                       |
| OGH 17.07.2024, 11Os55/24h                            | Verschlüsselte Kommunikation  |
| OGH 17.07.2024, 11Os20/24m                            | Verkehrsdaten, Lösungsfrist   |
| OGH 09.07.2024, 10ObS11/24a                           | Legitimität, sozialversicherungsrechtliches Geburtsdatum            |
| OGH 24.07.2024, 1Ob87/24m                             | Negativfeststellung, Schadenersatz, taugliches Beweisthema          |
| OGH 27.08.2024, 11Os85/24w                            | Überwachung, Kommunikationsdaten                                    |
| OGH 26.08.2024, 502Präs26/24d                         | Amtshaftung, feste Geschäftsverteilung, negativer Kompetenzkonflikt |
| OGH 27.08.2024, 6Ob159/23k und 27.08.2024, 6Ob217/23i | Unterlassungsanspruch, Aussetzung                                   |

|  |   |
|--|---|
| OGH 27.08.2024, 6Ob233/23t                         | Erstkopie, Krankengeschichte, Beschränkung von Betroffenenrechten, Verhältnismäßigkeit              |
| OGH 27.08.2024, 6Ob37/24w                          | Unterlassungsanspruch, Aussetzung   |
| OGH 28.08.2024, 7Ob95/24g                          | Bank, Transaktionsüberwachungssystem  |
| OGH 24.09.2024, 11Os75/24z; 24.09.2024, 11Os74/24b | StPO, Beschränkung der Akteneinsicht  |
| OGH 20.09.2024, 6Ob112/24z                         | Unterlassungsanspruch, Aussetzung   |
| OGH 20.09.2024, 6Ob164/24x                         | Bewertungsausspruch bei Datenschutzverletzungen   |
| OGH 24.09.2024, 11Os76/24x                         | StPO, Beschränkung der Akteneinsicht  |
| OGH 20.09.2024, 6Ob219/23h                         | Unterlassungsanspruch, Aussetzung   |
| OGH 20.09.2024, 6Ob221/23b                         | Google-Bewertungen, Zuständigkeit, Herkunftslandprinzip, Rollenverteilung, Datentransfer in die USA |
| OGH 08.10.2024, 14Os26/24s                         | Amtsgeheimnis, Amtsmissbrauch, Strafverfolgung  |
| OGH 22.10.2024, 4Ob109/24v                         | Schadenersatz   |
| OGH 05.11.2024, 14Os107/24b                        | Sky-ECC, EncroChat, Beweisverwertungsverbot   |
| OGH 05.11.2024, 14Os14/24a                         | ANOM, SKY ECC, Verwertungsverbot  |
| OGH 13.11.2024, 11Os129/24s                        | SKY ECC, Vollstreckungshindernis  |
| OGH 05.11.2024, 14Os100/24y                        | SKY ECC, Verwertungsverbot  |
| OGH 13.11.2024, 15Os51/24z                         | Persönlichkeitsrecht, Identifizierbarkeit   |
| OGH 28.10.2024, 3Ob191/24w                         | Smart Meter   |
| OGH 06.11.2024, 6Ob195/24f                         | Unterlassungsanspruch, Aussetzung   |

### **BVwG (ausgewählte Entscheidungen)**

| <b>Entscheidung</b>             | <b>Stichworte</b>             |
|---------------------------------|-------------------------------|
| BVwG 15.11.2023, W292 2259252-1 | Cookies, Ermittlungsverfahren |

|                                 |   |
|---------------------------------|---|
| BVwG 11.12.2023, W137 2276371-1 | Geldwäscheverdacht  |
| BVwG 14.12.2023, W256 2232894-1 | Rollenverteilung, Behörde   |
| BVwG 29.11.2023, W214 2233132-1 | Datenempfänger, Dokumentation   |
| BVwG 01.12.2023, W108 2265844-1 | Einwilligung, TKG   |
| BVwG 04.01.2024, W298 2266986-1 | Geltendmachung von Rechtsansprüchen, Übermaßverbot                                    |
| BVwG 14.12.2023, W287 2259251-1 | Zahlungserfahrungsdaten   |
| BVwG 20.12.2023, W211 2261679-1 | Dienstverhältnis  |
| BVwG 11.01.2024, W258 2243523-1 | Grundbuch, Löschung   |
| BVwG 18.01.2024, W137 2237426-1 | Privatdetektiv, Foto  |
| BVwG 22.01.2024, W211 2263717-1 | technische Daten, kein Personenbezug  |
| BVwG 09.01.2024, W256 2246709-1 | Form der Auskunft, Datenportabilität  |
| BVwG 22.01.2024, W252 2246156-1 | Dokumentenkopie, Anwaltsgeheimnis   |
| BVwG 22.01.2024, W252 2247042-1 | Mehrstufiger Auskunftsprozess, Dokumentenkopie, Akteneinsicht, physischer Datenträger |
| BVwG 01.02.2024, W287 2242238-1 | Papierakt, unzulässiger Erkundungsbeweis  |
| BVwG 22.12.2023, W292 2247003-1 | Bonitätsdaten, Speicherfristen  |
| BVwG 22.01.2024, W211 2262943-1 | Newsletter, § 174 TKG 2021  |
| BVwG 16.02.2024, W221 2268420-1 | KFZ, Versicherung, Geltendmachung von Rechtsansprüchen, Rollenverteilung              |
| BVwG 20.02.2024, W211 2261811-1 | Geldwäsche- und Terrorismusbekämpfung   |
| BVwG 18.01.2024, W137 2263970-1 | Dienstverhältnis, Koppelungsverbot, Überwachung                                       |
| BVwG 28.02.2024, W292 2235435-1 | Presserat, Auskunftsrecht   |
| BVwG 12.02.2024, W176 2247266-1 | Markt, Kamera, Negativauskunft  |
| BVwG 04.03.2024, W211 2263780-1 | Akteneinsicht, keine Auskunft über Mitarbeiter  |

|                                 |   |
|---------------------------------|---|
| BVwG 20.03.2024, W221 2257567-1 | Negativauskunft, Datenherkunft  |
| BVwG 26.03.2024, W137 2241630-1 | Geldbuße, Bank, Excel-Datei, Datensicherheit, wirtschaftliche Einheit                   |
| BVwG 11.03.2024, W252 2271937-1 | Beschwerdegegner, <i>res iudicata</i>   |
| BVwG 27.03.2023, W214 2259197-1 | KFZ, Informationspflicht  |
| BVwG 01.03.2024, W176 2249967-1 | AuskunftspflichtG, COVID-Kurzarbeitsbeihilfen, juristische Personen, AMS                |
| BVwG 30.04.2024, W252 2272830-1 | Akteneinsicht, justizielle Tätigkeit, Unzuständigkeit                                   |
| BVwG 02.04.2024, W176 2266382-1 | Berechtigte Interessen, Verteidigung der Rechtsposition, Verweigerung der Akteneinsicht |
| BVwG 12.04.2024, W108 2275368-1 | Mahnklage, Kirchenbeitrag, Grundbuch  |
| BVwG 26.04.2024, W211 2281997-1 | Cookies, Medienprivileg, forum shopping, Kopplungsverbot, "Pay or Okay"                 |
| BVwG 26.04.2024, W211 2261821-1 | Bonitätswerte, Berichtigung, Vervollständigung  |
| BVwG 15.04.2024, W211 2277264-1 | Mehrparteienhaus, Videoüberwachung  |
| BVwG 29.04.2024, W176 2234682-1 | Medienprivileg, Bürgerjournalismus  |
| BVwG 12.04.2024, W108 2249366-1 | Auskunft über Korrespondenz   |
| BVwG 12.04.2024, W108 2255217-1 | Auskunft, Dokumentenkopie, Akteneinsicht  |
| BVwG 19.04.2024, W287 2251990-1 | Hausverwaltung, Einwilligung  |
| BVwG 19.04.2024, W287 2276988-1 | Löschung, Feststellungsanspruch, antragsgebundene Rechte                                |
| BVwG 28.08.2023, W214 2226813-1 | PNR-Daten   |
| BVwG 24.05.2024, W271 2269889-1 | Direktwerbung, Einwilligung   |
| BVwG 17.04.2024, W108 2271999-2 | Anbieter von Kommunikationsdiensten, Kundendaten  |
| BVwG 22.05.2024, W298 2263508-1 | Aktiv- und Passivlegitimation   |
| BVwG 23.04.2024, W605 2289290-1 | Verfahrenshilfe   |

|                                 |  |
|---------------------------------|--|
| BVwG 03.06.2024, W211 2273051-1 | Justizielle Tätigkeit  |
| BVwG 23.04.2024, W292 2248672-1 | Automatisierte Entscheidungsfindung, Auskunft über Berechnung des Bonitätsscores |
| BVwG 28.05.2024, W176 2249328-1 | Kundenbindung, Verantwortlichkeit, Geldbuße iHv EUR 8 Mio behoben                |
| BVwG 28.06.2023, W214 2245388-1 | ERsB   |
| BVwG 06.06.2024, W108 2280859-1 | Medienprivileg, Redaktionsgeheimnis, juristische Personen                        |
| BVwG 18.04.2024, W137 2248575-1 | Erleichterungsgebot, Geldbuße iHv EUR 9,5 Mio auf EUR 0,5 Mio herabgesetzt       |
| BVwG 13.05.2024, W101 2249293-1 | Datenschutzbehörde, Mitwirkungspflicht   |
| BVwG 11.07.2023, W214 2257639-1 | COVID, Gesundheitsdaten  |
| BVwG 27.03.2024, W214 2243436-1 | Geldbuße, Selbstbeichtigungsverbot, Kundenbindung, Profiling                     |
| BVwG 07.06.2024, W256 2246230-1 | Geldbuße, Selbstbeichtigungsverbot, Kundenbindung, Profiling                     |
| BVwG 28.06.2024, W108 2250401-1 | Nada, Anti-Doping-Regelungen, Anwendungsbereich, erneute Vorlage                 |
| BVwG 17.06.2024, W287 2285759-1 | Unvertretener juristischer Laie  |
| BVwG 11.03.2024, W214 2235505-1 | AuskunftspflichtG, COVID-Hilfen  |
| BVwG 08.07.2024, W137 2278780-1 | Auskunft, Prozessposition  |
| BVwG 15.07.2024, W298 2284627-1 | Videoüberwachung, Gastronomie, Geldbuße  |
| BVwG 10.06.2024, W148 2291941-1 | WiEReG, Medien   |
| BVwG 10.07.2024, W298 2293438-1 | Hausverwaltung, WEG, berechtigtes Interesse                                      |
| BVwG 24.06.2024, W606 2286002-2 | Vergabe, Akteneinsicht   |
| BVwG 22.07.2024, W211 2271978-1 | Hausverwaltung, BYOD   |
| BVwG 08.07.2024, W252 2241322-1 | Genetische und biometrische Daten, Zentrale erkennungsdienstliche Evidenz        |

|                                 |   |
|---------------------------------|---|
| BVwG 27.06.2023, W298 2261979-1 | Negativfeststellung, Videoaufnahme  |
| BVwG 08.07.2024, W177 2287425-1 | KontRegG  |
| BVwG 27.06.2024, W176 2248629-1 | Gesundheitsdaten, Gesundheitswesen  |
| BVwG 31.07.2024, W108 2284491-1 | Dark Patterns, Cookie-Banner  |
| BVwG 22.04.2024, W214 2253376-1 | Universität, Rollenverteilung, neue Daten, juristische Person                               |
| BVwG 20.11.2023, W214 2222613-2 | Datenkopie, originalgetreue Reproduktion, Ermessen, Geschäftsgeheimnis                      |
| BVwG 22.07.2024, W211 2171666-1 | Auskunft, Herkunft, Profiling   |
| BVwG 31.07.2024, W108 2280724-1 | Dark Patterns, Cookies, Einwilligung, Widerruf  |
| BVwG 10.07.2024, W298 2261830-1 | COVID-Test, Gesundheitsdaten, Dienstverhältnis  |
| BVwG 21.08.2024, W176 2281424-1 | Exekution, justizielle Tätigkeit, Zustellung  |
| BVwG 08.08.2024, W282 2289350-1 | TKG, Werbeemail, Geldstrafe   |
| BVwG 05.07.2023, W292 2284228-1 | Auftragsverarbeiter, Zurechnung   |
| BVwG 21.08.2024, W258 2246325-1 | Anwendungsbereich, Unzuständigkeit, Schule, COVID   |
| BVwG 21.08.2024, W214 2254151-1 | Heizkostenabrechnung, Zuständigkeit   |
| BVwG 21.08.2024, W214 2280448-1 | Nichterteilung der Auskunft, mangelhafte Auskunftserteilung                                 |
| BVwG 28.08.2024, W221 2279014-1 | Tesla, Dash-Cam, Beweislast   |
| BVwG 22.08.2024, W256 2246158-1 | SPG, Identitätsdokumentenregister, AuvBZ, Unzuständigkeit                                   |
| BVwG 16.09.2024, W137 2288585-1 | Wildkamera, zeitlicher Anwendungsbereich, DSGVO 2000 Verhältnismäßigkeit, gelindeste Mittel |
| BVwG 02.09.2024, W290 2242336-1 | DSA, KoPI-G, KDD-G  |
| BVwG 01.10.2024, I406 2297556-1 | ORF-Beitrag   |

|                                 |  |
|---------------------------------|--|
| BVwG 19.09.2024, W287 2248365-1 | AuskunftspflichtG, Meinungsäußerungsfreiheit                       |
| BVwG 25.09.2024, W108 2287986-1 | Präklusion, Haushaltsausnahme, Forderungsbe-<br>treibung           |
| BVwG 16.09.2024, W137 2293092-1 | Sozialversicherung, AMS, rechtliche Verpflich-<br>tung             |
| BVwG 15.10.2024, W254 2291347-1 | Warnung  |
| BVwG 20.09.2024, W214 2291834-1 | Negativauskunft  |
| BVwG 30.09.2024, W603 2297646-1 | Cold Calling, Geldstrafe   |
| BVwG 22.10.2024, W252 2286224-1 | Eltern-App, Haushaltsausnahme, Familienleben                       |
| BVwG 25.10.2024, W108 2285546-1 | Geldbuße, sensible Daten, Verschulden, Straf-<br>zumessung         |
| BVwG 30.09.2024, W256 2248861-1 | Rechtsanwalt, Rechtsdurchsetzung, berechtig-<br>tes Interesse      |
| BVwG 13.09.2024, W298 2274626-1 | reCAPTCHA, Cookies, berechtigtes Interesse                         |
| BVwG 05.09.2024, W211 2291307-1 | Smart Meter, Vertragserfüllung, Koppelungs-<br>verbot, Transparenz |
| BVwG 17.09.2024, W298 2295130-1 | Geldbuße, Mitwirkung, Selbstbezeichnung                            |
| BVwG 30.09.2024, W108 2285483-1 | Geldbuße, Videoüberwachung, Kennzeichnung                          |
| BVwG 17.10.2024, W274 2291368-1 | Datenschutzbehörde, AuskunftspflichtG, amts-<br>wegige Verfahren   |
| BVwG 16.10.2024, W287 2258171-1 | Beipackwerbung   |
| BVwG 05.11.2024, W292 2247063-1 | Bonitätsdaten, Aufbewahrung  |
| BVwG 07.10.2024, W271 2294874-1 | Cold Calling   |
| BVwG 24.10.2024, W603 2301338-1 | Zuständigkeit, ORF-Beitrag   |
| BVwG 22.10.2024, W252 2249249-1 | Energieunternehmen, EEffG, intelligente Strom-<br>zähler           |
| BVwG 25.10.2024, W101 2256689-1 | Informationspflicht, Mitteilungspflicht                            |



|                                 |   |
|---------------------------------|---|
| BVwG 17.10.2024, W176 2284816-1 | Geldbuße, Videoüberwachung, Verfahrenskosten          |
| BVwG 22.10.2024, W252 2247518-1 | Stammzahlenregisterbehörde, ERSB, Informationspflicht |
| BVwG 22.11.2024, W211 2272917-1 | Tod, Verlust der Parteistellung                       |
| BVwG 27.11.2024, W603 2280263-1 | ISP, Zugangssperren, Vorabentscheidungsersuchen       |

### Weitere ausgewählte Entscheidungen

| Entscheidung                                 | Stichworte   |
|--|--|
| OLG Graz 12.02.2024, 9Bs274/23x              | Einspruch gemäß § 106 StPO   |
| BFG 19.03.2024, RV/7104071/2023              | Gebühr   |
| BFG 12.04.2024, RV/4100104/2024              | WiEReG   |
| BFG 20.06.2024, RV/5100216/2024              | GMSG   |
| BFG 05.06.2024, RV/7102695/2023              | Abgabenrechtliche Geheimhaltungspflicht  |
| OLG Graz 15.07.2024, 9Bs171/24a              | Spykamera, Appartement, Urlaub   |
| LVwG NÖ 06.06.2024, LVwG-AV-2018/001-2023    | Sicherheitspolizeiliche Fallkonferenzen  |
| LVwG Wien 06.08.2024, VGW-101/042/2543/2024  | Zentrales Personenstandsregister, Berichtigung, akademischer Titel eines Elternteils |
| LVwG Steiermark 12.04.2024, 30.5-736/2024    | Zustelldienst, eGovernment   |
| BFG 27.09.2024, RV/5100356/2024              | Beschreibbeschwerde, Pauschalgebühr  |
| LVwG Wien 29.02.2024, VGW-001/049/14641/2023 | Handelsstatistik, UID-Nummer, Art 6 Abs 1 lit e DSGVO                                |
| LVwG Tirol 03.12.2024, LVwG-2024/12/2131-5   | DNA, Observierungsvideo, Löschung  |

### DSB

| Entscheidung                   | Stichworte                            |
|--------------------------------|---------------------------------------|
| DSB 21.11.2022, 2022-0.792.182 | Juristische Person, öffentliche Daten |

|                                |   |
|--------------------------------|---|
| DSB 07.12.2023, 2023-0.637.760 | Geldbuße, juristische Person, Mitwirkung  |
| DSB 07.12.2023, 2023-0.583.644 | Geldbuße, juristische Person, Videoüberwachung  |
| DSB 11.12.2023, 2023-0.789.858 | Geldbuße, juristische Person, Auskunft  |
| DSB 09.06.2022, 2021-0.643.804 | Grundbuch, justizielle Tätigkeit  |
| DSB 12.12.2023, 2023-0.603.142 | Data Breach-Meldung, Mitwirkungspflicht, Geldbuße   |
| DSB 26.04.2023, 2023-0.072.284 | innerstaatliche Verarbeitung, juristische Person, negativer Vermerk                                       |
| DSB 18.09.2023, 2023-0.336.563 | Fund, SPG   |
| DSB 19.09.2023, 2023-0.632.875 | Räumlicher Anwendungsbereich, Cookie-Banner, Mitteilung gemäß Art 19 DSGVO                                |
| DSB 26.06.2023, 2023-0.227.210 | Anwaltskorrespondenz, rechtliche Verpflichtung, Nichtfeststellbarkeit                                     |
| DSB 06.11.2023, 2023-0.772.005 | Melderegister, Auskunftssperre  |
| DSB 10.08.2023, 2023-0.058.359 | Kommanditgesellschaft, Zuständigkeit  |
| DSB 19.11.2021, 2020-0.591.897 | Aufzeichnung eines Telefongesprächs, WAG, ZaDiG, MiFID II   |
| DSB 04.08.2023, 2023-0.159.938 | Videoüberwachung, WEG, berechtigtes Interesse   |
| DSB 08.09.2021, 2021-0.474.768 | BVT-Untersuchungsausschuss  |
| DSB 18.12.2023, 2023-0.594.826 | OSZE, Rollenverteilung, Anwendungsbereich, Zuständigkeit  |
| DSB 09.01.2023, 2022-0.479.809 | Wikipedia, Anwendungsbereich, Rollenverteilung, Recht auf Vervollständigung, Medien- und Meinungsfreiheit |
| DSB 04.01.2024, 2023-0.592.319 | Fußball, Löschung   |
| DSB 06.09.2023, 2022-0.858.901 | Schule, Videoüberwachung  |
| DSB 05.11.2020, 2020-0.714.215 | AMS, SozVersNr  |

|                                |   |
|--------------------------------|---|
| DSB 17.01.2022, 2021-0.512.929 | Betriebsrat, A1   |
| DSB 26.01.2024, 2024-0.044.042 | Panoramaaufnahmen, Rollenverteilung, DSFA, vorherige Konsultationen           |
| DSB 06.08.2021, 2021-0.415.529 | SMS-Werbung, Information, Löschung  |
| DSB 01.09.2022, 2022-0.616.013 | Minderjähriger, Auskunftsrecht  |
| DSB 16.12.2021, 2021-0.816.492 | Auskunftserteilung per E-Mail, AVG, ZustG                                     |
| DSB 06.10.2023, 2023-0.273.912 | Data Breach, Medienprivileg, Gesundheitsdaten                                 |
| DSB 04.07.2024, 2024-0.199.724 | Rechnungshof, Parteifinanzierung  |
| DSB 08.10.2021, 2021-0.698.184 | Firmenbuch, Geschäftsführer   |
| DSB 07.07.2024, 2023-0.358.049 | Buchhalterische Aufbewahrungspflichten  |
| DSB 05.09.2024, 2023-0.793.494 | Grundbuch, Rollenverteilung, Gemeinsam Verantwortliche, justizielle Tätigkeit |
| DSB 28.03.2024, 2024-0.215.259 | Zuständigkeit, Mandatsbescheid, Untersuchungsausschuss, COFAG                 |

# Rechtsakte und Leitlinien 2024

Die neu erscheinenden Rechtsakte sowie die Leitlinien des EDSA wurden erst im Laufe des Jahres in den Schönherr Datenschutzmonitor 2024 aufgenommen. In dieser Übersicht sind nur ausgewählte Rechtsakte und Leitlinien enthalten, die im Schönherr Datenschutzmonitor berücksichtigt wurden.

## EU-Rechtsakte

| Rechtsakt  | Stichworte  |
|--|---|
| VO (EU) 2024/1620 des Europäischen Parlaments und des Rates vom 31. Mai 2024 zur Errichtung der Behörde zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010, <a href="#">ABI L 2024/1620, 1.</a>   | Behörde zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung |
| VO (EU) 2024/1624 des Europäischen Parlaments und des Rates vom 31. Mai 2024 zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, <a href="#">ABI L 2024/1624, 1.</a>  | Geldwäsche, Terrorismusfinanzierung, Finanzsystem                 |
| RL (EU) 2024/1640 des Europäischen Parlaments und des Rates vom 31. Mai 2024 über die von den Mitgliedstaaten einzurichtenden Mechanismen zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, zur Änderung der Richtlinie (EU) 2019/1937 und zur Änderung und Aufhebung der Richtlinie (EU) 2015/849, <a href="#">ABI L 2024/1640, 1.</a> | Geldwäsche, Terrorismusfinanzierung, Finanzsystem                 |
| RL (EU) 2024/1654 des Europäischen Parlaments und des Rates vom 31. Mai 2024 zur Änderung der Richtlinie (EU) 2019/1153 in Bezug auf den Zugang zuständiger Behörden zu zentralen Bankkontenregistern über das Vernetzungssystem und auf technische Maßnahmen zur Erleichterung der Verwendung von Transaktionsaufzeichnungen, <a href="#">ABI L 2024/1654, 1.</a>                               | Cybercrime, Terrorismus, Transaktionsaufzeichnungen               |
| VO (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858,  | Künstliche Intelligenz  |

|  |   |
|--|---|
| <p>(EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), <a href="#">ABI L 2024/1689, 1.</a></p>  |   |
| <p>Beschluss (EU) 2024/2218 des Rates vom 28. August 2024 über die Unterzeichnung – im Namen der Europäischen Union – des Rahmenübereinkommens des Europarats über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit, <a href="#">ABI L 2024/2218, 1.</a></p>  | <p>Europarat, künstliche Intelligenz</p>  |
| <p>DurchführungsVO (EU) 2024/2690 der Kommission vom 17. Oktober 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltzustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt, <a href="#">ABI L 2024/2690, 1.</a></p> | <p>Cybersicherheit, Risikomanagement</p>  |
| <p>DurchführungsVO (EU) 2024/2835 der Kommission vom 4. November 2024 zur Festlegung von Vorlagen für die Transparenzberichtspflichten der Anbieter von Vermittlungsdiensten und der Anbieter von Online-Plattformen gemäß der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates, <a href="#">ABI L 2024/2835, 1.</a></p>  | <p>Transparenzberichtspflichten, Digital Service Act</p>                            |
| <p>RL (EU) 2024/2831 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit, <a href="#">ABI L 2024/2831, 1.</a></p>  | <p>Plattformarbeit; Datenschutz</p>   |
| <p>DurchführungsVO (EU) 2024/2916 der Kommission vom 25. November 2024 zur Festlegung eines Standardformulars für die Daten, die in dem Bericht über die Verarbeitung personenbezogener Daten enthalten sind, der von Dienstleistern gemäß der Verordnung (EU) 2021/1232 des Europäischen Parlaments und des Rates veröffentlicht und der zuständigen Aufsichtsbehörde und</p>   | <p>Anbieter nummernunabhängiger inter-personeller Kommunikationsdienste (NIICS)</p> |

|   |   |
|---|---|
| der Kommission vorgelegt wird, <a href="#">ABLL 2024/2916, 1.</a>   |   |
| DurchführungsVO (EU) 2024/2977, <a href="#">ABI L 2024/2977, 1</a> ; DurchführungsVO (EU) 2024/2979, <a href="#">ABI L 2024/2979, 1</a> ; DurchführungsVO (EU) 2024/2980, <a href="#">ABI L 2024/2980, 1</a> ; DurchführungsVO (EU) 2024/2981, <a href="#">ABI L 2024/2981, 1</a> ; DurchführungsVO (EU) 2024/2982, <a href="#">ABI L 2024/2982, 1.</a> | Europäische Brieftasche gemäß Art 5a der eIDAS-VO |

### Nationale Rechtsakte

| Rechtsakt   | Stichworte  |
|---|---|
| Bundesgesetz, mit dem das Bundes-Verfassungsgesetz geändert und ein Informationsfreiheitsgesetz erlassen wird, <a href="#">BGBl I 2024/5.</a>   | Amtsverschwiegenheit, Grundrecht auf Zugang zu staatlichen Information, Informationsfreiheitsgesetz |
| Bundesgesetz, mit dem das KommAustria-Gesetz und das Telekommunikationsgesetz 2021 geändert werden, <a href="#">BGBl I 2024/6.</a>  | Servicestelle für Künstliche Intelligenz  |
| Bundesgesetz, mit dem das Datenschutzgesetz geändert wird, <a href="#">BGBl I 2024/62.</a>  | Novelle des Medienprivilegs   |
| Bundesverfassungsgesetz, mit dem das Bundes-Verfassungsgesetz geändert wird, <a href="#">BGBl I 2024/68.</a><br><br>Bundesgesetz, mit dem das Informationsordnungsgesetz, das Datenschutzgesetz, das Beamten-Dienstrechtsgesetz 1979 und das Verwaltungsgerichtshofgesetz 1985 geändert werden, <a href="#">BGBl I 2024/70.</a><br><br>Bundesgesetz, mit dem das Rechnungshofgesetz 1948 und das Volksanwaltschaftsgesetz 1982 geändert werden, <a href="#">BGBl I 2024/71.</a> | Parlamentarisches Datenschutzkomitee  |
| Bundesgesetz zur Einrichtung einer nationalen Behörde für die Cybersicherheitszertifizierung (Cybersicherheitszertifizierungs-Gesetz; CSZG), <a href="#">BGBl I 2024/78.</a>  | Cybersicherheitszertifizierung  |
| Bundesgesetz, mit dem ein Qualifizierte-Einrichtungen-Gesetz erlassen wird und die Zivilprozessordnung, das Konsumentenschutzgesetz, das Gerichtsgebühren-gesetz und das Rechtsanwaltsstarifgesetz geändert werden  | Umsetzung der Verbandsklagen-Richtlinie 2020/1828   |

|   |   |
|---|---|
| (Verbandsklagen-Richtlinie-Umsetzungs-Novelle), <a href="#">BGBl I 2024/85</a> .  |   |
| Bundesgesetz, mit dem das KommAustria-Gesetz geändert wird, <a href="#">BGBl I 2024/90</a> .  | Koordinator-für-digitale-Dienste-Gesetz, RTR GmbH       |
| Bundesgesetz, mit dem das Arbeitsvertragsrechts-Anpassungsgesetz, das Arbeitsverfassungsgesetz, das Arbeitsinspektionsgesetz 1993, das Dienstnehmerhaftpflichtgesetz, das Allgemeine Sozialversicherungsgesetz, das Beamten-Kranken- und Unfallversicherungsgesetz, das Notarversorgungsgesetz, das Einkommensteuergesetz 1988, das Heimarbeitsgesetz und das Landarbeitsgesetz 2021 geändert werden (Telearbeitsgesetz), <a href="#">BGBl I 2024/110</a> .   | Telearbeit, Informations- und Kommunikationstechnologie |
| Bundesgesetz, mit dem ein DORA-Vollzugsgesetz erlassen und das Alternative Investmentfonds Manager-Gesetz, das Bankwesengesetz, das Börsengesetz 2018, das Finanzmarktaufsichtsbehördengesetz, das Investmentfondsgesetz 2011, das Pensionskassengesetz, das Sanierungs- und Abwicklungsgesetz, das Versicherungsaufsichtsgesetz 2016, das Wertpapieraufsichtsgesetz 2018 und das Zahlungsdienstegesetz 2018 geändert werden, <a href="#">BGBl I 2024/112</a> | DORA-Vollzugsgesetz, DORA-Verordnung 2022/2554          |
| Bundesgesetz, mit dem das E-Government-Gesetz geändert wird, <a href="#">BGBl I 2024/117</a> .  | E-Government  |
| Bundesgesetz, mit dem das Sicherheitspolizeigesetz geändert wird, <a href="#">BGBl I 2024/122</a> .   | Sicherheitsbehörden, Datenverarbeitung                  |
| Bundesgesetz, mit dem die Gewerbeordnung 1994 geändert wird, <a href="#">BGBl I 2024/130</a> .  | Gewerbeinformationssystem Austria (GISA)                |
| Verordnung des Bundesministers für Finanzen über die Abfrage von sensiblen Daten 2024 nach dem Transparenzdatenbankgesetz 2012 (Transparenzdatenbank-Abfrageverordnung 2024), <a href="#">BGBl II 2024/223</a> .  | Transparenzdatenbank                                    |
| Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung zur Registerforschung im Wirkungsbereich des Bundesministeriums für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie  | Registerforschung                                       |

|  |  |
|--|--|
| (Registerforschungsverordnung-BMK – RFV-BMK), <a href="#">BGBl II 2024/241</a> .   |  |
| Verordnung der Bundesministerin für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie, mit der die Automatisiertes Fahren Verordnung geändert wird (3. Novelle zur AutomatFahrV), <a href="#">BGBl II 2024/287</a> .   | Automatisiertes Fahren                               |
| Verordnung des Bundesministers für Soziales, Gesundheit, Pflege und Konsumentenschutz über Regelungen zu den Zugriffsberechtigungen auf die eHealth-Anwendung Elektronischer Impfpass (Zugriffsberechtigungsverordnung – ZugriffsV), <a href="#">BGBl II 2024/300</a> .  | eImpfpass  |
| Bundesgesetz, mit dem das Finanzmarkt-Geldwäschegesetz, das Wirtschaftliche Eigentümer Registergesetz, das Finanzmarktaufsichtsbehördengesetz und das Glücksspielgesetz geändert werden (FM-GwG-Anpassungsgesetz), <a href="#">BGBl I 2024/151</a> .   | Geldwäsche, Terrorismus, Kryptowerte                 |
| Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz, das Gerichtsorganisationsgesetz, das Finanzstrafgesetz, das Justizbetreuungsagentur-Gesetz, das Allgemeine Verwaltungsverfahrensgesetz 1991 und das Jugendgerichtsgesetz 1988 geändert werden (Strafprozessrechtsänderungsgesetz 2024) <a href="#">BGBl I 2024/157</a> . | Auswertung von Mobiltelefonen und Daten in der Cloud |

### Leitlinien

| Leitlinien   | Stichworte  |
|--|---|
| EDSA Leitlinien 2/2023 über den technischen Anwendungsbereich von Art 5 Abs 3 der ePrivacyRL <sup>2</sup> (2024) | Cookies, Tracking   |
| EDSA Guidelines 02/2024 on Article 48 GDPR (2024)  | Drittlandsbehörde, Datentransfer, Rechtsgrundlage, Zweistufentest |



# Rechtsprechungsübersicht 2025

Die Reihung der österreichischen Entscheidungen richtet sich nach dem Erscheinungsdatum im RIS, weil die Entscheidungen in dieser Reihenfolge für den Schönherr Datenschutzmonitor erfasst wurden.

Die Rechtsprechung zum IFG ist unter Pkt 10 gesondert erfasst.

## EGMR

| <b>Entscheidung</b>  | <b>Stichworte</b>   |
|--|---|
| EGMR 23.01.2025, 31175/14, <i>Reznik/Ukraine</i>   | Durchsuchung, Beschlagnahme, Anwaltsgeheimnis, wirksames Rechtsmittel |
| EGMR 04.02.2025, 33421/16, <i>Klimova/Russland</i>   | Vorratsdatenspeicherung, Aktivistin, Meinungsfreiheit                 |
| EGMR 04.02.2025, 8825/22, <i>Bazhenov/Russland</i>   | Positive Pflicht, sexuelle Orientierung, soziales Netzwerk            |
| EGMR 13.02.2025, 51409/19, <i>Macharik/Tschechien</i>                                      | Schutz der Kommunikation, faires Verfahren                            |
| EGMR 18.02.2025, 33067/22, <i>Khara-zishvili/Georgien</i>                                  | Anwaltsgeheimnis, Telefonüberwachung                                  |
| EGMR 03.04.2025, 57748/21, <i>Kulák/Slovakia</i>   | Rechtsanwalt, Kanzleidurchsuchung, Auswertung eines Computers         |
| EGMR 01.04.2025, 2799/16, <i>Ships Waste Oil Collector B.V. and Others/the Netherlands</i> | Telefonabhörung, Datenweitergabe, Beweismittel                        |
| EGMR 08.04.2025, 22077/19, <i>Green/UK</i>   | Datenoffenlegung, parlamentarische Immunität                          |
| EGMR 29.04.2025, 49617/22, <i>Kavecansky/Slowakei</i>                                      | Notariat, Hausdurchsuchung, Rechtsstaatsprinzip                       |
| EGMR 27.05.2025, 39056/22, <i>Selishcheva/Russland</i>                                     | politische Meinung, Rückwirkungsverbot                                |
| EGMR 03.06.2025, 9389/19, <i>Uygun/Türkei</i>  | Recht auf Korrespondenz, Haft   |
| EGMR 12.06.2025, 33037/22, <i>TH/Tschechien</i>  | Geschlechtseintrag, Personenstand, körperliche Unversehrtheit         |
| EGMR 01.07.2025, 6033/19, <i>AR/Vereinigtes Königreich</i>                                 | Strafregisterauszug, Vorhersehbarkeit, Unschuldvermutung              |

|  |   |
|--|---|
| EGMR 10.07.2025, 64753/14, <i>Gulotti/Italien</i>                                    | Überwachung, Briefverkehr, Haft                                 |
| EGMR 10.07.2025, 2599/16, <i>Korniyets/Ukraine</i>                                   | Hausdurchsuchung, wirksamer Rechtsbehelf                        |
| EGMR 09.09.2025, 24729/17, <i>Ilareva/Bulgaria</i>                                   | Hassrede, Ermittlungspflicht, Facebook-Account                  |
| EGMR 11.09.2025, 26519/16, <i>Yakym-chuk/Ukraine</i>                                 | geheime Videoüberwachung, Gerichtsbeschluss                     |
| EGMR 11.09.2025, 28473/22, <i>Charki/France</i>                                      | Medien, Telefonüberwachung                                      |
| EGMR 06.11.2025, 46704/16, <i>Guyvan/Ukraine</i>                                     | Personenbezogene Daten, Kommunikationsüberwachung, Arbeitsplatz |
| EGMR 06.11.2025, 37639/19, <i>AV/Schweiz</i>   | Haft, Korrespondenz   |
| EGMR 13.11.2025, 5778/17, <i>Manukyan/Armenien</i>                                   | Überwachung, Drohung, Privatleben                               |
| EGMR 18.11.2025, 50756/17, <i>Stanev and Bulgarian Helsinki Committee v Bulgaria</i> | Informationszugang, NGO, Watchdog-Funktion                      |
| EGMR 18.12.2025, 37514/20, <i>Cerny/Tschechien</i>                                   | Anwaltskorrespondenz, Datenextraktion                           |

### **EuGH (Urteile und Schlussanträge)**

| <b>Entscheidung</b>  | <b>Stichworte</b>                                     |
|--|---|
| EuGH 09.01.2025, C-394/23, <i>Mousse</i>                             | Anrede, Vertragserfüllung, berechtigtes Interesse     |
| EuGH 09.01.2025, C-416/23, <i>Österreichische Datenschutzbehörde</i> | Exzess, Wahlrecht der Aufsichtsbehörde                |
| EuGH SA 06.02.2025, C-413/23 P, <i>EDSB/SRB</i>                      | Personenbezug, Pseudonymisierung, Informationspflicht |
| EuGH SA 06.02.2025, C-492/23, <i>Russmedia Digital</i>               | Online-Marktplatz, Hosting, Rollenverteilung          |
| EuGH 13.02.2025, C-383/23, <i>ILVA</i>                               | Geldbuße, Unternehmensbegriff, Verhältnismäßigkeit    |
| EuGH 13.02.2025, C-612/23, <i>Verbraucherzentrale Berlin</i>         | Telekommunikation, Mindestvertragslaufzeit            |

|   |   |
|---|---|
| EuGH 25.02.2025, C-233/23, <i>Alphabet</i>  | Missbrauch einer beherrschenden Stellung, Interoperabilität                             |
| EuGH 27.02.2025, C-203/22, <i>Dun &amp; Bradstreet</i>  | Automatisierte Entscheidungsfindung, Profiling, Auskunftsrecht, Geschäftsgeheimnis      |
| EuGH 27.02.2025, C-638/23, <i>Amt der Tiroler Landesregierung</i>   | Rollenverteilung per Gesetz, öffentliche Stelle   |
| EuGH SA 27.02.2025, C-57/23, <i>Policejní prezidium</i>   | Biometrische und genetische Daten, DSRL-PJ, Recht der Mitgliedstaaten                   |
| EuGH 13.03.2025, C-247/23, <i>Deldits</i>   | Berichtigung, öffentliches Register, Geschlechtseintrag, Transidentität, Nachweis       |
| EuGH SA 20.03.2025, C-655/23, <i>Quirin Privatbank</i>  | Unterlassungsanspruch, Wiederholungsgefahr, Schadenersatz                               |
| EuGH SA 27.03.2025, C-654/23, <i>Inteligo Media</i>   | Direktwerbung, ePrivacyRL, personenbezogene Daten als Ware                              |
| EuGH SA 27.03.2025, C-97/23 P, <i>WhatsApp Ireland/EDSA</i>   | WhatsApp, EDSA, verbindlicher Beschluss, Rechtsschutzsystem der EU                      |
| EuGH 03.04.2025, C-710/23, <i>Ministerstvo zdravotnictví</i>  | Vertreter juristischer Personen, personenbezogene Daten, Zugang zu amtlichen Dokumenten |
| EuGH 08.04.2025, C-292/23, <i>EUSTa</i>   | Europäische Staatsanwaltschaft, Rechtsschutz, Zuständigkeit                             |
| EuGH 30.04.2025, C-313/23, <i>Inspektorat kam Visshia</i>   | Datenschutz-Aufsicht, Gerichtsbarkeit, Rollenverteilung                                 |
| EuGH SA 15.05.2025, Rs C-327/24, <i>Lolach</i>  | Telekommunikation, Wettbewerb, Zugangsverpflichtung                                     |
| EuGH 22.05.2025, C-213/23, <i>Kommission/Niederlande</i> ; C-215/23, <i>Kommission/Belgien</i> ; C-237/23, <i>Kommission/Bulgarien</i> ; C-238/23, <i>Kommission/Lettland</i> | PSI-II-RL, Vertragsverletzungsverfahren   |
| EuGH 05.06.2025, C-541/24, <i>Naltov</i>  | Akteneinsicht, Unzuständigkeit  |
| EuGH SA 05.06.2025, C-769/22, <i>Kommission/Ungarn</i>  | Strafregisterdaten  |
| EuGH SA 15.05.2025, C-209/23, <i>RRC Sports</i>   | FIFA, FFAR, berechnigte Interessen  |

|  |   |
|--|---|
| EuGH 19.06.2025, C-509/23, <i>Laimz</i>  | Geldwäsche, Glücksspiel, Datenschutzstrategien, Informationsaustausch, Identitätsfeststellung |
| EuGH 19.06.2025, C-200/24, <i>Kommission/Polen (Publicité pour les pharmacies)</i> | reglementierte Berufe, Apotheken, Online-Werbung  |
| EuGH 26.06.2025, C-555/23, <i>Makeleio</i>   | Audiovisuelle Medien, Grundsatz der Rechtssicherheit bei der Verhängung von Strafen           |
| EuGH SA 19.06.2025, C-738/22 P, <i>Google/Kommission</i>                           | kartellrechtliche Geldbuße, Android, Google Suche und Chrome                                  |
| EuGH SA 03.06.2025, C-291/24, <i>Steiermärkische Bank und Sparkasse</i>            | Geldwäsche, Haftung, juristische Person, Verjährung   |
| EuGH 03.07.2025, C-529/23 P, <i>Parlament/TC</i>                                   | Parteiengehör, Akteneinsicht, Datenspeicherung im Konfliktfall, Personalakte                  |
| EuGH 10.07.2025, C-367/24, <i>Telekom România</i>                                  | Internetzugangsdienst, Netzneutralität, Video-streaming                                       |
| EuGH SA 01.08.2025, C-422/24, <i>Storstockholms</i>                                | Bodycams, Informationspflicht   |
| EuGH SA 01.08.2025, C-371/24, <i>Comdribus</i>                                     | Biometrie, Erforderlichkeit, erkennungsdienstliche Behandlung                                 |
| EuGH 04.09.2025, C-413/23 P, <i>EDSB/SRB</i>                                       | Personenbezug, Pseudonymisierung, Empfänger, Einwilligung                                     |
| EuGH 04.09.2025, C-655/23, <i>Quirin Privatbank</i>                                | Unterlassungsanspruch, immaterieller Schaden, Ausgleichsfunktion                              |
| EuGH SA 04.09.2025, C-414/24, <i>Datenschutzbehörde (Articulation des recours)</i> | Doppelgleisigkeit, Aufsichtsbehörde, Gericht  |
| EuGH SA 04.09.2025, C-199/24, <i>Legal Newsdesk Sweden</i>                         | Medienfreiheit, Meinungsfreiheit, Strafurteil   |
| EuGH SA 04.09.2025, C-312/24, <i>Darashev</i>                                      | Personalakt, Dateisystem, strafrechtliche Ermittlungen, DSRL-PJ                               |
| EuGH 11.09.2025, C-115/24, <i>Österreichische Zahnärztekammer</i>                  | Telemedizin, Herkunftslandprinzip   |
| EuGH SA 18.09.2025, C-526/24, <i>Brillen Rottler</i>                               | Auskunftsrecht, Missbrauchsabsicht, Schadenersatz   |

|  |  |
|--|--|
| EuGH SA 18.09.2025, C-514/24, <i>Magyar Telekom</i>                  | "Nulltarif", GEREK-Leitlinien, Vorabentscheidungsersuchen                |
| EuGH SA 18.09.2025, C-188/24, <i>WebGroup Czech</i>                  | E-Commerce-RL, Herkunftslandprinzip                                      |
| EuGH SA 25.09.2025, C-474/24, <i>NADA</i>                            | Doping, Gesundheitsdaten, strafrechtliche Daten                          |
| EuGH 30.09.2025, C-40/25, <i>CRIF</i>                                | Streichung   |
| EuGH SA 16.10.2025, C-484/24, <i>NTH Haustechnik</i>                 | Gerichtsbarekeit, Beweisverwertung, Speicherbegrenzung                   |
| EuGH 29.10.2025, C-206/25 P, <i>Kommission/Bindl</i>                 | Streithilfe, Meta Ireland  |
| EuGH 30.10.2025, C-2/23, <i>FL und KM Baugesellschaft</i>            | Kronzeugenerklärung, Geheimhaltung                                       |
| EuGH 13.11.2025, C-654/23, <i>Integlio Media</i>                     | E-Mail-Newsletter, Direktwerbung, ePrivacy-RL                            |
| EuGH 20.11.2025, C-57/23, <i>Policejni prezidium</i>                 | biometrische Identifizierungsmaßnahmen, Strafverfahren, Datenspeicherung |
| EuGH 20.11.2025, C-327/24, <i>Lolach</i>                             | Telekommunikation, bauliche Anlagen, Zugangsverpflichtung                |
| EuGH SA 27.11.2025, C-421/24, <i>AGCOM</i>                           | Glücksspiel, Werbung, E-Commerce-RL, Video Sharing                       |
| EuGH 02.12.2025, C-492/23, <i>Russmedia Digital</i>                  | DSA, Haftungsprivileg, Verantwortlicheneigenschaft                       |
| EuGH 02.12.2025, C-34/24, <i>Stichting Right to Consumer Justice</i> | Online-Plattform, Verbandsklage, Gerichtsstand                           |
| EuGH SA 11.12.2025, C-684/24, <i>Across Fiduciaria</i>               | AML/CFT, wirtschaftliche Eigentümer, Register                            |
| EuGH SA 11.12.2025, C-468/24, <i>Netz Niederösterreich</i>           | Smart Meter, Stromnetz, elektronisches Kommunikationsnetz                |
| EuGH 18.12.2025, C-422/24, <i>Storstockholms Lokaltrafik</i>         | Körperkamera, Informationspflicht, gestuftes Informationsverfahren       |
| EuGH SA 18.12.2025, C-604/24, <i>Farmakeio YZ &amp; Sia</i>          | Apotheke, Online-Shop, Arzneimittel                                      |

## EuG

| <b>Entscheidung</b>   | <b>Stichworte</b>  |
|---|--|
| EuG 08.01.2025, T-354/22, <i>Bindl/Kommission</i>                                   | IP-Adresse, Datentransfer, Schadenersatz                                 |
| EuG 29.01.2025, T-70/23, <i>DPC/EDSA</i>  | DPC, EDSA, Kohärenzverfahren, verbindlicher Beschluss                    |
| EuG 26.03.2025, T-441/21, <i>UBS Group und UBS/Kommission</i>                       | Schutz von personenbezogenen Daten und Geschäftsgeheimnissen, alte Daten |
| EuG 29.04.2025, T-319/24, <i>Meta/EDPB</i>  | Meta, EDSA, unverbindliche Stellungnahme                                 |
| EuG 14.05.2025, T-36/23, <i>Stevi und The New York Times</i>                        | Dokumentenzugang, Richtigkeitsvermutung, Beweislast                      |
| EuG 16.07.2025, T-183/23, <i>Ballmann/EDSA</i>                                      | EDSA, Aktenzugang, Kohärenzverfahren                                     |
| EuG 03.09.2025, T-553/23, <i>Latombe</i>  | EU-US Data Privacy Framework, DPRC, US-Nachrichtendienste                |
| EuG 10.09.2025, T-58/24, <i>Tiktok</i> ; 10.09.2025, T-55/24, <i>Meta Platforms</i> | DSA, Online-Plattformen, Aufsichtsgebühr                                 |
| EuG 01.10.2025, T-384/20 RENV, <i>OC/Kommission</i>                                 | OLAF, Pressemitteilung, Unschuldsvermutung, Schadenersatz                |
| EuG 15.10.2025, T-291/23, <i>MeSoFa</i>   | Dokumentenzugang, Geschäftsinteresse, Personenbezug, berufliche Daten    |
| EuG 29.10.2025, T-590/23, <i>De Capitani</i>  | Dokumentenzugang, Entscheidungsprozess                                   |
| EuG 19.11.2025, T-367/23 R, <i>Amazon EU/Kommission</i>                             | Amazon, DSA, VLOP  |
| EuG 19.11.2025, T-623/22, <i>SD/EMA</i>   | EU-Organ, Dokumentenzugang, Geschäftsgeheimnis                           |
| EuG 03.12.2025, T-318/24, <i>WS/Kommission</i>                                      | Auskunft, Mitarbeiter, Dokument, Empfänger, Protokollierung              |
| EuG 19.12.2025, T-557/20 RENV, <i>EDPB/SRB</i>                                      | Streichung der Rechtssache   |

**VfGH**

| <b>Entscheidung</b>                                 | <b>Stichworte</b>   |
|---|---|
| VfGH 09.03.2023, E2097/2021                         | Finanzdatenaustausch, Besteuerung, GMSG                           |
| VfGH 02.12.2024, E1380/2024; 02.12.2024, E1379/2024 | Nationalrat, Auskunftsrecht                                       |
| VfGH 25.02.2025, G160/2024                          | NRWO, Wahlkarte, Identitätsdiebstahl, Identitätsprüfung           |
| VfGH 11.03.2025, E4624/2024                         | Massenverfahren, ORF-Beitrag, Datenschutz                         |
| VfGH 25.02.2025, G20/2025                           | SKY ECC, § 134 Z 3 StPO, Legaldefinition                          |
| VfGH 16.06.2025, G55/2025                           | Gesetzesprüfungsverfahren, Beweisverwertung, StPO                 |
| VfGH 24.06.2025, E4624/2024                         | ORF-Beitrags-Service GmbH, Beitragsdaten, Massenverfahren         |
| VfGH 12.08.2025, DS1/2025                           | Doppelgleisigkeit, Zuständigkeit, justizielle Tätigkeit, Web-ERV  |
| VfGH 25.06.2025, G71/2025                           | Gesetzesbeschwerde, Nachrichtenüberwachung                        |
| VfGH 11.09.2025, E1734/2025                         | Universität, Verordnung, Rechtsgrundlage, Audioaufzeichnung       |
| VfGH 12.09.2025, G175/2024                          | Gesetzesprüfung, Auswertung von Datenträgern                      |
| VfGH 12.09.2025, G108/2025                          | Gesetzesbeschwerde, Nachrichtenüberwachung                        |
| VfGH 24.09.2025, E1925/2025                         | strafgerichtliche Verurteilung, Staatsbürgerschaft                |
| VfGH 07.10.2025, G62/2025                           | WiEReG, public watchdog, Interessenabwägung, Gleichheitsgrundsatz |
| VfGH 07.10.2025, G26/2025                           | BilDokG, Interessenabwägung, Verfassungswidrigkeit                |
| VfGH 07.10.2025, G116/2025                          | Offenlegungspflicht, Jahresabschluss, Beugemittel                 |
| VfGH 07.10.2025, E599/2025                          | BilDokG, Anlassfall, verfassungswidrige Gesetzesanwendung         |

|                            |   |
|----------------------------|---|
| VfGH 11.09.2025, G48/2025  | Spenden, Veröffentlichung, Gesetzesprüfung                    |
| VfGH 27.11.2025, G99/2025  | Kartellrecht, Auswertung elektronischer Datenträger           |
| VfGH 09.12.2025, E335/2025 | Geldbuße, Strafkompetenz der DSB                              |
| VfGH 18.12.2025, G105/2025 | Arzneimittel-Großhandel, juristische Person, Wirtschaftsdaten |

## VwGH

| Entscheidung   | Stichworte  |
|--|---|
| VwGH 26.11.2024, Ra 2024/04/0408   | Zurückweisung, Abweichung von bisheriger Rechtsprechung                             |
| VwGH 19.12.2024, Ro 2022/15/0018   | Steuern, Spende, erhebliches öffentliches Interesse                                 |
| VwGH 05.12.2024, Ro 2023/01/0008   | Zentrale Personenstandsregister, Geschlechtseintrag, Transidentität                 |
| VwGH 20.12.2024, Ra 2024/04/0425   | öffentliche Daten   |
| VwGH 20.12.2024, Ra 2024/04/0427   | Säumenisbeschwerde  |
| VwGH 11.12.2024, Ra 2024/04/0423   | keine aufschiebende Wirkung   |
| VwGH 16.01.2025, Ra 2024/04/0424   | Cookies, Widerruf   |
| VwGH 10.12.2024, Ra 2022/04/0107   | Nachholung des Auskunftersuchens  |
| VwGH 16.01.2025, Ra 2024/04/0438   | Auskunftersuchen, Auslegung   |
| VwGH 10.12.2024, Ro 2021/04/0022   | Suchmaschine, Unterlassungsanspruch, Löschung, De-Indexierung, Informationsfreiheit |
| VwGH 27.02.2025, Ra 2024/04/0305   | GISA, schlicht-hoheitliches Handeln   |
| VwGH 29.01.2025, Ra 2023/04/0002   | Rechtsmissbrauch, Exzess, Auskunft  |
| VwGH 29.01.2025, Ra 2022/04/0049   | Rechtsmissbrauch, offenkundige Unbegründetheit, Berichtigung                        |
| VwGH 29.01.2025, Ro 2023/04/0018;<br>Ro 2022/04/0016;<br>Ra 2020/04/0084 | Rechtsmissbrauch, Exzess  |



|  |  |
|--|--|
| VwGH 20.03.2025, Ro 2022/01/0010                                 | Passgesetz, personenbezogene Daten                                   |
| VwGH 20.03.2025, Ro 2023/04/0050                                 | Informationspflicht, Feststellungskompetenz                          |
| VwGH 01.04.2025, Ro 2024/04/0005;<br>Ro 2023/04/0051             | Kohärenzverfahren, Aussetzung  |
| VwGH 03.04.2025, Ra 2025/01/0073                                 | Berichtigung, Melderegister, Zuständigkeit                           |
| VwGH 31.03.2025, Ra 2022/04/0143                                 | Exzess, Missbrauchsabsicht   |
| VwGH 09.05.2025, Ra 2022/16/0118                                 | Bescheidadressat, Gültigkeit   |
| VwGH 27.03.2025, Ro 2022/04/0023                                 | Mitarbeiter, Rollenverteilung, Übergangsbestimmung, Beschwerdegegner |
| VwGH 30.04.2025, Ro 2021/04/0005                                 | Übergangsbestimmung, Lösungsersuchen, Informationspflicht            |
| VwGH 30.04.2025, Ro 2021/04/0024                                 | Videoüberwachung, Geldbuße, Kumulationsprinzip                       |
| VwGH 15.04.2025, Ra 2021/04/0094                                 | Anwaltsgeheimnis, Auskunft   |
| VwGH 15.04.2025, Ro 2021/04/0012                                 | ASFINAG, Mautprellerei   |
| VwGH 06.05.2025, Ra 2024/07/0121                                 | Forderungskauf, keine Winkelschreiberei                              |
| VwGH 24.04.2025, Ra 2023/15/0105                                 | Arbeitnehmerveranlagung, Werbungskosten                              |
| VwGH 30.04.2025, Ra 2021/04/0118                                 | Melddaten, Bürgerbeteiligung, Übergangsbestimmung                    |
| VwGH 29.04.2025, Ra 2024/11/0150;<br>29.04.2025, Ra 2024/11/0151 | KFZ, Zulassungsevidenz, rechtliches Interesse                        |
| VwGH 05.06.2025, Ra 2024/04/0008                                 | AMS, Beschwerdegegner, Verantwortlicher                              |
| VwGH 17.06.2025, Ra 2025/04/0146                                 | Kohärenzverfahren, Säumnis   |
| VwGH 28.05.2025, Ro 2025/13/0001;<br>28.05.2025, Ro 2024/13/0022 | Kontenregister, Erbschaft  |
| VwGH 25.06.2025, Ra 2024/12/0115                                 | Auskunftsersuchen, Auslegung, Revision                               |
| VwGH 24.06.2025, Ra 2025/04/0148                                 | Videoüberwachung, berechtigtes Interesse                             |

|  |  |
|--|--|
| VwGH 04.07.2025, Ra 2023/04/0220                                 | COVID, Gesundheitsdaten, Verwaltungsstrafverfahren                           |
| VwGH 28.07.2025, Fr 2025/04/0002                                 | Zuständigkeit, DSGVO   |
| VwGH 29.07.2025, Ro 2022/04/0017                                 | Rollenverteilung, ELAK, Anwendungsbereich                                    |
| VwGH 01.08.2025, Ro 2023/04/0030;<br>01.08.2025, Ro 2023/04/0031 | Onlineshop, Einwilligung, Koppelungsverbot                                   |
| VwGH 01.08.2025, Ra 2023/04/0058                                 | lebenswichtige Interessen  |
| VwGH 06.08.2025, Ra 2025/04/0163                                 | Einwilligung, Widerruf   |
| VwGH 06.08.2025, Ra 2024/04/0309                                 | berechtigte Interessen, Einzelfallprüfung                                    |
| VwGH 20.08.2025, Ra 2024/04/0321                                 | Ersatz der Beschwerdekosten, Revision  |
| VwGH 20.08.2025, Ra 2023/04/0260                                 | Zurückverweisung, Bindungswirkung  |
| VwGH 20.08.2025, Ra 2025/04/0049                                 | Parteienbezeichnung, Verantwortlichenaustausch                               |
| VwGH 21.08.2025, Ra 2025/04/0143;<br>21.08.2025, Ra 2025/04/0147 | Missbrauchsabsicht, Exzess   |
| VwGH 02.09.2025, Ro 2023/04/0027                                 | Finanzprokurator, Verantwortliche, Aufwandsatz                               |
| VwGH 20.08.2025, Ro 2020/04/0010                                 | Auskunft, automatisierte Entscheidungsfindung, Profiling, Geschäftsgeheimnis |
| VwGH 16.09.2025, Ra 2025/04/0181                                 | Revision, Zulässigkeit, Rechtsfrage grundsätzlicher Bedeutung                |
| VwGH 11.09.2025, Ra 2024/03/0031                                 | Auskunft, Einsichtstermine   |
| VwGH 16.09.2025, Ra 2023/04/0008                                 | Rollenverteilung, StVO, städtischer Magistrat                                |
| VwGH 22.09.2025, Ra 2023/04/0108                                 | Beschwerdegegner   |
| VwGH 25.09.2025, Ra 2023/04/0279                                 | Melderegisterabfrage, Aufgabe im öffentlichen Interesse, Unzulässigkeit      |
| VwGH 29.09.2025, Ra 2025/04/0089                                 | Tatzeitraum, Strafbemessung, Leistungsfähigkeit                              |
| VwGH 24.09.2025, Ra 2024/04/0322                                 | verfahrensrechtliche Präklusivfrist  |

|                                  |  |
|----------------------------------|--|
| VwGH 29.09.2025, Ro 2023/04/0045 | Einwilligung, Prüfumfang, Kognitionsbefugnis   |
| VwGH 29.09.2025, Ra 2023/04/0246 | Videoüberwachung, Rechtsfrage grundsätzlicher Bedeutung                                    |
| VwGH 08.10.2025, Ra 2023/04/0117 | Erlaubnistatbestand, Informationspflicht, Geheimhaltung                                    |
| VwGH 17.10.2025, Ro 2022/04/0015 | Revision, konkrete Rechtsfrage   |
| VwGH 22.10.2025, Ra 2023/04/0075 | Videoüberwachung, § 12 DSGVO, berechnete Interessen, Datenminimierung, Verhältnismäßigkeit |
| VwGH 13.11.2025, Ra 2023/04/0271 | vergleichbarer Fall, automatisierte Entscheidung   |
| VwGH 13.11.2025, Ra 2022/04/0115 | Revisionspunkt, subjektives Recht, Zurückweisung   |
| VwGH 11.11.2025, Ro 2025/11/0002 | Gesundheitsdiensteanbieter, eHVD, öffentliche Apotheke                                     |
| VwGH 26.11.2025, Ra 2022/04/0157 | Untergang der Rechtspersönlichkeit   |
| VwGH 25.11.2025, Ra 2023/04/0268 | Revisionspunkt, mündliche Verhandlung  |
| VwGH 19.11.2025, Ra 2025/04/0190 | Verantwortlicher, Beschwerdegegner, Ermittlungspflicht                                     |
| VwGH 26.11.2025, Ra 2023/04/0020 | Wiedereinsetzung, Unvorhergesehenheit, Zuständigkeit                                       |

## Justiz

| Entscheidung  | Stichworte  |
|---|---|
| OGH 11.12.2024, 6Ob147/24x                            | Zentrales Testamentsregister, Erbe, Notar                 |
| OLG Linz 10.01.2025, 8Bs249/24k                       | Europäische Ermittlungsanordnung, Vollstreckungshindernis |
| OLG Linz 15.01.2025, 2R174/24g; 15.01.2025, 2R172/24p | Vollmacht, Auskunft, Anerkenntnis, Kosten                 |
| OLG Linz 23.01.2025, 1R4/25a                          | Vollmacht, Auskunft                                       |
| OGH 17.01.2025, 6ObA2/23x                             | Betriebsrat, E-Mail-Herausgabe                            |

|                                     |  |
|-------------------------------------|--|
| OLG Linz 27.01.2025, 11R1/25h       | Identitätsnachweis, elektronische Signatur   |
| OGH 22.01.2025, 13Os105/24a         | Erneuerungsantrag, Mobiltelefonauswertung  |
| OLG Linz 06.02.2025, 6R10/25w       | Vollmacht, Identitätsnachweis, Ablehnung der Auskunft                                  |
| OGH 22.01.2025, 9ObA79/24v          | sensible Daten, Dritte   |
| OLG Graz 30.12.2024, 10Bs118/24i    | Sicherstellung, Mobiltelefon, Verhältnismäßigkeit                                      |
| OGH 18.02.2025, 14Os11/25m          | SKY-ECC, Auswertung eines Mobiltelefons  |
| OGH 29.01.2025, 12Os79/24w          | Sicherstellung personenbezogener Daten, Einspruch nach § 106 StPO                      |
| OLG Graz 19.12.2024, 2R192/24h      | Auskunftersuchen, Identitätsnachweis, Vollmacht  |
| OGH 18.02.2025, 6Ob102/24d          | Vorabentscheidungsersuchen, Verantwortliche, Datenherkunft, Schadenersatz, Amtshaftung |
| OGH 18.02.2025, 6Ob137/24a          | Auskunft, Schadenersatz, Aussetzung  |
| OLG Innsbruck 08.01.2025, 4R136/24t | Personenbezug, Zuordnung, Differenzgeschäfte   |
| OLG Linz 05.03.2025, 2R32/25a       | Auskunft, Vollmacht, Kostenersatz  |
| OLG Linz 13.03.2025, 6R29/25i       | Auskunftersuchen, Identifizierung  |
| OGH 19.03.2025, 9Ob48/24k           | Streamingdienst, Verbraucherschutz   |
| OGH 25.02.2025, 11Os7/25a           | Datenbetrug  |
| OGH 18.02.2025, 6Ob218/24p          | Aussetzung, Smart Meter  |
| OLG Wien 27.08.2024, 17Bs267/24z    | § 63 DSG, Officialdelikt   |
| OGH 27.02.2025, 8ObA61/24i          | Einsichtsrechte des Betriebsrats   |
| OLG Graz 17.01.2025, 5R205/24t      | Auskunft, Vollmacht, Rechtsanwalt, Kostenersatz  |
| OLG Linz 09.01.2025, 6R171/24w      | Auskunft, Prozessposition, Rechtsmissbrauch  |
| OLG Innsbruck 29.01.2024, 10R87/24f | Auskunft, Vollmacht, Rechtsanwalt, Kostenersatz  |

|  |   |
|--|---|
| OLG Linz 02.04.2025, 4R29/25z  | Auskunft, Identitätsnachweis, Vollmacht                                   |
| OGH 26.03.2025, 6Ob50/24g  | eCommerce, Herkunftslandprinzip, DSA                                      |
| OLG Graz 14.03.2025, 5R28/25i  | Auskunft, Vollmacht, Kostenersatz   |
| OLG Graz 13.03.2025, 2R32/25f  | Auskunft, Identifizierung   |
| OGH 28.03.2025, 8Ob14/25d  | Smart Meter, Aussetzung   |
| OLG Wien 28.02.2025, 16R161/24z  | Datenkopie, Fernzugriff   |
| OLG Wien 02.11.2025, 4R133/24v   | Zuständigkeit, Klauselkontrolle, Speicherfrist, Drittlandtransfer         |
| OLG Innsbruck 27.03.2025, 7Bs64/25g  | Trennung des Ermittlungsverfahrens, § 27 StPO                             |
| OLG Graz 19.03.2025, 4R52/25m  | Auskunft, Datenkopie, Bestimmtheit  |
| OLG Wien 12.02.2025, 33R23/25g   | Beweisbeschaffung, Prozessstandpunkt, kein Rechtsmissbrauch               |
| OLG Wien 20.02.2025, 4R191/24y   | routinemäßige Identitätsprüfung, Vollmacht                                |
| OGH 24.04.2025, 10Ob5/25w; 10Ob18/25g  | Smart Meter, einstweilige Verfügung                                       |
| OGH 30.04.2025, 5Ob35/25w  | Smart Meter, Stromabschaltung   |
| OLG Linz 13.05.2025, 4R64/25x  | Beweismittel, Rechtsstaat   |
| OLG Linz 14.05.2025, 3R58/25g  | Erleichterungsgrundsatz, Identifizierung                                  |
| LG Innsbruck 19.06.2024, 350Jv184/25a  | Dienste der Informationsgesellschaft, Herkunftslandprinzip, Zuständigkeit |
| OGH 13.05.2025, 10b27/25i; 14.05.2025, 5Ob23/25f; 21.05.2025, 7Ob34/25p; 22.05.2025, 4Ob11/25h; 22.05.2025, 4Ob61/25m                      | Smart Meter, einstweilige Verfügung, Sicherheitsleistung                  |
| OLG Wien 27.03.2025, 33R49/25f   | Prozessführung, Rechtsmissbrauch, Geschäftsgeheimnis                      |
| OGH 22.05.2025, 4Ob28/25h; 26.05.2025, 8Ob11/25p; 27.05.2025, 9Ob22/25p; 27.05.2025, 9Ob26/25a; 27.05.2025, 9Ob7/25g; 27.05.2025, 9Ob9/25a | Smart Meter, einstweilige Verfügung, Sicherheitsleistung                  |

|  |   |
|--|---|
| OLG Graz 16.05.2025, 5R25/25y                    | Berichterstattung, Persönlichkeitsrecht, Bildnisschutz  |
| OGH 28.05.2025, 3Ob30/25w; 03.06.2025, 2Ob31/25k | Smart Meter, einstweilige Verfügung, Sicherheitsleistung  |
| OLG Wien 20.03.2025, 1R22/25z                    | Auskunft, Beweismaterial, Spielverluste   |
| OLG Linz 10.04.2025, 1R32/25v                    | Videoüberwachung, § 12 DSG, Überwachungsdruck   |
| OLG Wien 27.01.2025, 16R43/24x                   | Auskunft, Rechtsmissbrauch, Prozessposition   |
| OGH 03.07.2025, 6Ob113/24x                       | Marketingklassifikationen, kein Schadenersatz ohne Schaden                                      |
| OGH 03.07.2025, 6Ob53/25z                        | Recht am eigenen Wort, Tonbandaufnahme, Beweismittel  |
| OGH 03.07.2025, 6Ob62/25y                        | Doppelgleisigkeit des Rechtsschutzes, Behörde, beliehenes Unternehmen, Unterlassungsanspruch    |
| OGH 30.07.2025, 23Ds4/24a                        | Rechtsanwalt, direkte Kontaktaufnahme   |
| OGH 23.07.2025, 3Ob58/25p                        | Smart Meter, Aussetzung   |
| OGH 05.08.2025, 12Os71/25w                       | Datenverarbeitung in Schädigungsabsicht, § 63 DSG, tatbestandliche Handlungseinheit             |
| OLG Wien 11.02.2025, 4R5/25x                     | Auskunft, Rechtsanwalt, Vollmacht   |
| OLG Linz 16.01.2025, 4R157/24x                   | Auskunft, datenschutzfremdes Ziel, Rechte von Dritten   |
| OLG Wien 26.02.2025, 11R202/24t                  | Hoheitsverwaltung, Datenverarbeitung, Unterlassung  |
| OLG Linz 10.06.2025, 7Bs96/25d                   | Handyauswertung, Cloud-Speicher, HealthApp  |
| OGH 13.08.2025, 6Ob15/25m                        | Vorabentscheidungsersuchen, automatisierte Entscheidungsfindung, Bonitätsprüfung, Zahlungsarten |
| OGH 13.08.2025, 6Ob173/24w                       | Handelsregister, Offenlegungspflicht, juristische Person  |
| OLG Wien 28.07.2025, 30Bs196/25f                 | Beschlagnahme, Datenträger, Daten   |

|   |   |
|---|---|
| OGH 26.08.2025, 9ObA83/24g                                | Führungsorgan, Dritte, sensible Daten, Rechtsverteidigung                   |
| OGH 13.08.2025, 6Ob121/25z                                | Datenschutz, Schadenersatz, Bewertungsanspruch                              |
| OLG Wien 16.07.2025, 2R62/25i                             | Auskunft, Fristverlängerung, Kostentragung                                  |
| OGH 09.09.2025, 1Ob91/25a                                 | COFAG, abgabenrechtliche Geheimhaltungspflicht                              |
| OLG Wien 13.09.2025, 16R92/25d                            | Auskunft, Prozessposition, Geschäftsgeheimnis                               |
| OLG Graz 20.08.2025, 10Bs215/25f                          | Datenschutzverletzung, unbedeutende Schädigung, Diversion                   |
| OLG Wien 28.04.2025, 12R2/25i                             | Auskunftsrecht, Videoaufnahme, strukturierte Datensammlung, Neuerungsverbot |
| OGH 03.10.2025, 11Os83/25b                                | Beschlagnahme, Daten, Datenträger, StPO                                     |
| OLG Linz 30.06.2025, 4R89/25y                             | Auskunft, Beweismittelbeschaffung, Rechtsmissbrauch                         |
| OLG Wien 24.02.2025, 1R125/24w                            | Rollenqualifikation, Rechtsfrage  |
| OLG Linz 11.09.2025, 10Bs198/25a                          | Akteneinsicht, Datenschutz, überwiegende private Interessen                 |
| OLG Wien 10.01.2025, 33R157/24m;<br>11.04.2025, 16R21/25p | Auskunftsrecht, Identitätsprüfung, Vollmacht, Kostenrekurs                  |
| OLG Wien 19.05.2025, 33R10/25w                            | AGB, elektronische Post, Rechtsgrundlage                                    |
| OLG Wien 26.06.2025, 2R37/25p                             | Geschäftsführer, interne Datenübermittlung                                  |
| OLG Linz 10.09.2025, 4R114/25z                            | Akteneinsicht, Geheimhaltung, schutzwürdige Interessen                      |
| OLG Wien 11.02.2025, 3R5/25i                              | Auskunft, Vollmacht, Erleichterungsgebot                                    |
| OGH 16.10.2025, 6Ob230/24b                                | Geschäftsunterlagen, Offenlegungspflicht, Rechtsgrundlage                   |
| OLG Wien 10.06.2025, 15R74/25z                            | Shitstorm, immaterieller Schadenersatz                                      |
| OLG Wien, 27.08.2025, 15R35/25i                           | Persönlichkeitsrecht, Interessenabwägung                                    |

|  |  |
|--|--|
| OLG Innsbruck 01.10.2025, 4R117/25z                                    | Auskunft, Selbstbedienungstools, Datenkopie                                      |
| OLG Wien 24.10.2025, 13R149/25i  | Schadenersatz, Gesamtschaden, DSGVO  |
| OLG Wien 25.09.2025, 7Ra17/25h   | betriebliche Echtzeit-Videoüberwachung, Screenshots                              |
| OLG Wien 07.10.2025, 20Bs245/25p; OLG Innsbruck 07.10.2025, 7Bs232/25p | Beschlagnahme von Datenträgern   |
| OLG Wien 21.03.2024, 13R3/24t  | DSGVO, Verwaltungsverfahrenskosten, Rettungsaufwand                              |
| OLG Innsbruck 05.06.2025, 2R65/25p                                     | Akteneinsicht, rechtliches Interesse, Rechtsanspruch                             |
| OGH 11.11.2025, 10b155/25p   | Videoüberwachung, Servitut, Interessenabwägung                                   |
| OLG Innsbruck 18.06.2025, 114Ds1/23f                                   | Disziplinarverfahren, IKT-NV, Ansehen des öffentlichen Dienstes                  |
| OGH 26.11.2025, 6Ob141/24i   | Google Fonts, Aufforderungsschreiben, Aussetzung                                 |
| OGH 26.11.2025, 6Ob189/24y   | Bestimmtheit des Klagebegehrens, Feststellungsklage, Vertragserfüllung, Auskunft |
| OLG Wien 18.07.2025, 15R16/25w   | Kontenregisterauskunft, Verlassenschaft  |
| OLG Wien 05.11.2025, 22Bs306/25y                                       | Europäische Ermittlungsanordnung, Auswertung von Datenträgern und Daten          |

### **BVwG (ausgewählte Entscheidungen)**

| <b>Entscheidung</b>   | <b>Stichworte</b>                                   |
|---|---|
| BVwG 22.11.2024, W211 2272744-1; 18.11.2024, W137 2272120-1 | Betroffenheit, Mitwirkungspflicht                   |
| BVwG 25.11.2024, W252 2282050-1                             | Dark Patterns, Cookie-Banner, Widerruf              |
| BVwG 18.11.2024, W274 2284469-1                             | Entschiedene Sache, Exekutionsverfahren             |
| BVwG 18.11.2024, W137 2297057-1                             | Auskunftsrecht, Rechte von Dritten, Öffnungsklausel |
| BVwG 25.11.2024, W214 2273462-1                             | Bürgermeister, staatliche Behörde                   |



|                                 |  |
|---------------------------------|--|
| BVwG 06.11.2024, L532 2300411-1 | Gesetzesprüfungsantrag, Handyauswertung                      |
| BVwG 18.10.2024, W256 2248161-1 | Verarbeitung, Informationspflicht, Ausnahme                  |
| BVwG 30.10.2024, W256 2247276-1 | Präklusion   |
| BVwG 27.11.2024, W256 2246546-1 | konkrete Rechtsverletzung, kein Recht auf Strafverfahren     |
| BVwG 10.12.2024, W211 2272735-1 | Verstorbener, Verlust der Parteistellung                     |
| BVwG 16.12.2024, W137 2288040-1 | Rollenverteilung, Identitätsdokumentenregister               |
| BVwG 16.12.2024, W137 2292450-1 | Trafik, Video, Piktogramm, Geldstrafe                        |
| BVwG 04.12.2024, W176 2295345-1 | Rechtsanwalt, Anwaltsgeheimnis, Beschwerdegegner             |
| BVwG 25.10.2024, W211 2295570-1 | Besetzung des Präsidiums des BVwG, "social watchdog"         |
| BVwG 27.11.2024, W252 2299666-1 | Beschwer, Untersagung, keine Geldbuße                        |
| BVwG 02.09.2024, W256 2251016-1 | Auskunft, Datenübertragung, neuer Verantwortlicher           |
| BVwG 18.12.2024, W252 2294338-1 | Rollenverteilung, Anwendungsbereich, Videoüberwachung        |
| BVwG 18.12.2024, W256 2285492-1 | Videoüberwachung, Arbeitsplatz, Anweisung, Geldbuße          |
| BVwG 27.11.2024, W252 2280461-1 | Anwendungsbereich, StVO, Verwaltungsstrafverfahren, Straftat |
| BVwG 10.01.2025, W108 2290157-1 | WEG, mündliche Mitteilung, gesetzliche Pflicht               |
| BVwG 09.01.2025, W256 2244544-1 | Auskunftsrecht, Dokumentenkopie, Antragsinhalt               |
| BVwG 09.01.2025, W211 2283857-1 | Video, Servitut, Ausdehnung der Datenschutzbeschwerde        |
| BVwG 07.01.2025, W108 2286042-1 | Prüfbefugnis, Oficialmaxime                                  |
| BVwG 07.01.2025, W108 2284293-1 | Erlaubnistatbestände, Parteiengehör, Art 29 DSGVO            |

|                                 |  |
|---------------------------------|--|
| BVwG 14.01.2025, W298 2300879-1 | Beschwerdegegner, Passivlegitimation   |
| BVwG 13.01.2025, W137 2304495-1 | Video, Servitut, Datenminimierung  |
| BVwG 10.01.2025, W252 2271738-1 | Beschwerdegegner, <i>res iudicata</i>  |
| BVwG 27.12.2024, W258 2227269-1 | Geldbuße, Kontrollmaßnahmen, VVZ, DSFA   |
| BVwG 19.12.2024, W287 2297969-1 | Bundespräsident, Journalist, Postenbesetzung   |
| BVwG 17.01.2025, W298 2293073-1 | Strafverfolgung, öffentliches Interesse, zwangsweise Unterbringung                   |
| BVwG 09.12.2024, W292 2285487-1 | Unerbetene Nachricht, Selbstbelastungsverbot, Kosten des Beschwerdeverfahrens        |
| BVwG 23.01.2025, W605 2284399-1 | Mitwirkung, Geldbuße, Kosten des Beschwerdeverfahrens                                |
| BVwG 07.01.2025, W108 2288748-1 | Auskunft, Empfänger, Speicherfrist, Beweisverfahren                                  |
| BVwG 09.09.2024, W176 2283061-1 | Auskunft, Datenkopie   |
| BVwG 13.01.2025, W137 2302430-1 | Wildkamera, Servitut, Selbsthilfe  |
| BVwG 22.01.2024, W108 2288584-1 | Rechtsschutzinteresse, formelle Beschwer   |
| BVwG 28.01.2025, W108 2286343-1 | Identifikationsregister, e-Card, Auskunft, Verantwortliche                           |
| BVwG 31.01.2025, W258 2247059-1 | Löschung, Klaglosstellung, Feststellungskompetenz, allgemeines rechtliches Interesse |
| BVwG 05.02.2025, W291 2298821-1 | Geldbuße, veröffentlichte Gesundheitsdaten, Rechtsanspruch, Weiterverarbeitung       |
| BVwG 30.01.2025, W101 2248744-1 | berechtigtes Interesse, Identifizierbarkeit, Grundbuch                               |
| BVwG 30.01.2025, W101 2248650-1 | berechtigtes Interesse, Erforderlichkeit   |
| BVwG 28.01.2025, W108 2274731-1 | Gesichtserkennungsplattform, Verarbeitungsverbot, Abhilfemaßnahme, Antragsrecht      |
| BVwG 20.02.2024, W287 2306632-1 | Nichterteilung der Auskunft, unvollständige Auskunft, Säumnisbeschwerde              |

|                                 |  |
|---------------------------------|--|
| BVwG 05.02.2025, W298 2292389-1 | Bundespräsident, Amtsverschwiegenheit, Datenschutz                             |
| BVwG 11.02.2025, W256 2247121-1 | Bauverfahren, Interessenabwägung, Datenaustausch aufgrund von Rechtsansprüchen |
| BVwG 03.02.2025, W292 2285781-1 | Direktwerbung, TKG, Widerspruch  |
| BVwG 03.02.2025, W292 2285575-1 | Löschung, Insolvenzdaten, keine rückwirkende Feststellung                      |
| BVwG 26.02.2025, W101 2250871-1 | Warnliste der Banken, Berichtigung, Löschung                                   |
| BVwG 18.02.2025, W129 2303356-1 | Universität, Satzung, Videoaufzeichnungen                                      |
| BVwG 14.02.2025, W211 2299661-1 | Streitanhängigkeit, entschiedene Sache, Beschwerdeergänzung                    |
| BVwG 11.02.2025, W254 2295624-1 | Auskunft, Empfänger, Zeitpunkt der Erteilung, Löschung, Widerspruch            |
| BVwG 17.02.2025, W274 2302842-1 | Geheimhaltung, veröffentlichte Daten, Einwilligung                             |
| BVwG 26.02.2025, W101 2284403-1 | Videoüberwachung, Geldbuße, Strafzumessung, Kennzeichnung, öffentlicher Raum   |
| BVwG 03.02.2025, W292 2289286-1 | Statistik Austria, Namensgleichheit, Register der statistischen Einheiten      |
| BVwG 11.03.2025, W292 2280453-2 | Videokamera, Rechtsanspruch, Vermieter   |
| BVwG 24.02.2025, W298 2296144-1 | historische Zahlungsinformationen, Inkasso, Kreditauskunftei, Löschung         |
| BVwG 27.02.2025, W258 2230578-1 | Bürgerjournalismus, Medienfreiheit, Meinungsfreiheit                           |
| BVwG 21.02.2025, W211 2288083-1 | Auskunft, konkrete Empfänger, zukünftige Empfänger, Erhebungspflicht           |
| BVwG 05.03.2025, W211 2291833-1 | Medienprivileg, Bürgerjournalismus   |
| BVwG 06.03.2025, W292 2289837-1 | Auskunft, Identifizierung, Zurückverweisung                                    |
| BVwG 11.03.2025, W211 2293097-1 | Hackerangriff, Benachrichtigung, Präklusion                                    |
| BVwG 10.03.2025, W287 2286005-1 | Geldbuße, Mitwirkungspflicht, Anweisung, Selbstbezeichnung, Strafbemessung     |

|                                 |  |
|---------------------------------|--|
| BVwG 10.02.2025, W176 2285593-1 | Auskunft, Vollmacht, Korrespondenz, Datenkopie, Löschung   |
| BVwG 11.03.2025, W137 2305838-1 | Exzess, Rechtsmissbrauch, unzumutbarer Aufwand   |
| BVwG 11.03.2025, W211 2288587-1 | Beweislast, Datenoffenlegung   |
| BVwG 27.02.2025, W298 2305443-1 | Rechtsanwalt, Auskunft, Reaktionspflicht, Geldbuße   |
| BVwG 13.03.2025, W137 2253556-1 | AuskunftspflichtG, Grundrecht auf Informationen  |
| BVwG 27.03.2025, W298 2285480-1 | Erleichterungsgebot, Geldbuße, VStG, Anwendungsvorrang   |
| BVwG 04.03.2025, W176 2285563-1 | Arzt, Rolle, Gesundheitsdaten, Weiterverarbeitung  |
| BVwG 05.09.2024, W211 2287218-1 | Videoüberwachung, Personenbezug, Interessenabwägung, statistische Zwecke                                 |
| BVwG 06.03.2025, W292 2284288-2 | Betroffenheit, Amtswegigkeit, Mitwirkungspflicht   |
| BVwG 05.03.2025, W211 2272384-1 | Betroffenheit, Mitwirkungspflicht  |
| BVwG 24.03.2025, W101 2269148-1 | Datenschutzbeauftragte, Aussageverweigerungsrecht, Rechtsirrtum  |
| BVwG 01.04.2025, W252 2297124-1 | Anwendungsbereich, Paketzustellung, Rollenverteilung   |
| BVwG 10.02.2025, W287 2265979-1 | Online-Handel, Zustellbenachrichtigung, Rollenverteilung   |
| BVwG 31.03.2025, W287 2246105-1 | Verantwortlicher, Betriebsrat, Betriebsratsfonds, Wahlvorstand, Fürsorgepflicht, Internal Investigations |
| BVwG 28.03.2025, W292 2301229-1 | automatisierte Entscheidung, Bonitätsscore, Zahlungserfahrungsdaten, Speicherfrist                       |
| BVwG 07.04.2025, W256 2245984-1 | Apotheke, berechtigtes wirtschaftliches Interesse, gelindere Mittel                                      |
| BVwG 31.03.2025, W137 2256492-1 | Verantwortlicher, Auftragsverarbeiter  |

|  |  |
|--|--|
| BVwG 31.03.2025, W137 2254660-1                                | Nachbarschaft, berechtigtes Interesse, allgemein verfügbare Daten                    |
| BVwG 31.03.2025, W258 2134678-1                                | Verhandlungsprotokoll, Datenweitergabe innerhalb der Organisationsstruktur           |
| BVwG 31.03.2025, W258 2245052-1                                | OGH, Personalakt, Geheimhaltung  |
| BVwG 27.03.2025, W254 2297150-1                                | E-Mail, Personenbezug, Auskunft  |
| BVwG 02.04.2025, W291 2307872-1                                | Datenschutzbeschwerde, Feststellungsbegehren   |
| BVwG 27.01.2025, W605 2248297-1                                | Grundbuch, informationeller Mehrwert, konkrete Empfänger, Dateninhalt, Akteneinsicht |
| BVwG 03.04.2025, W176 2259543-1                                | Adressverlag, Kreditauskunftei, Bonitätsbewertung                                    |
| BVwG 21.05.2024, W605 2232133-1                                | justizielle Tätigkeit, Gerichtsvollzieher  |
| BVwG 21.05.2024, W605 2287853-1                                | objektive Präklusivfrist   |
| BVwG 04.03.2024, W605 2274353-1                                | BVwG, Anonymisierung, Kostenersatz   |
| BVwG 14.04.2025, W137 2297606-1                                | Säumnis, Schadenersatz, Privatbeteiligung  |
| BVwG 21.05.2024, W605 2286028-1                                | Ermittlungspflicht   |
| BVwG 09.07.2024, W258 2261773-1                                | ne bis in idem   |
| BVwG 09.04.2025, W287 2272807-1;<br>22.04.2025, W287 2271841-1 | Betroffenheit, Mitwirkungspflicht  |
| BVwG 29.04.2025, W254 2252989-2                                | Akteneinsicht, Vollmacht, Telefax  |
| BVwG 24.04.2025, W298 2308675-1                                | Unterrichtungspflicht, Feststellung  |
| BVwG 24.04.2025, W298 2310614-1                                | Zuständigkeit, justizielle Tätigkeit, Notar, Gerichtskommissär                       |
| BVwG 11.06.2025, W211 2308914-1                                | Videoüberwachung, Transparenz, Geldbuße  |
| BVwG 06.05.2025, W254 2309877-1                                | Kohärenzverfahren, Fristenhemmung  |
| BVwG 14.04.2025, W137 2257572-1                                | Kreditinstitut, Datenlöschung, Sorgfaltspflicht, öffentliches Interesse              |

|                                 |   |
|---------------------------------|---|
| BVwG 09.04.2025, W287 2271595-1 | Direktmarketingunternehmen, Lösungsersuchen, Sperrdatei                           |
| BVwG 22.04.2025, W256 2248647-1 | Gesundheitsdaten, Krankenanstalt, Übermittlungsform                               |
| BVwG 17.04.2025, W605 2257579-1 | Bilddatenverarbeitung, Öffnungsklausel, gelindere Mittel                          |
| BVwG 23.04.2025, W291 2299266-1 | Cookie-Banner, Leistungsauftrag   |
| BVwG 02.12.2024, W254 2299670-1 | Datenschutzbeschwerde, Mindestinhalt, Verbesserungsauftrag                        |
| BVwG 02.05.2025, W137 2301309-1 | Universität, Videoaufnahme, Verordnung  |
| BVwG 28.04.2025, W211 2289521-1 | Rechtsanwalt, Exekution, justizielle Tätigkeit                                    |
| BVwG 30.04.2025, W171 2298465-1 | Krankentransport, Spendenbrief, Gesundheitsdaten, Zweckänderung                   |
| BVwG 28.04.2025, W211 2283135-1 | Exzess, Missbrauchsabsicht, Ressourcen  |
| BVwG 29.04.2025, W101 2308679-1 | Kohärenzverfahren, Fristhemmung   |
| BVwG 23.04.2025, W605 2307742-1 | Untätigkeitsklage, Kohärenzverfahren, Nichtweiterleiten der Datenschutzbeschwerde |
| BVwG 23.04.2024, W605 2283487-1 | Berichtigung, Geschlechtsidentität, "Sanierung"                                   |
| BVwG 06.05.2025, W256 2307865-1 | Auskunftserteilung im laufenden Verfahren   |
| BVwG 08.05.2025, W274 2264017-1 | Vollstreckung, ausländische Geldbuße, Inkasso                                     |
| BVwG 06.05.2025, W252 2271318-1 | CAPTCHA, Zuständigkeit, Barrierefreiheit  |
| BVwG 06.05.2025, W252 2293098-1 | Staatsanwaltschaft, Akteneinsicht, Beschränkung                                   |
| BVwG 07.05.2025, W176 2273922-1 | Gerichtsverfahren, Rechtsanspruch, berechtigtes Interesse                         |
| BVwG 08.05.2025, W274 2257892-1 | Datenweitergabe, Datenminimierung, gelindere Mittel                               |
| BVwG 12.05.2025, W292 2311008-1 | Beschwer, Rechtsschutzinteresse   |
| BVwG 08.05.2025, W292 2310611-1 | Beschwer  |

|   |   |
|---|---|
| BVwG 16.05.2025, W296 2310875-1   | Datenzugriff, Amtsmissbrauch, Verjährung  |
| BVwG 13.05.2025, W258 2224654-1   | Obsorge, Verwaltungshandeln, Personenstand  |
| BVwG 09.05.2025, W291 2301858-1   | Auskunftsrecht, Auskunftersuchen  |
| BVwG 08.05.2025, W171 2251246-1   | Auskunft, aufschiebende Wirkung   |
| BVwG 06.05.2025, W298 2309832-1   | Zuständigkeit, justizielle Tätigkeit, Kostenersatz                                      |
| BVwG 06.05.2025, W271 2303184-1;<br>07.05.2025, W282 2303188-1; 08.05.2025,<br>W179 2303090-1 | Cold Calling, Geldstrafe, Rechtsauskunft  |
| BVwG 03.06.2025, W211 2292541-1   | Initiativantrag, Beschwerdegegner, konkludente Einwilligung, gesetzliche Grundlage      |
| BVwG 28.05.2025, W137 2259971-1   | Auskunft, Data Breach, Personenbezug  |
| BVwG 10.06.2025, W274 2307868-1   | Auskunftserteilung im laufenden Verfahren, Feststellungskompetenz                       |
| BVwG 28.05.2025, W108 2230691-1   | Automatisierte Entscheidungsfindung, Bonitäts-score, Auskunftsrecht, Geschäftsgeheimnis |
| BVwG 20.06.2025, W256 2246580-1   | ÄrzteG, Informationspflicht, Datenübertragbarkeit                                       |
| BVwG 12.06.2025, W211 2291308-1   | Rollenverteilung, Informationspflicht, Schadenersatz                                    |
| BVwG 16.06.2025, W211 2310626-1   | Exekutionsverfahren, justizielle Tätigkeit  |
| BVwG 20.06.2025, W252 2290822-1   | Auskunft, Akteneinsicht, nationale Sicherheit, Exzess                                   |
| BVwG 23.06.2025, W211 2297059-1   | Insolvenzverfahren, strafrechtliche Verurteilung, Rechtsanspruch                        |
| BVwG 26.05.2025, W101 2267859-1;<br>26.05.2025, W101 2280857-1                                | Data Breach, COVID, Nachweis  |
| BVwG 28.05.2025, W137 2255428-1   | Suchmaschine, De-Indexierung, Person des öffentlichen Lebens                            |
| BVwG 24.06.2025, W176 2291296-1   | Amtswissen, Datenherkunft, Dokumentation, Befangenheit                                  |
| BVwG 04.06.2025, W298 2301992-1   | Rückwirkung, öffentliches Interesse, Löschung   |

|  |   |
|--|---|
| BVwG 30.05.2025, W256 2246885-1                                | Gesundheitsdatum, Rechtsanspruch, Erforderlichkeit                              |
| BVwG 26.06.2025, W298 2291079-1                                | Rollenverteilung, Rechtsnorm  |
| BVwG 23.06.2025, W211 2291530-1                                | Rechenschaftspflicht, Auskunft, Protokollierung, Feststellung                   |
| BVwG 25.06.2025, W254 2307864-1                                | Auskunft, Feststellung, Sanierung   |
| BVwG 17.06.2025, W252 2280887-1;<br>17.06.2025, W252 2280766-1 | Missbrauchsabsicht, Unrichtigkeit des Rechtsstandpunkts, Obsorge                |
| BVwG 22.05.2025, W101 2295861-1                                | Geldbuße, COVID, Gesundheitsdaten, Strafbemessung                               |
| BVwG 02.06.2025, W292 2298457-1                                | Geldbuße, Google-Rezension, berechtigte Interessen                              |
| BVwG 17.06.2025, W252 2296540-1                                | Videoüberwachung, Dienstverhältnis, Einwilligung                                |
| BVwG 30.06.2025, W137 2295299-1                                | Geheimhaltungsinteresse, Familienangehöriger, Personenbezug, Bescheidzustellung |
| BVwG 05.06.2025, W211 2296350-1                                | AuskunftspflichtG, vorhandene Informationen                                     |
| BVwG 27.05.2025, W603 2304292-1                                | unerbetene Nachricht, Privatsphäre, Ermahnung                                   |
| BVwG 03.07.2025, W252 2312918-2                                | Verfahrenshilfe, Dokumentenkopie  |
| BVwG 27.05.2025, W605 2270910-1                                | Adressverlag, Kreditauskunftei, Zweckänderung, Abhilfebefugnis                  |
| BVwG 30.06.2025, W137 2253891-1                                | FMA, Behörde, Empfänger, Auskunft   |
| BVwG 01.07.2025, W256 2252595-1                                | Rechtsanspruch, strafrechtliche Verurteilung, berechtigtes Interesse            |
| BVwG 20.06.2025, W291 2300813-1                                | Geldbuße, Videoüberwachung, Rollenverteilung                                    |
| BVwG 01.07.2025, W176 2226261-1                                | Exzess, Missbrauchsabsicht  |
| BVwG 03.07.2025, W211 2301099-1                                | ORF-Beitrag, Inkasso, Rückstandsausweis   |
| BVwG 09.07.2025, W298 2309078-1                                | berechtigtes Interesse, Warnliste der Kreditinstitute, Kleinkreditevidenz       |



|  |  |
|--|--|
| BVwG 01.09.2025, W256 2235360-1                                | Profiling, Art 22 DSGVO, menschliche Entscheidung                  |
| BVwG 14.07.2025, W274 2309030-1                                | Medienprivileg, Löschung, Namensanonymität                         |
| BVwG 22.07.2025, W211 2309849-1                                | internationaler Schutz, Rückkehrentscheidung, biometrische Daten   |
| BVwG 14.07.2025, W274 2309622-1                                | Gesundheitsdaten, Erlaubnistatbestand                              |
| BVwG 16.07.2025, W211 2302514-1                                | Ediktsdatei, Insolvenz, öffentliche Daten                          |
| BVwG 09.07.2025, W274 2244313-1                                | Missbrauchsabsicht, feindselige Motivation, Gebühr                 |
| BVwG 17.07.2025, W137 2300883-1                                | AuskunftspflichtG, Akteneinsicht                                   |
| BVwG 10.07.2025, W137 2306286-2                                | AuskunftspflichtG, Richtlinien                                     |
| BVwG 23.05.2025, W164 2279298-1                                | AMS, Bewerbung, Datenschutz  |
| BVwG 29.07.2025, W211 2310137-1                                | Auskunftsrecht, Negativauskunft, private Notizen                   |
| BVwG 24.07.2025, W605 2256082-1                                | Gesundheitsdaten, Vergleich, Erforderlichkeit, Beweiserheblichkeit |
| BVwG 13.08.2025, W291 2272970-1                                | Cookie-Banner, Pay or Okay, Medien                                 |
| BVwG 29.07.2025, W211 2307081-1                                | Kriminalpolizei, Sozialversicherungsdaten, Verhältnismäßigkeit     |
| BVwG 24.07.2025, W101 2163119-1                                | Bürgerumfrage, Meldebehörde, zeitlicher Anwendungsbereich          |
| BVwG 07.08.2025, W605 2289883-1                                | KKE, Lösungsersuchen, Sanierung                                    |
| BVwG 23.07.2025, W101 2255209-1                                | Untersuchungsausschuss, Mandatsbescheid                            |
| BVwG 05.08.2025, W137 2308681-1;<br>05.08.2025, W137 2310023-1 | Entscheidungspflicht, Kohärenzverfahren, Hemmung                   |
| BVwG 01.08.2025, W605 2308677-1                                | Kohärenzverfahren, Untätigkeitsklage, Hemmung                      |
| BVwG 06.08.2025, W256 2279237-1                                | Tod, Parteistellung  |
| BVwG 05.08.2025, W137 2308027-1                                | Beschwer, Schadenersatz, Zuständigkeit                             |

|                                 |   |
|---------------------------------|---|
| BVwG 29.07.2025, W211 2311353-1 | Zurückweisung, Parteistellung, Bescheidzustellung   |
| BVwG 21.08.2025, W176 2250812-1 | Auskunft, automatisierte Entscheidungsfindung, involvierte Logik                          |
| BVwG 25.07.2025, W258 2299744-1 | Geldbuße, Videoüberwachung, Rechtsgrundlage   |
| BVwG 11.07.2025, W295 2243015-1 | Energieversorgung, E-Control, Auskunfts- und Einsichtspflicht, Erforderlichkeitsvorbehalt |
| BVwG 26.08.2025, W291 2309033-1 | Widerspruchsrecht, Antragspflicht   |
| BVwG 28.04.2025, W258 2224229-1 | PNR-System, Fluggastdaten   |
| BVwG 10.06.2024, W148 2291941-1 | WiEreG, public watchdog, Einsichtsrecht   |
| BVwG 11.07.2025, W292 2291080-1 | Medien, Bürgerjournalismus, Verschwörungstheorien   |
| BVwG 14.08.2025, W298 2309032-1 | ELGA, Auskunft, Feststellungsinteresse, Erkundungsbeweis                                  |
| BVwG 18.07.2025, W292 2235791-1 | Auskunft, Empfänger, Auftragsverarbeiter  |
| BVwG 19.08.2025, W292 2307870-1 | Auskunft, Formalismus   |
| BVwG 04.09.2025, W252 2301118-1 | fehlende Betroffenheit, Zurückweisung   |
| BVwG 04.09.2025, W252 2312918-1 | Auskunftsrecht, Datenkopien, Beweislast   |
| BVwG 10.09.2025, W258 2299744-1 | aufschiebende Wirkung, Strafvollzug   |
| BVwG 11.09.2025, W258 2241500-1 | Staatsanwaltschaft, StPO, Akteneinsicht   |
| BVwG 04.09.2025, W258 2232927-1 | Kohärenzverfahren, Dringlichkeitsverfahren, Wiederaufnahme                                |
| BVwG 15.09.2025, W258 2242162-1 | Video, Treu und Glauben, Transparenz  |
| BVwG 02.09.2025, W256 2250819-1 | Rollenverteilung, Mitarbeiter   |
| BVwG 26.08.2025, W252 2307842-1 | Exzess, Missbrauchsabsicht, Feindseligkeit  |
| BVwG 19.08.2025, W292 2314174-1 | Recht auf Einschränkung, antragsbedürftig, Sache des Verfahrens                           |

|                                 |   |
|---------------------------------|---|
| BVwG 28.08.2025, W137 2311069-1 | Schengener Informationssystem, Asylantrag, Löschbegehren                    |
| BVwG 07.10.2025, W137 2310624-1 | Unterhalt, Universität, ECTS, Verfahrensgesetze                             |
| BVwG 07.08.2025, W605 2311036-1 | Untätigkeitsklage, Kohärenzverfahren  |
| BVwG 25.09.2025, W252 2315664-1 | Schengener Informationssystem, Asylantrag, Löschbegehren                    |
| BVwG 03.09.2025, W292 2248134-1 | Exzess, Auslandsbezug, hohe Anzahl  |
| BVwG 24.09.2025, W295 2297643-1 | unerbetene Werbeanrufe, Einwilligung, wirksames Kontrollsystem, Verschulden |
| BVwG 23.10.2025, W101 2268654-1 | Auskunft, Beweislast, Geschäftsgeheimnis                                    |
| BVwG 07.10.2025, W292 2285608-1 | Auskunft, grenzüberschreitende Verarbeitung, Eizellenspende                 |
| BVwG 23.10.2025, W176 2288880-1 | Firmendaten, öffentlich zugängliche Daten, Interessenabwägung               |
| BVwG 25.09.2025, W252 2289069-1 | Rechtsanwalt, Rechtsanspruch, Interessenabwägung                            |
| BVwG 25.09.2025, W252 2292573-1 | Disziplinaranzeige, Rechtsgrundlage   |
| BVwG 14.10.2025, W137 2236019-1 | Datenrichtigkeit, Datenzwillinge  |
| BVwG 06.10.2025, W256 2278150-1 | Gutachten, subjektive Meinung, Berichtigung                                 |
| BVwG 10.09.2025, W137 2297602-2 | Bundesheer, dienstliche Weisung   |
| BVwG 01.10.2025, W170 2314010-1 | Disziplinarerkenntnis, dienstliche Weisung, Datenbankzugriff                |
| BVwG 05.09.2025, W256 2255025-1 | Personenbezug, Impfstatus   |
| BVwG 07.10.2025, W137 2307782-1 | Akteneinsicht, Interessenabwägung   |
| BVwG 08.09.2025, W605 2309836-1 | Auskunftspflichtgesetz, Akteneinsicht                                       |
| BVwG 29.07.2025, W605 2251236-1 | Besitzstörung, Tonaufnahme, Beweisnotstand, Haushaltsausnahme               |
| BVwG 22.10.2025, W254 2316529-1 | SIS, Ausschreibung, erhebliches öffentliches Interesse                      |

|                                 |   |
|---------------------------------|---|
| BVwG 20.10.2025, W258 2246973-1 | Mitarbeiter, Gesundheitsdaten, breite Öffentlichkeit      |
| BVwG 28.08.2025, W298 2280052-1 | Besitzstörung, elektronischer Wachhund, Überwachungsdruck |
| BVwG 24.07.2025, W129 2310165-1 | Studierendendaten, private E-Mail-Adressen                |
| BVwG 17.10.2025, W252 2311432-1 | Berichtigung, objektiver Erklärungswert                   |
| BVwG 04.11.2025, W605 2324043-1 | Abweisung, aufschiebende Wirkung                          |
| BVwG 05.11.2025, W258 2292731-1 | Massenverfahren, Aussetzung                               |

### Weitere ausgewählte Entscheidungen

| Entscheidung                                     | Stichworte   |
|--|--|
| BFG 19.12.2024, RV/7102904/2021                  | WiEReG, Meldepflicht   |
| LVwG Wien 13.01.2025, VGW-101/042/17553/2024     | Grundbuch, Abbruchbewilligung, Auskunft  |
| LVwG Tirol 20.02.2025, LVwG-2024/44/2718-6       | Wassergenossenschaft, Mitgliederverzeichnis, Vertragserfüllung                         |
| BFG 19.02.2025, RV/5100235/2024                  | Sonderausgaben, bPK  |
| BFG 03.03.2025, RV/7102539/2021                  | Abgaben  |
| LVwG Tirol 26.03.2025, LVwG-2024/12/2583-3       | Sicherstellung und Auswertung von Mobiltelefonen, DSRL-PJ, vorherige Gerichtskontrolle |
| LVwG Steiermark 10.12.2024, LVwG 413.9-2959/2024 | Verwaltungsgericht, Beweisverfahren  |
| LVwG Kärnten 23.08.2022, KLVwG-1400/3/2022       | Smart Meter, IME-VO  |
| LVwG NÖ 25.03.2025, LVwG-AV-1248/002-2024        | Amtsgeheimnis, Steuergeheimnis, Besitzstörung, Hundehaltung                            |
| EK Pressemitteilung 23.04.2025, IP/25/1085       | Apple, Meta, Facebook Marketplace, "Consent or Pay"                                    |
| BFG 14.05.2025, RV/7100831/2020                  | Online-Glücksspiel, Glücksspielabgabe, Teilnahme vom Inland                            |

|  |  |
|--|--|
| LVwG NÖ 07.05.2025, LVwG-AV-1103/001-2024                                      | KFZ, Zulassungsevidenz, Pressefreiheit, Art 6 Abs 1 lit e DSGVO            |
| BDB 07.05.2025, 2024-0.832.779   | Polizei, Abfrage, Zentrales Melderegister                                  |
| BDB 29.04.2025, 2025-0.175.429   | Aktenverwaltungssystem der Polizei, Abfrage                                |
| BFG 27.06.2025, RV/3100085/2025  | Eingabengebühr, Verfahrenshilfe  |
| LVwG NÖ 14.07.2025, LVwG-AV-508/001-2024                                       | KFZ, Zulassungsevidenz, Garagierungsgewerbe                                |
| BFG 02.07.2025, RV/7104521/2020  | Glücksspielabgabe, Wettgebühr, Inland                                      |
| BFG 08.07.2025, RV/4100275/2022;<br>08.07.2025, RV/4100327/2023                | Abgabenerhebung, Gesundheitsdaten, außergewöhnliche Belastung              |
| LVwG Vorarlberg 07.08.2025, LVwG-352-1/2025-R22; 28.08.2025, LVwG-352-3/2025-R | Amtsverschwiegenheit, public watchdog, Interessenabwägung                  |
| BFG 30.06.2025, RV/7100116/2020  | Finanzpolizei, Datenschutz   |
| LVwG NÖ 19.08.2025, LVwG-AV-1302/001-2024                                      | Akteneinsicht, Verfahrensabschluss, DSGVO                                  |
| LVwG Tirol 06.10.2025, LVwG-2025/S2/1049-8                                     | Vergabeverfahren, Rollenverteilung, Auftragsverarbeiter, Pseudonymisierung |
| BFG 14.10.2025, RV/7103129/2025  | Spenden, Identifikationsdaten  |
| LVwG NÖ 09.10.2025, LVwG-AV-436/001-2025                                       | KFZ-Zulassungsevidenz, rechtliches Interesse                               |
| LVwG Tirol 11.11.2025, LVwG-2025/46/2168-3                                     | Berichtigung, Eigendaten   |
| LVwG Vorarlberg 09.10.2025, LVwG-352-2/2025-R12                                | Informationsbegehren, public watchdog, politische Meinung, Standort        |

## DSB

| Entscheidung                   | Stichworte  |
|--------------------------------|---|
| DSB 27.06.2024, 2024-0.028.256 | Anzeige, Akteneinsicht, Interessenabwägung                              |
| DSB 16.10.2024, 2024-0.641.771 | Geldstrafe, handelsrechtlicher Geschäftsführer, Datenschutzbeauftragter |
| DSB 21.09.2022, 2022-0.672.331 | Videoüberwachung, Mitwirkungspflicht, freie Beweiswürdigung             |

|                                |   |
|--------------------------------|---|
| DSB 12.12.2024, 2024-0.796.258 | Aktfotos, Geldbuße  |
| DSB 26.09.2024, 2024-0.112.476 | Maut, KFZ-Kennzeichen, Passage-Daten  |
| DSB 11.02.2025, 2024-0.195.679 | Straßenfotografie, Kunstfreiheit, Fotos   |
| DSB 17.03.2025, 2025-0.192.907 | Parkraum, Videoüberwachung, Mitwirkung, Liquidation, Untersagung, aufschiebende Wirkung               |
| DSB 04.02.2025, 2025-0.021.375 | Pflegedienst, Videoüberwachung  |
| DSB 13.01.2022, 2021-0.450.072 | Berufsemailkonto, Löschung, Datenübertragung, Informationspflicht, Einschränkung                      |
| DSB 07.10.2024, 2024-0.671.673 | Data Breach, Mitwirkung, Doppelbestrafung   |
| DSB 18.04.2025, 2025-0.303.076 | Schengener Informationssystem, Löschung   |
| DSB 03.06.2025, 2025-0.177.424 | Mitwirkungspflicht, Geldbuße, Vorsatz   |
| DSB 04.07.2024, 2024-0.199.724 | Rechnungshof, politische Meinung, Parteiengesetz, Zuständigkeit, Parlamentarisches Datenschutzkomitee |
| DSB 12.06.2024, 2023-0.836.312 | justizielle Tätigkeit, Zuständigkeit, Beschwerdegegner, Übermaßverbot                                 |
| DSB 24.03.2025, 2025-0.165.785 | Akteneinsicht, Parteistellung, Zulässigkeitsprüfung   |
| DSB 24.02.2025, 2025-0.045.624 | Medienprivileg, Bürgerjournalismus, berufliche Kontaktdaten   |
| DSB 19.05.2025, 2025-0.327.266 | Videoüberwachung, Behörde, Privatwirtschaftsverwaltung, berechtigtes Interesse                        |
| DSB 12.06.2025, 2024-0.490.294 | Homeoffice, Zutrittssystem, Betriebsrat   |
| DSB 07.08.2025, 2025-0.626.844 | Auskunft, Fernzugriff, Format, Erleichterungsgebot, Marktortprinzip                                   |
| DSB 05.09.2025, 2025-0.271.604 | Kreditauskunftei, Zweckänderung, Informationspflicht  |
| DSB 16.08.2024, 2023-0.680.196 | Videoüberwachung, Geldbuße  |
| DSB 04.09.2025, 2025-0.699.550 | Data Breach, Mitarbeiter, Strafbemessung  |

|                                |   |
|--------------------------------|---|
| DSB 05.09.2025, 2025-0.712.691 | Auskunft, Markortprinzip  |
| DSB 29.07.2025, 2024-0.368.729 | Wirtschaftsdaten, Abfall- und Umweltinformationen                                     |
| DSB 04.09.2025, 2025-0.178.139 | Beschäftigtendaten, Dienst-PC, Rechtsverteidigung                                     |
| DSB 07.11.2025, 2025-0.911.653 | Grundbuch, Akquise, berechnete Interessen   |
| DSB 05.11.2025, 2024-0.869.675 | Namensverzeichnis, strafverfahrensbezogene Daten, Speicherfristen, Interessenabwägung |
| DSB 09.09.2025, 2023-0.346.325 | Staatsanwaltschaft, relativer Geheimhaltungsbegriff, Datenrichtigkeit                 |
| DSB 03.09.2025, 2025-0.699.488 | Geheimhaltungsinteresse, Kaufvertrag, Interessenabwägung                              |
| DSB 10.09.2025, 2025-0.607.071 | Videoüberwachung, öffentlicher Raum, Datenminimierung                                 |
| DSB 07.11.2025, 2025-0.910.735 | Disziplinaranzeige, Kinder, gelinderes Mittel   |
| DSB 03.09.2025, 2024-0.739.846 | Aufrufsystem im Wartebereich, Einwilligung, Kopplungsverbot, Anonymisierung           |
| DSB 09.09.2025, 2025-0.243.414 | Löschbegehren, berechtigtes Interesse, Online-Auftritt                                |
| DSB 08.10.2025, 2025-0.477.534 | Microsoft 365 Education, Rollenverteilung, Auskunft, Löschung                         |
| DSB 11.11.2025, 2025-0.758.101 | Bewerberdaten, Strafregisterauszug, Löschung  |
| DSB 17.09.2025, 2025-0.746.087 | Wahrunterstellung, juristische Person, Videoüberwachung                               |
| DSB 22.09.2025, 2025-0.742.062 | vorvertragliche Maßnahme, Rechtsgrundlage   |
| DSB 17.09.2025, 2025-0.677.482 | Plattform, Auskunft, Namensidentität  |
| DSB 11.09.2025, 2023-0.643.180 | Rollenverteilung, Übermaßverbot, behördeninterne Datenweitergabe, Förderung           |
| DSB 12.09.2025, 2024-0.739.833 | Videoüberwachung, öffentliche Fläche, Besitzstörung                                   |

|                                |   |
|--------------------------------|---|
| DSB 17.09.2025, 2025-0.502.649 | Auskunft, Umfang, Negativauskunft, Löschprotokoll                 |
| DSB 25.09.2025, 2025-0.355.103 | automatisierte Entscheidung, Scoring, Auskunft, Energieversorger  |
| DSB 24.09.2025, 2025-0.533.437 | Rechtsanwalt, Rolle, Verarbeitungsvorgänge                        |
| DSB 24.09.2025, 2025-0.757.118 | Videotürklingel, berechtigtes Interesse, digitaler Spion          |
| DSB 23.09.2025, 2025-0.746.088 | Typo, falsche E-Mail-Adresse                                      |
| DSB 19.09.2025, 2025-0.470.791 | Personenbezug, Identifizierbarkeit, Offenlegung                   |
| DSB 31.07.2024, 2023-0.521.417 | irrtümliche Datenerhebung, Datenübermittlung                      |
| DSB 29.09.2025, 2025-0.682.666 | Geldstrafe, Dashcam, Kennzeichnung, Verschulden                   |
| DSB 26.09.2025, 2025-0.117.456 | Insolvenzverwalter, justizielle Tätigkeit, Unzuständigkeit        |
| DSB 25.09.2025, 2025-0.432.701 | Rechtsanwalt, Rolle, Beschwerdegegner                             |
| DSB 29.09.2025, 2025-0.754.485 | SIS, Rückkehrentscheidung, Löschung                               |
| DSB 29.09.2025, 2024-0.501.636 | Verwirkung eines Rechts, Gläubigerschutz, Zuständigkeit           |
| DSB 01.10.2025, 2025-0.765.344 | Vollmacht, Missbrauch, kein Auskunftersuchen                      |
| DSB 08.10.2025, 2025-0.794.213 | Zuständigkeit, Rechtsschutz                                       |
| DSB 30.09.2025, 2025-0.757.551 | Auskunft, Tracking-Pixel, Auftragsexzess                          |
| DSB 03.10.2025, 2025-0.677.597 | Referenzdatenbank, Zweckbindung                                   |
| DSB 01.10.2025, 2025-0.757.155 | Unternehmensserviceportal, veröffentlichte Daten, social watchdog |
| DSB 05.12.2025, 2025-0.874.918 | Datenspeicherung, bonitätsrelevante Daten                         |
| DSB 14.10.2025, 2025-0.823.962 | Auskunft, heimliche Audioaufnahmen, Zivilverfahren, Datenkopie    |
| DSB 06.08.2025, 2025-0.276.820 | Leistungsauftrag, aufschiebende Wirkung, Geldbuße                 |



|                                |   |
|--------------------------------|---|
| DSB 08.10.2025, 2025-0.620.443 | Grundrecht auf Datenschutz, juristische Person            |
| DSB 30.09.2025, 2025-0.783.392 | Veterinärbereich, Nichtfeststellbarkeit, Erkundungsbeweis |

### Rechtsprechung zum IFG

| Entscheidung                                    | Stichworte  |
|---|---|
| LVwG NÖ 24.09.2025, LVwG-AV-1085/001-2025       | Auskunftsanspruch, IFG  |
| DSB 12.09.2025, 2025-0.703.379                  | IFG, Auskunftspflicht, sachlicher Anwendungsbereich               |
| VwGH 09.10.2025, Ra 2025/03/0087                | AuskunftspflichtG, IFG, Übergangsbestimmung, Geheimhaltungsgrund  |
| BVwG 10.11.2025, W176 2322793-1                 | IFG, Leistungsauftrag, keine Feststellungskompetenz               |
| BVwG 11.11.2025, W274 2323801-1                 | IFG, private Informationspflichtige, Frist                        |
| LVwG Wien 04.11.2025, VGW-113/032/16206/2025    | IFG, ORF, Zuständigkeit   |
| LVwG Wien 16.10.2025, VGW-113/027/15142/2025    | IFG, Fristverlängerung, Anhörungsrecht                            |
| LVwG Kärnten 13.11.2025, KLVwG-1828/5/2025      | IFG, innergemeindlicher Instanzenzug, keine Aufzeichnung          |
| LVwG Kärnten 06.11.2025, KLVwG-1830/5/2025      | IFG, Wirkungsbereich, keine Aufzeichnung                          |
| LVwG Tirol 11.12.2025, LVwG-2025/21/2529-8      | IFG, dienst- und disziplinarrechtliche Informationen, Datenschutz |
| LVwG Vorarlberg 24.10.2025, LVwG-488-1/2025-R22 | IFG, Informationspflicht, börsennotierte Gesellschaft             |
| LVwG NÖ 16.12.2025, LVwG-AV-1158/001-2025       | IFG, informationspflichtige Gesellschaft, Geheimhaltungsgründe    |

# Rechtsakte und Leitlinien 2025

In dieser Übersicht sind ausgewählte Rechtsakte und Leitlinien enthalten, die im Schönherr Datenschutzmonitor 2025 berücksichtigt wurden.

## EU-Rechtsakte

| Rechtsakt  | Stichworte   |
|--|--|
| <p>VO (EU) 2024/3228 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 zur Aufhebung der Verordnung (EU) Nr. 524/2013 und zur Änderung der Verordnungen (EU) 2017/2394 und (EU) 2018/1724 im Hinblick auf die Einstellung der Europäischen Plattform für Online-Streitbeilegung, <a href="#">ABI L 2024/3228, 1.</a></p>   | <p>Europäische Plattform für Online-Streitbeilegung, Einstellung</p>               |
| <p>RL (EU) 2024/3237 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 zur Änderung der Richtlinie (EU) 2015/413 zur Erleichterung des grenzüberschreitenden Austauschs von Informationen über die Straßenverkehrssicherheit gefährdende Verkehrsdelikte, <a href="#">ABI L 2024/3237, 1.</a></p>  | <p>Fahrzeugzulassungsdaten, Amts- und Rechts-hilfe</p>                             |
| <p>VO (EU) 2025/12 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über die Erhebung und Übermittlung vorab übermittelter Fluggastdaten zur Verbesserung und Erleichterung der Kontrollen an den Außengrenzen, zur Änderung der Verordnungen (EU) 2018/1726 und (EU) 2019/817 sowie zur Aufhebung der Richtlinie 2004/82/EG des Rates, <a href="#">ABI L 2025/12, 1.</a></p> | <p>Fluggastdaten, API-Daten, Grenzbehörden</p>                                     |
| <p>VO (EU) 2025/13 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über die Erhebung und Übermittlung vorab übermittelter Fluggastdaten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität und zur Änderung der Verordnung (EU) 2019/818, <a href="#">ABI L 2025/13, 1.</a></p>                                   | <p>Fluggastdaten, organisierte Kriminalität, Terrorismus, API-Daten, PNR-Daten</p> |
| <p>RL (EU) 2025/25 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 zur Änderung der Richtlinien 2009/102/EG und (EU) 2017/1132 zur Ausweitung und Optimierung</p>  | <p>Gesellschaftsrecht, Unternehmensregister, digitalen Werkzeuge</p>               |

|   |   |
|---|---|
| des Einsatzes digitaler Werkzeuge und Verfahren im Gesellschaftsrecht, <a href="#">ABI L 2025/25, 1.</a>  |   |
| VO (EU) 2025/37 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 zur Änderung der Verordnung (EU) 2019/881 im Hinblick auf verwaltete Sicherheitsdienste, <a href="#">ABI L 2025/37, 1.</a>  | verwaltete Sicherheitsdienste, Cybersicherheitszertifizierung |
| VO (EU) 2025/38 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der Verordnung (EU) 2021/694 (Cybersolidaritätsverordnung), <a href="#">ABI L 2025/38, 1.</a>   | Cybersolidaritätsverordnung, Cyberbedrohungen                 |
| Delegierte Verordnung (EU) 2025/295 der Kommission vom 24. Oktober 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Harmonisierung der Bedingungen für die Durchführung von Überwachungstätigkeiten, <a href="#">ABI L 2025/295, 1.</a>  | DORA, IKT-Drittdienstleister                                  |
| DelegierteVO (EU) 2025/292, <a href="#">ABI L 2025/292, 1.</a> ; DelegierteVO (EU) 2025/296, <a href="#">ABI L 2025/296, 1.</a> ; DelegierteVO (EU) 2025/297, <a href="#">ABI L 2025/297, 1.</a> ; DelegierteVO (EU) 2025/298; <a href="#">ABI L 2025/298, 1.</a> ; DelegierteVO (EU) 2025/299, <a href="#">ABI L 2025/299, 1.</a>  | MiCAR, technische Regulierungsstandards                       |
| Delegierte Verordnung (EU) 2025/301 der Kommission vom 23. Oktober 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung des Inhalts und der Fristen für die Erstmeldung, die Zwischenmeldung und die Abschlussmeldung schwerwiegender IKT-bezogener Vorfälle sowie des Inhalts der freiwilligen Meldung erheblicher Cyberbedrohungen, <a href="#">ABI L 2025/301.</a> | DORA, Meldungen, IKT-Vorfälle                                 |
| Durchführungsverordnung (EU) 2025/302 der Kommission vom 23. Oktober 2024 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates im Hinblick auf Standardformulare, Vorlagen und Verfahren für Finanzunternehmen   | DORA, Meldungen, IKT-Vorfälle                                 |

|   |   |
|---|---|
| <p>zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls oder einer erheblichen Cyberbedrohung, <a href="#">ABI L 2025/302</a>.</p>  |   |
| <p>Delegierte Verordnung (EU) 2025/303 der Kommission vom 31. Oktober 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der von bestimmten Finanzunternehmen in die Mitteilung zur Bekundung ihrer Absicht zur Erbringung von Krypto-Dienstleistungen aufzunehmenden Angaben, <a href="#">ABI L 2025/303</a>.</p>                                      | <p>MiCAR, technische Regulierungsstandards</p>  |
| <p>Durchführungsverordnung (EU) 2025/304 der Kommission vom 31. Oktober 2024 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates im Hinblick auf Standardformulare, Mustertexte und Verfahren für die Mitteilung von bestimmten Finanzunternehmen zur Bekundung ihrer Absicht zur Erbringung von Krypto-Dienstleistungen, <a href="#">ABI L 2025/304</a>.</p> | <p>MiCAR, Regulierungsstandards</p>   |
| <p>VO (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847, <a href="#">ABI L 2025/327</a>.</p>   | <p>Gesundheitsdaten, europäischer Gesundheitsdatenraum, Primär- und Sekundärnutzung</p> |
| <p>Delegierte Verordnung (EU) 2025/416 der Kommission vom 29. November 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung des Inhalts und des Formats von Auftragsbuchaufzeichnungen für Anbieter von Kryptowerte-Dienstleistungen, die eine Handelsplattform für Kryptowerte betreiben, <a href="#">ABI L 2025/416</a>.</p>                            | <p>MiCAR, Handelsplattformen für Kryptowerte, Auftragsbuchaufzeichnungen</p>            |
| <p>Delegierte Verordnung (EU) 2025/417 der Kommission vom 28. November 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung der Art der Darstellung von Daten zur Transparenz durch Anbieter von Kryptowerte-Dienstleistungen, die eine Handelsplattform für Kryptowerte betreiben, <a href="#">ABI L 2025/417</a>.</p>                                 | <p>MiCAR, Handelsplattformen für Kryptowerte, Transparenz</p>                           |

|   |   |
|---|---|
| <p>Durchführungsverordnung (EU) 2025/512 der Kommission vom 13. März 2025 über technische Modalitäten für die Entwicklung, Wartung und Nutzung elektronischer Systeme für den Austausch und die Speicherung von Informationen gemäß der Verordnung (EU) Nr. 952/2013 des Europäischen Parlaments und des Rates, <a href="#">ABI L 2025/512</a>.</p>   | <p>Zollkodex, Data Mining, künstliche Intelligenz</p>   |
| <p>Delegierte Verordnung (EU) 2025/300 der Kommission vom 10. Oktober 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für die zwischen zuständigen Behörden auszutauschenden Informationen, <a href="#">ABI L 2025/300</a>; Delegierte Verordnung (EU) 2025/305 der Kommission vom 31. Oktober 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der in einen Antrag auf Zulassung als Anbieter von Krypto-Dienstleistungen aufzunehmenden Angaben, <a href="#">ABI L 2025/305</a>; Delegierte Verordnung (EU) 2025/413 der Kommission vom 18. Dezember 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung des genauen Inhalts der Informationen, die für die Beurteilung einer geplanten Übernahme einer qualifizierten Beteiligung an einem Emittenten eines vermögenswertereferenzierten Tokens erforderlich sind, <a href="#">ABI L 2025/413</a>; Delegierte Verordnung (EU) 2025/414 der Kommission vom 18. Dezember 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung des genauen Inhalts der Informationen, die für die Beurteilung einer geplanten Übernahme einer qualifizierten Beteiligung an einem Anbieter von Kryptowerte-Dienstleistungen erforderlich sind, <a href="#">ABI L 2025/414</a>;</p> | <p>MiCAR, technische Regulierungsstandards</p>          |
| <p>Durchführungsverordnung (EU) 2025/306 der Kommission vom 31. Oktober 2024 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und</p>  | <p>MiCAR, Standardformulare, Mustertexte, Verfahren</p> |

|  |  |
|--|--|
| <p>des Rates im Hinblick auf Standardformulare, Mustertexte und Verfahren für die in einen Antrag auf Zulassung als Anbieter von Krypto-Dienstleistungen aufzunehmenden Angaben, <a href="#">ABI L 2025/306</a>.</p>   |  |
| <p>Durchführungsverordnung (EU) 2025/846 der Kommission vom 6. Mai 2025 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf den grenzüberschreitenden Identitätsabgleich natürlicher Personen, <a href="#">ABI L 2025/846</a>, Durchführungsverordnung (EU) 2025/847 der Kommission vom 6. Mai 2025 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Reaktion auf Sicherheitsverletzungen europäischer Brieftaschen für die digitale Identität, <a href="#">ABI L 2025/847</a>, Durchführungsverordnung (EU) 2025/848 der Kommission vom 6. Mai 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Registrierung von auf Brieftaschen vertrauenden Beteiligten, <a href="#">ABI L 2025/848</a>, und Durchführungsverordnung (EU) 2025/849 der Kommission vom 6. Mai 2025 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Übermittlung von Informationen an die Kommission und die Kooperationsgruppe für die Liste der zertifizierten europäischen Brieftaschen für die digitale Identität, <a href="#">ABI L 2025/849</a>.</p> | <p>eIDAS-VO, Europäische Brieftaschen</p>  |
| <p>Proposal for a Regulation of the european parliament and of the council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures, <a href="#">COM(2025) 501 final</a>; Proposal for a Directive of the european parliament and of the council amending Directives 2014/65/EU and (EU) 2022/2557 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap</p>   | <p>Omnibus IV, small mid-cap enterprises, DSGVO, Verarbeitungsverzeichnis, Digitalisierung, MiFID, CER</p> |

|  |   |
|--|---|
| <p>enterprises and further simplifying measures, <a href="#">COM(2025) 502 final</a>; Proposal for a Directive of the European Parliament and of the Council amending Directives 2000/14/EC, 2011/65/EU, 2013/53/EU, 2014/29/EU, 2014/30/EU, 2014/31/EU, 2014/32/EU, 2014/33/EU, 2014/34/EU, 2014/35/EU, 2014/53/EU, 2014/68/EU and 2014/90/EU of the European Parliament and of the Council as regards digitalisation and common specifications, <a href="#">COM(2025) 503 final</a>; und Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) No 765/2008, (EU) 2016/424, (EU) 2016/425, (EU) 2016/426, (EU) 2023/1230, (EU) 2023/1542 and (EU) 2024/1781 as regards digitalisation and common specifications, <a href="#">COM(2025) 504 final</a>.</p>   |   |
| <p>Delegierte Verordnung (EU) 2025/1140 der Kommission vom 27. Februar 2025 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der über sämtliche Kryptowerte-Dienstleistungen, Tätigkeiten, Aufträge und Geschäfte zu führenden Aufzeichnungen, <a href="#">ABI L 2025/1140</a>; Delegierte Verordnung (EU) 2025/1141 der Kommission vom 27. Februar 2025 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung der Anforderungen an Strategien und Verfahren zu Interessenkonflikten für Emittenten vermögenswertereferenzierter Token, <a href="#">ABI L 2025/1141</a>; und Delegierte Verordnung (EU) 2025/1142 der Kommission vom 27. Februar 2025 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung der Anforderungen an Strategien und Verfahren zu Interessenkonflikten für Anbieter von Kryptowerte-Dienstleistungen und der Einzelheiten und Methoden für den Inhalt der Offenlegung von Interessenkonflikten, <a href="#">ABI L 2025/1142</a>.</p> | <p>MiCAR, technische Regulierungsstandards, Aufzeichnungspflichten, Interessenkonflikte</p> |
| <p>Delegierte Verordnung (EU) 2025/532 der Kommission vom 24. März 2025 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische</p>   | <p>DORA, Untervergabe, IKT-Dienstleistungen</p>   |

|   |  |
|---|--|
| <p>Regulierungsstandards zur Präzisierung der Aspekte, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss, <a href="#">ABI L 2025/532</a>.</p>  |  |
| <p>Durchführungsbeschluss (EU) 2025/1382 der Kommission vom 15. Juli 2025 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten durch die Europäische Patentorganisation, <a href="#">ABI L 2025/1382</a>.</p>  | <p>Angemessenheitsbeschluss, Europäische Patentorganisation</p>                |
| <p>Durchführungsverordnung (EU) 2025/1410 der Kommission vom 9. Juli 2025 über das Format, das Muster und die technischen Spezifikationen der Kennzeichnungen und Transparenzbekanntmachungen politischer Anzeigen gemäß den Artikeln 11 und 12 der Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates, <a href="#">ABI L 2025/1410</a>.</p>  | <p>TTPW-VO, politischen Anzeigen, Transparenz</p>                              |
| <p>Durchführungsverordnung (EU) 2025/1566 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards für die Überprüfung der Identität und der Attribute der Person, der das qualifizierte Zertifikat oder die qualifizierte elektronische Attributsbescheinigung ausgestellt werden soll, <a href="#">ABI L 2025/1566</a>; Durchführungsverordnung (EU) 2025/1567 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Verwaltung von qualifizierten elektronischen Fernsignaturerstellungseinheiten und qualifizierten elektronischen Fernsieglerstellungseinheiten, <a href="#">ABI L 2025/1567</a>; Durchführungsverordnung (EU) 2025/1568 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Verfahrensmodalitäten für gegenseitige Begutachtungen elektronischer Identifizierungssysteme und für die Zusammenarbeit bei der Organisation solcher Begutachtungen innerhalb der</p> | <p>eIDAS-VO, Europäische Briefftasche, Anforderungen, Standards, Verfahren</p> |



|   |  |
|---|--|
| <p>Kooperationsgruppe und zur Aufhebung des Durchführungsbeschlusses (EU) 2015/296 der Kommission, <a href="#">ABI L 2025/1568</a>; Durchführungsverordnung (EU) 2025/1569 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf qualifizierte elektronische Attributsbescheinigungen und von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen bereitgestellte elektronische Attributsbescheinigungen, <a href="#">ABI L 2025/1569</a>; Durchführungsverordnung (EU) 2025/1570 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Notifizierung von Informationen über zertifizierte qualifizierte elektronische Signaturerstellungseinheiten und zertifizierte qualifizierte elektronische Siegelerstellungseinheiten, <a href="#">ABI L 2025/1570</a>; Durchführungsverordnung (EU) 2025/1571 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Formate und Verfahren für die jährlichen Berichte der Aufsichtsstellen, <a href="#">ABI L 2025/1571</a>; Durchführungsverordnung (EU) 2025/1572 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf das Format und die Verfahren für die Absichtsmitteilung und die Überprüfung im Hinblick auf den Beginn der Erbringung qualifizierter Vertrauensdienste, <a href="#">ABI L 2025/1572</a>.</p> |  |
| <p>Durchführungsverordnung (EU) 2025/1328 der Kommission vom 30. Juni 2025 zur Durchführung der Richtlinie (EU) 2024/1275 des Europäischen Parlaments und des Rates durch die Erstellung gemeinsamer Vorlagen für die Übermittlung von Informationen aus den nationalen Datenbanken über die Gesamtenergieeffizienz von Gebäuden an die Beobachtungsstelle für den EU-Gebäudebestand, <a href="#">ABI L 2025/1328</a>.</p>  | <p>Gesamtenergieeffizienz von Gebäuden, Anonymisierung</p> |
| <p>Delegierte Verordnung (EU) 2025/1125 der Kommission vom 5. Juni 2025 zur Ergänzung der Verordnung (EU) 2023/1114 des</p>   | <p>MiCAR, vermögenswertereferenzierte Token, Zulassung</p> |

|  |  |
|--|--|
| <p>Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung der Informationen in einem Antrag auf Zulassung zum öffentlichen Angebot vermögenswertereferenzierter Token oder ihre Zulassung zum Handel, <a href="#">ABI L 2025/1125</a>.</p>  |  |
| <p>Durchführungsverordnung (EU) 2025/1126 der Kommission vom 5. Juni 2025 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates im Hinblick auf die Festlegung von Standardformularen, Mustertexten und Verfahren für die in den Antrag auf Zulassung zum öffentlichen Angebot vermögenswertereferenzierter Token und ihre Zulassung zum Handel aufzunehmenden Informationen, <a href="#">ABI L 2025/1126</a>.</p>   | <p>MiCAR, vermögenswertereferenzierte Token, Zulassung, Standardformulare, Mustertexte</p> |
| <p>Delegierte Verordnung (EU) 2025/1264 der Kommission vom 27. Juni 2025 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung des Mindestinhalts der Strategien und Verfahren für das Liquiditätsmanagement für bestimmte Emittenten von vermögenswertereferenzierten Token oder E-Geld-Token, <a href="#">ABI L 2025/1264</a>.</p>   | <p>MiCAR, Liquiditätsmanagement, vermögenswertereferenzierte Token, E-Geld-Token</p>       |
| <p>Durchführungsverordnung (EU) 2025/1942 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf qualifizierte Validierungsdienste für qualifizierte elektronische Signaturen und qualifizierte Validierungsdienste für qualifizierte elektronische Siegel, <a href="#">ABI L 2025/1942</a>; Durchführungsverordnung (EU) 2025/1943 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards für qualifizierte Zertifikate für elektronische Signaturen und qualifizierte Zertifikate für elektronische Siegel, <a href="#">ABI L 2025/1943</a>; Durchführungsverordnung (EU) 2025/1944 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des</p> | <p>eIDAS-VO, Referenzstandards, Spezifikationen</p>  |

|  |  |
|--|--|
| <p>Europäischen Parlaments und des Rates in Bezug auf Referenzstandards für Prozesse des Absendens und Empfangens von Daten in qualifizierten Diensten für die Zustellung elektronischer Einschreiben und in Bezug auf die Interoperabilität dieser Dienste, <a href="#">ABI L 2025/1944</a>; Durchführungsverordnung (EU) 2025/1945 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Validierung qualifizierter elektronischer Signaturen und qualifizierter elektronischer Siegel sowie die Validierung fortgeschrittener elektronischer Signaturen, die auf qualifizierten Zertifikaten beruhen, und fortgeschrittener elektronischer Siegel, die auf qualifizierten Zertifikaten beruhen, <a href="#">ABI L 2025/1945</a>; Durchführungsverordnung (EU) 2025/1946 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen und qualifizierte elektronische Siegel, <a href="#">ABI L 2025/1946</a>.</p> |  |
| <p>Delegierte Verordnung (EU) 2025/2050 der Kommission vom 1. Juli 2025 zur Ergänzung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates durch Festlegung der technischen Bedingungen und Verfahren, unter denen die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen zugelassenen Forschenden Daten zur Verfügung stellen müssen, <a href="#">ABI L 2025/2050</a>.</p>   | <p>DSA, Forschungsdaten, Datenzugangsportale</p>   |
| <p>Delegierte Verordnung (EU) 2025/1871 der Kommission vom 23. Juli 2025 zur Änderung der Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates hinsichtlich der Normen für eCalls und zur Änderung der Delegierten Verordnung (EU) 2017/79 hinsichtlich der technischen Anforderungen und Prüfverfahren für die Genehmigung von Kraftfahrzeugen, die mit auf dem 112-Notruf basierenden bord-eigenen eCall-Systemen ausgerüstet sind", <a href="#">ABI L 2025/1871</a>.</p>  | <p>eCall-Systeme, Fahrzeugtypen, Prüfverfahren</p> |

|  |  |
|--|--|
| <p>Durchführungsverordnung (EU) 2025/2160 der Kommission vom 27. Oktober 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards, Spezifikationen und Verfahren für das Management der Risiken bei der Erbringung nichtqualifizierter Vertrauensdienste, <a href="#">ABI L 2025/2160</a>; Durchführungsverordnung (EU) 2025/2162 der Kommission vom 27. Oktober 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Akkreditierung von Konformitätsbewertungsstellen, die qualifizierte Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste bewerten, den Konformitätsbewertungsbericht und das Konformitätsbewertungssystem, <a href="#">ABI L 2025/2162</a>.</p> | <p>eIDAS-VO, Referenzstandards, Spezifikationen, Akkreditierung, Konformitätsbewertungsstellen</p> |
| <p>Vorschläge der Europäischen Kommission für (i) einen "Digital Omnibus", <a href="#">COM(2025) 837 final</a>, (ii) einen "Digital Omnibus on AI", <a href="#">COM(2025) 836 final</a> und (iii) "European Business Wallets", <a href="#">COM(2025) 838 final</a>.</p>  | <p>DSGVO, Cookies, KI-VO, Data Acts, eIDAS-VO</p>  |
| <p>Verordnung (EU) 2025/2518 des Europäischen Parlaments und des Rates vom 26. November 2025 zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679, <a href="#">ABI L 2025/2518</a>.</p>  | <p>DSGVO, Durchsetzung, grenzüberschreitende Verfahren</p>   |
| <p>Durchführungsverordnung (EU) 2025/2527 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards und Spezifikationen für qualifizierte Zertifikate für die Website-Authentifizierung, <a href="#">ABI L 2025/2527</a>; Durchführungsverordnung (EU) 2025/2530 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Anforderungen an qualifizierte Vertrauensdiensteanbieter, die qualifizierte Vertrauensdienste erbringen, <a href="#">ABI L 2025/2530</a>; Durchführungsverordnung (EU) 2025/2531 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften</p>   | <p>eIDAS-VO, Referenzstandards, Spezifikationen, qualifizierte Vertrauensdiensteanbieter</p>       |

|  |  |
|--|--|
| <p>für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards und Spezifikationen für qualifizierte elektronische Journale, <a href="#">ABI L 2025/2531</a>; Durchführungsverordnung (EU) 2025/2532 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards und Spezifikationen für qualifizierte elektronische Archivierungsdienste", <a href="#">ABI L 2025/2532</a>.</p>  |  |
| <p>Durchführungsbeschluss (EU) 2025/2571 der Kommission vom 19. Dezember 2025 zur Änderung des Durchführungsbeschlusses (EU) 2021/1773 der Kommission gemäß der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich, <a href="#">ABI L 2025/2571</a>; Durchführungsbeschluss (EU) 2025/2574 der Kommission vom 19. Dezember 2025 zur Änderung des Durchführungsbeschlusses (EU) 2021/1772 der Kommission gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich, <a href="#">ABI L 2025/2574</a>.</p> | <p>Vereinigtes Königreich, Angemessenheitsbeschluss, Geltungsdauer</p> |

### Nationale Rechtsakte

| Rechtsakt  | Stichworte  |
|--|---|
| <p>Verordnung des Bundesministers für Soziales, Gesundheit, Pflege und Konsumentenschutz, mit der die Gesundheitstelematikverordnung 2013 und die ELGA-Verordnung 2015 geändert und die ELGA- und eHealth-Supporteinrichtungsverordnung sowie die eHealth-Verordnung 2025 neu erlassen wird (Gesundheitstelematik-Anpassungsverordnung 2025), <a href="#">BGBl II 2025/11</a>.</p> | <p>Gesundheitstelematikverordnung 2013, eHealth, Gesundheitsdaten</p> |
| <p>FATF-Prüfungsanpassungsgesetz 2024, <a href="#">BGBl I 2025/5</a>.</p>  | <p>FATF, Sanktionen, Kontenregister</p>                               |
| <p>Verordnung des Bundesministers für Kunst, Kultur, öffentlichen Dienst und Sport, mit der die</p>  | <p>Beamtendienstrecht, Aufbewahrungspflichten</p>                     |

|   |  |
|---|--|
| BMKÖS-Datenaufbewahrungsverordnung geändert wird, <a href="#">BGBl II 2025/18</a> .   |  |
| Einzelentgeltnachweisverordnung 2025, <a href="#">BGBl II 2025/75</a> .   | Telekommunikation, nummerngebundene interpersonelle Kommunikationsdienste, Internetzugangsdienste  |
| Oberösterreichisches Informationstechnologien-Einsatz-Gesetz (Oö ITEG), <a href="#">LGBl 2025/46</a> .  | digitale Transformation, künstliche Intelligenz, automatisierte Entscheidungen, KI-Reallabore  |
| Bundesgesetz, mit dem das Universitätsgesetz 2002 und das Bildungsdokumentationsgesetz 2020 geändert werden, <a href="#">BGBl I 2025/28</a> .   | Studierendenregister, digitaler Studierendenausweis, Datenverbund der Universitäten und Hochschulen (DVUH), des Austrian Higher Education Systems Networks (AHESN) |
| Datenzugangsgesetz, <a href="#">BGBl I 2025/33</a> .  | Data Governance Act (DGA), Weiterverwendung, öffentliche Stelle, zuständige Behörde  |
| Informationsfreiheits-Anpassungsgesetz, <a href="#">BGBl I 2025/50</a> .  | IFG, Grundrecht auf Information  |
| MiCAR-Emittenten-Meldeverordnung (MiCAR-EMV)  | MiCAR, vermögenswertereferenzierte Token, E-Geld-Token   |
| Daten-Governance-Benennungsverordnung (DGBenV), <a href="#">BGBl II 2025/186</a> .  | Statistik Austria, Weiterverwendung  |
| Bundesgesetz, mit dem das Staatsschutz- und Nachrichtendienst-Gesetz, das Sicherheitspolizeigesetz, das Telekommunikationsgesetz 2021, das Bundesverwaltungsgerichtsgesetz und das Richter- und Staatsanwaltschaftsdienstgesetz geändert werden, <a href="#">BGBl I 2025/54</a> . | Bundestrojaner, Journaldienst, Evidenzstelle des BVwG  |
| Bundesgesetz, mit dem das Bundesgesetz zur Sicherstellung eines hohen Resilienznieaus von kritischen Einrichtungen (Resilienz kritischer Einrichtungen-Gesetz; RKEG) erlassen und das Tilgungsgesetz 1972 geändert wird, <a href="#">BGBl I 2025/60</a> .                         | RKE-RL, CER, Bundesminister für Inneres  |
| Strafrechtliches EU-Anpassungsgesetz 2025, <a href="#">BGBl I 2025/65</a> ,   | Drittstaatsangehörige, Staatenlose, Fingerabdruck, Strafregister   |
| Bundesgesetz, mit dem das Gesundheitstelematikgesetz 2012 und das Allgemeine Sozialversicherungsgesetz geändert werden, <a href="#">BGBl I 2025/71</a> .  | GtelG, MyHealth@EU, EU-Rezept, EU-Patientenkurzakte  |

|   |  |
|---|--|
| Zweites EU-Informationssysteme-Anpassungsgesetz, <a href="#">BGBl I 2025/87</a> .   | Europäische Reiseinformationssystem (ETIAS)              |
| Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsystemsicherheitsgesetz 2026 – NISG 2026) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden, <a href="#">BGBl I 2025/94</a> . | NIS-2-RL, Cybersicherheit, Europäisches Kompetenzzentrum |

## Leitlinien

| Leitlinien  | Stichworte  |
|---|---|
| EDSA, Leitlinien 1/2025 über Pseudonymisierung (2025)   | Pseudonymisierung, Personenbezug, Weiterverarbeitung                          |
| EK, Commission Guidelines on prohibited AI practices  | verbotene KI-Praktiken  |
| EK, Commission Guidelines on the definition of an AI system established   | KI-Systeme, Definition  |
| EDSA, Guidelines 02/2025 on processing of personal data through blockchain technologies <sup>1.1</sup> (2025)                         | Blockchain, Datenschutz   |
| EK, Leitlinien zum Schutz Minderjähriger im Internet nach dem Gesetz über digitale Dienste  | Schutz Minderjähriger, Online-Plattformen                                     |
| EDSA, Guidelines 2/2024 on Article 48 GDPR <sup>2</sup>   | Art 48 DSGVO, Drittlandtransfer, Urteile, Verwaltungsentscheidungen           |
| DSB 30.06.2025, Leitfaden zum Informationsfreiheitsgesetz   | IFG, Informationsfreiheit, Datenschutz  |
| KI-Verhaltenskodex für allgemeine Zwecke  | künstliche Intelligenz, Sicherheit, Gefahrenabwehr, Transparenz, Urheberrecht |
| EK, Erläuterung und Vorlage für die öffentliche Zusammenfassung von Schulungsinhalten für KI-Modelle mit allgemeinem Verwendungszweck | KI-Modelle mit allgemeinem Verwendungszweck, Training                         |
| EDSA, Guidelines 3/2025 on the interplay between the DSA and the GDPR (2025)  | DSGVO, DSA, Dark Patterns, Schutz von Minderjährigen                          |

|   |  |
|---|--|
| EDSA/EK, Joint Guidelines on the Interplay between the DMA and the GDPR | DSGVO, DMA, "Pay-or-Ok"-Modell             |
| EDSA, Recommendations 2/2025 on e-commerce Websites                     | E-Commerce-Websites, Rechtsgrundlage, Gast |



# Digital Law Monitor – Contacts

**János Böszörményi**

Attorney at Law  
Austria, Vienna  
+43 1 534 37 50211  
[j.boeszormentyi@schoenherr.eu](mailto:j.boeszormentyi@schoenherr.eu)

**Florian Terharen**

Attorney at Law  
Austria, Vienna  
+43 664 80060 3625  
[fl.terharen@schoenherr.eu](mailto:fl.terharen@schoenherr.eu)

**Marin Demirev**

Attorney at Law  
Bulgaria  
+359 88 412 96 06  
[ma.demirev@schoenherr.eu](mailto:ma.demirev@schoenherr.eu)

**Sven Sušanj**

Associate in cooperation with Schoenherr  
Croatia  
+385 14828183  
[sv.susanj@schoenherr.eu](mailto:sv.susanj@schoenherr.eu)

**Natálie Hrubá**

Associate  
Czech Republic  
+420 225 996 500  
[natalie.dubska@schoenherr.eu](mailto:natalie.dubska@schoenherr.eu)

**Sebastian Špeta**

Attorney at Law  
Czech Republic  
+420 225 996 500  
[se.speta@schoenherr.eu](mailto:se.speta@schoenherr.eu)

**Barbara Darcsi**

Associate  
Hungary  
+36 70 416 3419  
[ba.darcsi@schoenherr.eu](mailto:ba.darcsi@schoenherr.eu)

**Gergely Horváth**

Attorney at Law  
Hungary  
+36 70 367 1112  
[ge.horvath@schoenherr.eu](mailto:ge.horvath@schoenherr.eu)

**Andrian Guzun**

Attorney at Law  
Moldova  
+373 22 240 300  
[a.guzun@schoenherr.eu](mailto:a.guzun@schoenherr.eu)

**Vladimir Iurkovski**

Office Managing Partner  
Moldova  
+373 79 106 382  
[v.iurkovski@schoenherr.eu](mailto:v.iurkovski@schoenherr.eu)

**Daria Rutecka**

Partner  
Poland (Warsaw)  
+48 22 223 09 23  
[d.rutecka@schoenherr.eu](mailto:d.rutecka@schoenherr.eu)

**Piotr Podsiedlik**

Junior Associate  
Poland  
+48 22 223 09 10  
[pi.podsiedlik@schoenherr.eu](mailto:pi.podsiedlik@schoenherr.eu)

**Katarzyna Szczudlik**

Partner  
Poland  
+48 883 395 980  
[ka.szczudlik@schoenherr.eu](mailto:ka.szczudlik@schoenherr.eu)

**Karolina Pikula-Obalek**

Associate  
Poland (Warsaw)  
+48 538 946 468  
[ka.pikula@schoenherr.eu](mailto:ka.pikula@schoenherr.eu)

**Carla Filip**

Attorney at Law  
Romania  
+40 21 319 67 90  
[c.filip@schoenherr.eu](mailto:c.filip@schoenherr.eu)

**Špela Lovšin**

Attorney at Law  
Slovenia  
+386 1 200 09 71  
[sp.lovsin@schoenherr.eu](mailto:sp.lovsin@schoenherr.eu)

**Miriam Gajšek**

Senior Associate  
Slovenia  
+386 1 200 09 66  
[m.gajsek@schoenherr.eu](mailto:m.gajsek@schoenherr.eu)

**Didem Kara**

Attorney at Law  
Türkiye  
+90 212 324 70 70  
[di.kara@schoenherr.eu](mailto:di.kara@schoenherr.eu)

**Damla Aydoğan**

Associate  
Türkiye (Istanbul)  
+90 532 701 16 75  
[da.aydogan@schoenherr.eu](mailto:da.aydogan@schoenherr.eu)

**Emir Kuris**

Attorney at Law  
Türkiye  
+386 1 200 09 66  
[em.kuris@schoenherr.eu](mailto:em.kuris@schoenherr.eu)

to the point

# DIGITAL LAW MONITOR. 1/2025

Keeping up with developments in Digital Law is an increasing challenge.

To assist you handling this challenge, we created this comprehensive (though not necessarily complete) overview of these developments and will update it on a regular basis. This overview includes **legal acts**, **draft legal acts**, **guidelines** and occasionally other legal materials.

For **weekly news** please subscribe to the [Schönherr Datenschutzmonitor](#) for updates on legal acts and guidelines (in German)

## EU Legal Acts, Guidelines and more

### • **Regulations**

Passenger Data Regulation  
Passenger Data Regulation for Law Enforcement  
Managed Security Services Regulation  
Cyber Solidarity Act  
European Health Data Space Regulation

### • **Directives**

Corporate Directive on Digital Tools

### • **Commission Guidelines**

Draft Commission Guidelines on prohibited AI practices  
Draft Commission Guidelines on the definition of an AI system established by AI Act

### • **European Data Protection Board**

Guidelines 01/2025 on Pseudonymisation  
Guidelines 02/2025 on processing of personal data through blockchain technologies

### • **Commission Delegated and Implemented Regulations (incl. drafts)**

Digital Operational Resilience Act (DORA)  
Markets in Crypto-Assets Regulation (MiCAR)  
Cyber Resilience Regulation (CRA)  
EU Customs Code  
eIDAS

## Austrian Acts

Health Telematics Adjustment Ordinance 2025  
FATF Report Adjustment Act 2024  
BMKÖS Data Retention Ordinance  
Amendment of the Ordinance on the e-justice system (ERV 2021)  
Transparency Database Query Ordinance 2025  
Ordinance of the Federal Minister of the Interior on the e-justice system in the Field of Criminal Justice

## EU legal acts

### Regulations

#### Passenger Data Regulation

- On **08.01.2025** the "Regulation (EU) 2025/12 of the European Parliament and of the Council of 19 December 2024 on the collection and transfer of advance passenger information for enhancing and facilitating external border checks, amending Regulations (EU) 2018/1726 and (EU) 2019/817, and repealing Council Directive 2004/82/EC", [OJ L 2025/12](#), was published.

The **Passenger Data Regulation** imposes an obligation on airlines to collect so-called **API data** (advance passenger information) for flights to the EU and to transmit this data in encrypted form to the competent **border authorities**. The API data includes identification, aircraft and baggage data.

#### Passenger Data Regulation for Law Enforcement

- On **08.01.2025** the "Regulation (EU) 2025/13 of the European Parliament and of the Council of 19 December 2024 on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818", [OJ L 2025/13](#), was published.

The **Passenger Data Regulation for Law Enforcement** imposes an obligation on **airlines** to transmit encrypted **API data** and other **PNR data** to the so-called **Passenger Information Units (PIU)** in order to combat **transnational serious and organized crime and terrorism**.

#### Managed Security Services Regulation

- On **15.01.2025** the "Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services", [OJ L 2025/37](#), was published.

The **Managed Security Services Regulation** introduces European schemes for **cybersecurity certification**. It also creates a European certification framework for cybersecurity.

#### Cyber Solidarity Act

- On **15.01.2025** the "Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (**Cyber Solidarity Act**)", [OJ L 2025/38](#), was published.

The **Cyber Solidarity Act** establishes measures to strengthen the EU's capacity to detect, prevent and respond to **cyber threats** and **security incidents**.

#### European Health Data Space Regulation

- On **05.03.2025** the "Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847" was published, [OJ L 2025/327](#).

The **European Health Data Space Regulation** specifies, *inter alia*, the **rights of natural persons** regarding the **primary and secondary use** of their **personal electronic health data**. The aim of the Regulation is to improve natural persons' **access to** their personal electronic **health data**.

### Directives

#### Corporate Directive on Digital Tools

- On **10.01.2025** the "Directive (EU) 2025/25 of the European Parliament and of the Council of 19 December 2024 amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law", [OJ L 2025/25](#), was published.

The aim of the **Corporate Directive on Digital Tools** is to facilitate **the cross-border establishment of companies**, the registration of branches and the submission of documents and information to the business registers by creating **digital tools and processes**.

## **Commission Guidelines**

### Commission Guidelines on prohibited AI practices

- On **04.02.2025** the **European Commission** published its [Draft Commission Guidelines on prohibited AI practices](#).

The "**Commission Guidelines on prohibited AI practices**" provide detailed definition of the prohibited AI systems described in Art. 5 of the AI Act. The Guidelines, moreover, attempt to clarify the difference between prohibited and permissible AI practices by using examples. For instance, the examples address the permissibility of AI practices such as social scoring and real-time biometric identification. Additionally, the Commission Guidelines deal with interactions with other EU legal acts, such as the GDPR, the DSA, etc.

### Commission Guidelines on the definition of an AI system established by AI Act

- On **06.02.2025** the **European Commission** published its [Draft commission Guidelines on the definition of an AI system established by AI Act](#).

The "**Commission Guidelines on the definition of an AI system established by AI Act**" provide a more concrete definition of the term "AI systems". Additionally, this Commission Guidelines include exceptions for which the AI Act does not apply.

## **European Data Protection Board (EDPB)**

### Guidelines 01/2025 on Pseudonymisation

- On **17.01.2025** the **EDPB** published its [Guidelines 01/2025 on Pseudonymisation](#).

The "**Guidelines 01/2025 on Pseudonymisation**" offer a detailed guidance on pseudonymization techniques and the effects of pseudonymization.

### Guidelines 02/2025 on processing of personal data through blockchain technologies

- On **14.04.2025** the **EDPB** published its [Guidelines 02/2025 on processing of personal data through blockchain technologies<sup>1,1</sup>](#).

The "**Guidelines 02/2025 on processing of personal data through blockchain technologies**" offer a detailed guidance on the interaction between **blockchain technologies** and the **GDPR**. The guidelines discuss roles and responsibilities, international transfers, retention periods, security, data protection impact assessments, data subject rights and much more.

## **Commission Delegated and Implemented Regulations**

### Digital Operational Resilience Act (DORA)

- On **13.02.2025** the "*Commission Delegated Regulation (EU) 2025/295 of 24 October 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards on harmonisation of conditions enabling the conduct of the oversight activities*" was published, [OJ L 2025/295](#).

This **Delegated Regulation supplements** "*Regulation (EU) 2022/2554 on digital operational resilience for the financial sector*" ([DORA](#)) with regard to **regulatory technical standards** for the provision of information which must be provided by so-called **ICT third-party service providers**.

- On **20.02.2025** the "*Commission Delegated Regulation (EU) 2025/301 of 23 October 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats*" was published, [OJ L 2025/301](#).

This **Delegated Regulation supplements** "*Regulation (EU) 2022/2554 on digital operational resilience for the financial sector*" ([DORA](#)) with regard to **regulatory technical standards specifying** which information must be transmitted with reports of major **ICT-related incidents**.

- On **20.02.2025** the "*Commission Implementing Regulation (EU) 2025/302 of 23 October 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms,*

templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat" was published, [OJ L 2025/302](#).

This **Implementing** Regulation contains **technical standards** for the application of the "Regulation (EU) 2022/2554 **on digital operational resilience for the financial sector**" (**DORA**). The Regulation provides standard forms, templates and procedures for reporting **obligations regarding major ICT-related incidents**.

#### Markets in Crypto-Assets Regulation (MiCAR)

- On **13.02.2025** the following five Commission Delegated Regulations were published to supplement "Regulation (EU) 2023/1114 on markets in crypto-assets":
  1. Commission Delegated Regulation (EU) 2025/292 on cooperation arrangements between competent authorities and supervisory authorities of third countries, [OJ L 2025/292](#),
  2. Commission Delegated Regulation (EU) 2025/296 on the procedure for the approval of a crypto-asset white paper, [OJ L 2025/296](#),
  3. Commission Delegated Regulation (EU) 2025/297 on the conditions for the establishment and functioning of consultative supervisory colleges, [OJ L 2025/297](#),
  4. Commission Delegated Regulation (EU) 2025/298 on the methodology to estimate the number and value of transactions associated to uses of non-EU asset-referenced tokens and of e-money tokens, [OJ L 2025/298](#), and
  5. Commission Delegated Regulation (EU) 2025/299 on continuity and regularity in the performance of crypto-asset services, [OJ L 2025/299](#).

These five **Delegated** Regulations **supplement** "Regulation (EU) 2023/1114 **on markets in crypto-assets**" (**MiCAR**) with regard to **regulatory technical standards** for cooperation arrangements between authorities, approval procedures, establishment of consultative supervisory colleges, methodologies and more.

- On **20.02.2025** the "Commission Delegated Regulation (EU) 2025/303 of 31 October 2024 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information to be included by certain financial entities in the notification of their intention to provide crypto-asset services" was published, [OJ L 2025/303](#).

This **Delegated** Regulations **supplements** "Regulation (EU) 2023/1114 **on markets in crypto-assets**" (**MiCAR**) with regard to **regulatory technical standards** for the provision of information to be included by certain financial entities in the **notification** of their intention to **provide crypto-asset services**.

- On **20.02.2025** the "Commission Implementing Regulation (EU) 2025/304 of 31 October 2024 laying down implementing technical standards for the application of Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to standard forms, templates and procedures for the notification by certain financial entities of their intention to provide crypto-asset services" was published, [OJ L 2025/304](#).

This **Implementing** Regulation contains **standard forms, templates, and procedures** for the notification by certain financial entities of their intention to provide crypto-asset services pursuant to the Regulation (EU) 2023/1114 **on markets in crypto-assets**" (**MiCAR**).

- On **14.03.2025** the "Commission Delegated Regulation (EU) 2025/416 of 29 November 2024 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and format of order book records for crypto-asset service providers operating a trading platform for crypto-assets" was published, [OJ L 2025/416](#).

This **Delegated** Regulation **supplements** "Regulation (EU) 2023/1114 on markets in crypto-assets" (**MiCAR**) with regard to **regulatory technical standards** for **crypto asset trading platforms**.

- On **14.03.2025** the "Commission Delegated Regulation (EU) 2025/417 of 28 November 2024 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the manner in which crypto-asset service

providers operating a trading platform for crypto-assets are to present transparency data" was published, [OJ L 2025/417](#).

This **Delegated Regulation supplements** "Regulation (EU) 2023/1114 on markets in crypto-assets" (**MiCAR**) with regard to **regulatory technical standards** for **transparency obligations** of **crypto asset trading platforms**.

- On **31.03.2025** the following four Commission Delegated Regulations were published to supplement "Regulation (EU) 2023/1114 on markets in crypto-assets":
  1. Commission Delegated Regulation (EU) 2025/300 on information to be exchanged between competent authorities, [OJ L 2025/300](#),
  2. Commission Delegated Regulation (EU) 2025/305 on the information to be included in an application for authorisation as a crypto-asset service provider, [OJ L 2025/305](#),
  3. Commission Delegated Regulation (EU) 2025/413 on the detailed content of information necessary to carry out the assessment of a proposed acquisition of a qualifying holding in an issuer of an asset-referenced token, [OJ L 2025/413](#) and
  4. Commission Delegated Regulation (EU) 2025/414 on the detailed content of information necessary to carry out the assessment of a proposed acquisition of a qualifying holding in a crypto-asset service provider, [OJ L 2025/414](#).

These four Delegated Regulations **supplement** "Regulation (EU) 2023/1114 on markets in crypto-assets" (**MiCAR**) with regard to **regulatory technical standards** on the exchange of information between authorities, crypto-asset service providers and issuers of asset-referenced tokens.

- On **31.03.2025** the "Commission Implementing Regulation (EU) 2025/306 of 31 October 2024 laying down implementing technical standards for the application of Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to standard forms, templates and procedures for the information to be included in the application for authorisation as a crypto-asset service provider" was published, [OJ L 2025/306](#).

This **Implementing Regulation** contains **standard forms, templates, and procedures** for the information to be included in the application for authorisation as a crypto-asset service provider pursuant to "Regulation (EU) 2023/1114 on markets in crypto-assets" (**MiCAR**).

#### Cyber Resilience Regulation (CRA)

- On **13.04.2025** the **European Commission** published its [Draft Commission Implementing Regulation on the technical description of the categories of important and critical products with digital elements pursuant to Regulation \(EU\) 2024/2847](#).

This **Implementing Regulation** and its annexes describe the technical specifications of "**Important products with digital elements**" and "**Critical products with digital elements**" listed in Annexes III and IV of the **Cyber Resilience Regulation (CRA)**.

#### EU Customs Code

- On **20.03.2025** the "Commission Implementing Regulation (EU) 2025/512 of 13 March 2025 on technical arrangements for developing, maintaining and employing electronic systems for the exchange and storage of information under Regulation (EU) No 952/2013 of the European Parliament and of the Council" was published, [OJ L 2025/512](#).

This **Implementing Regulation** is based on "Regulation (EU) 952/2013 laying down the Union Customs Code" (**Customs Code**) and defines technical modalities for the exchange of information in central systems as required by customs regulations. *Inter alia*, the usage of **data mining** and thus, the usage of **artificial intelligence**, is permitted.

#### eIDAS

- On **15.04.2025** the **European Commission** published the following 12 draft Commission Implementing Regulations to implement "Regulation (EU) 910/2014 on electronic identification and trust services":
  1. [Verification of identity and attributes at qualified certificate or qualified attestation of attributes issuance](#),
  2. [Management of remote qualified signature creation devices as a qualified trust service](#),

3. [Validation of qualified electronic signatures and seals as well as advanced electronic signatures and seals,](#)
4. [Qualified validation services for qualified electronic signatures and seals,](#)
5. [Provision of qualified electronic time stamping services,](#)
6. [Requirements for qualified electronic registered services,](#)
7. [Notification and verification of the initiation of a qualified trust service,](#)
8. [Submissions of the annual reports by supervisory bodies to the Commission,](#)
9. [Procedural arrangements for peer-reviews of electronic identification schemes to be notified to the Commission,](#)
10. [Notification of qualified electronic signature & seal creation devices that have been certified by certification bodies,](#)
11. [Qualified preservation services for qualified electronic signatures and for qualified electronic seals](#) and
12. [Qualified certificates for electronic signatures and electronic seals.](#)

These twelve **Implementing** Regulations and their annexes contain **reference standards** for identity verification, seals, qualified signatures, time stamping, electronic registered services, trust services and annual reports pursuant to "*Regulation (EU) 910/2014 on electronic identification and trust services*" (**eIDAS**).

## Austrian legal acts

### Health Telematics Adjustment Ordinance 2025

- On **28.01.2025** the "Ordinance of the Federal Minister for Social Affairs, Health, Care, and Consumer Protection, amending the Health Telematics Ordinance 2013 and the ELGA Ordinance 2015, and newly publishing the ELGA and eHealth Support Facility Ordinance as well as the eHealth Ordinance 2025 (Health Telematics Adjustment Ordinance 2025)," was published in the [Federal Law Gazette II 2025/11](#).

The **Health Telematics Adjustment Ordinance 2025** ("Gesundheitstelematik-Anpassungsverordnung 2025") amends the **Health Telematics Ordinance 2013** ("Gesundheitstelematikverordnung 2013") and the **ELGA Ordinance 2015** ("ELGA-Verordnung 2015"). Additionally, within this ordinance **two new ordinances**, namely the **eHealth Support Facility Ordinance** ("eHealth-Supporteinrichtungsverordnung") and the **eHealth Ordinance 2025** ("eHealth-Verordnung 2025") were published. The amendments and the new ordinances overhaul the regulations on the processing of **health data** and **genetic data** by **healthcare service providers**.

### FATF Report Adjustment Act 2024

- On **10.02.2025** the "FATF Report Adjustment Act 2024", was published in the [Federal Law Gazette I 2025/5](#).

In the **FATF Report Adjustment Act 2024** ("FATF-Prüfungsanpassungsgesetz 2024"), the **Sanctions Act 2024** ("Sanktionengesetz 2024") was published. Moreover, several acts, such as the Banking Act (BWG), the Financial Market Authority Act (FMABG), and the Account Register Act (KontRegG) were amended. The regulation includes provisions on the **processing of personal data** by the competent authorities for the implementation of restrictive measures ("sanctions").

### BMKÖS Data Retention Ordinance

- On **14.02.2025** the "Ordinance of the Federal Minister for Arts, Culture, Public Service, and Sports, amending the BMKÖS Data Retention Ordinance", was published in the [Federal Law Gazette II 2025/18](#).

This ordinance overhauls certain **retention obligations** regarding the processing of **civil servants' data**.

### Amendment of the Ordinance on the e-justice system (ERV 2021)

- On **18.02.2025** an "Amendment of the Ordinance on the e-justice system (ERV 2021)", was published in the [Federal Law Gazette II 2025/27](#).

The amendments to the **e-justice system** concern, e.g., **land register procedures** and the **E-ID**.

### Transparency Database Query Ordinance 2025

- On **03.03.2025** the "Transparency Database Query Ordinance 2025" was published in the [Federal Law Gazette II 2025/41](#).

The **Transparency Database Query Ordinance 2025** governs the **read permissions** for service offerings with special categories of personal data ("**sensitive data**") in the **Transparency Database**.

### Ordinance of the Federal Minister of the Interior on the e-justice system in the Field of Criminal Justice

- On **08.04.2025** the "Ordinance of the Federal Minister of the Interior on the e-justice system in the Field of Criminal Justice" was published in the [Federal Law Gazette II 2025/63](#).

The ordinance contains provisions on the usage of the **e-justice system** for communications with **criminal courts, prosecutors** and **prison authorities**.



to the point

# Digital Law Monitor. 2/2025

Keeping up with developments in **digital law** is an increasing challenge.

To assist you in handling this challenge, we have prepared a comprehensive (though not necessarily exhaustive) overview of recent developments, which we will update regularly. This overview covers legal developments **across jurisdictions** and includes **legal acts, draft legal acts, guidelines** and occasionally other relevant legal materials.

For **weekly news**, please subscribe to the [Schönherr Datenschutzmonitor](#) for updates on legal acts and guidelines (in German).

## EU legal acts

- **Regulations and Directives (incl. drafts)**

Omnibus IV Simplification Package

GDPR Procedural Regulation

- **Commission Guidelines**

Commission Guidelines on Protection of Minors online under the Digital Services Act

- **European Data Protection Board**

Guidelines 02/2024 on Article 48 GDPR<sup>2</sup>

- **Counsel Recommendations**

Cyber Blueprint

- **European Commission Decisions**

Digital Markets Act – Apple and Meta

Digital Services Act – AliExpress

- **Commission Delegated and Implementing Regulations (incl. drafts)**

Regulation on Political Advertising

eIDAS

Markets in Crypto-Assets Regulation (MiCAR)

## Austrian legal acts

Ordinance on Itemised Bills 2025

Upper Austrian Information Technology Application Act

"ID Austria" mobile app

Austrian Accessibility Act

Austrian Data Access Act

## Bulgarian legal acts

Act on Accessibility Requirements for Products and Services

Act on Markets in Crypto-Assets

## Croatian legal acts

Decision on the Publication of Price Lists and Quotation of Additional Prices Intended as a Measure of Direct Price Control in Retail Sale

Act on Accessibility Requirements for Products and Services

Fiscalisation Act

## Hungarian legal acts

Act amending certain laws in connection with cash payment

## Moldovan legal acts

Law on Cyber Security

Law on promoting fairness and transparency for business users of online intermediation services

Law on Electronic Communications

Instruction regarding the procedure for stopping access to web pages containing crime-related information

## Polish legal acts

Act amending the Act on Electronic Delivery

Guide to Data Protection Breaches

Act on Accessibility Requirements for Products and Services

## Romanian legal acts

Norm No. 14/2025 on the management of operational risks generated by information systems

Regulation No. 1/2025 on the amendment of certain legal acts issued by the National Bank of Romania

Law No. 232/2022 on accessibility requirements applicable to products and services

Draft Order on the approval of the requirements for the notification/registration process under NIS2

Draft Order on the approval of criteria and thresholds for determining the degree of disruption of a service and the methodology for assessing the risk level of entities under NIS2

### **Slovenian legal acts**

Act amending the Act on the Promotion of Digital Inclusion

Act amending the Act on Prevention of Money Laundering and Terrorist Financing Act

Act amending the Banking Act

Act implementing Regulation (EU) on information accompanying the transfer of funds and certain crypto-assets

Regulation implementing Regulation (EU) on digital operational resilience for the financial sector

Information Security Act

### **Turkish legal acts**

Compliance Obligations for Cross-Border E-Commerce Products

Communiqué on keeping commercial books not related to the accounting of the business in electronic format

Implementation of the Centralised Crypto-Asset Reporting System

Cybersecurity Law No. 7545

## EU legal acts

### Regulations and directives (incl. drafts)

#### Omnibus IV Simplification Package

- The European Commission aims to reduce the administrative burden for companies with the so-called **Omnibus Packages**. On **21 May 2025**, the [Omnibus IV Package](#) was published. This Package includes, amongst others, a (i) "Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures", [COM\(2025\) 501 final](#); (ii) "Proposal for a Directive of the European Parliament and of the Council amending Directives 2014/65/EU and (EU) 2022/2557 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplifying measures", [COM\(2025\) 502 final](#); (iii) "Proposal for a Directive of the European Parliament and of the Council amending Directives 2000/14/EC, 2011/65/EU, 2013/53/EU, 2014/29/EU, 2014/30/EU, 2014/31/EU, 2014/32/EU, 2014/33/EU, 2014/34/EU, 2014/35/EU, 2014/53/EU, 2014/68/EU and 2014/90/EU of the European Parliament and of the Council as regards digitalisation and common specifications", [COM\(2025\) 503 final](#); and (iv) "Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) No 765/2008, (EU) 2016/424, (EU) 2016/425, (EU) 2016/426, (EU) 2023/1230, (EU) 2023/1542 and (EU) 2024/1781 as regards digitalisation and common specifications", [COM\(2025\) 504 final](#). The Commission introduces the new term "small mid-cap enterprises" (**SMCs**), which is intended to cover larger companies than the previous term of SMEs. Like SMEs, this new category of enterprises will benefit from the administrative burden reduction measures of Omnibus IV. In addition to the **GDPR**, the **MiFID** and the **CER** directives will be revised. The **other two legislative proposals** modernise several specified Directives and Regulations by introducing the "**digital by default**" principle. According to the first proposal, COM(2025) 501 final, the **GDPR** obligation to maintain a **record of processing activities** will no longer apply to companies and organisations with fewer than 750 employees, provided the processing activity is unlikely to result in a high risk within the meaning of Art. 35 GDPR. Read more in our [technology & digitalisation newsletter 06/2025](#).
- On **16 June 2025**, the Council and the European Parliament reached a provisional deal on the draft of the new **GDPR Procedural Regulation**, [COM\(2023\) 348 final](#). This Regulation aims to harmonise the admissibility of cross-border data protection complaints. Among other things, deadlines and mechanisms in the **coherence mechanism** were agreed upon ([Press release of the Council](#); [Press release of the EP](#)).

### Commission guidelines

#### Commission Guidelines on Protection of Minors Online under the Digital Services Act

- On **13 May 2025**, the **Commission** published its [Guidelines](#) on the **Protection of Minors Online for public consultation**. Pursuant to **Art. 28 Digital Services Act** ("Online Protection of Minors"), **online platforms** accessible to minors must take appropriate and proportionate measures to ensure a high level of privacy, safety and security of minors within their services. While the DSA does not prescribe specific measures, Art. 28(4) empowers the Commission to issue guidelines to assist platform providers in the application of such measures. Read more in our [technology & digitalisation newsletter 06/2025](#).

### European Data Protection Board (EDPB)

#### Guidelines 02/2024 on Article 48 GDPR<sup>2</sup>

- Following a public consultation, the **EDPB** published the final "[Guidelines 02/2024 on Article 48 GDPR<sup>2</sup>](#)" on **5 June 2025**. Pursuant to Art. 48 GDPR, judgments or decisions of courts and administrative authorities of a third country may only be recognised or enforced if based on an international agreement. The Guidelines provide recommendations to controllers and processors on how to handle requests from courts and administrative authorities from third countries. They clarify that the disclosure of personal data at the request of a third country's authority is only permissible if it complies with the principles of Art. 5 GDPR, is based on a legal basis under Art. 6 GDPR and relies on a valid **transfer mechanism** under Chapter V GDPR ("**two-step test**").

## **Council recommendation**

### Cyber Blueprint

- On **6 June 2025**, the "**Cyber Blueprint**", a recommendation of the Council, was adopted. This blueprint aims to establish a Union-wide framework for cybersecurity crisis management in the event of a large-scale cybersecurity incident. It describes cooperation mechanisms between the various actors involved.

## **European Commission decisions**

### Digital Markets Act – Apple and Meta

- On **23 April 2025**, the **European Commission (EC)** published a press release announcing, among other things, that it had imposed fines on Apple and Meta based on the Digital Markets Act (**DMA**). Apple was fined EUR 500m for failing to comply with the DMA's **steering terms**. Meta was fined EUR 200m for a binary "consent or pay" model (which in the meantime has been modified). Furthermore, the EC determined that Facebook Marketplace should no longer be designated as an online intermediation service under the DMA ([EC press release 23 April 2025, IP/25/1085](#)).

### Digital Services Act – AliExpress

- On **18 June 2025**, the **European Commission (EC)** published a press release announcing its acceptance of commitments offered by **AliExpress** to comply with the Digital Services Act (**DSA**), while noting violations by AliExpress regarding the dissemination of illegal products. Through the commitments offered and made binding, the Commission hopes to increase the transparency of the platform's **advertising and recommender systems** ([EC press release 18 June 2025, IP/25/1551](#)).

## **Commission delegated and implementing regulations (incl. drafts)**

### Regulation on Political Advertising

- On **30 April 2025**, the European Commission published a [Draft Implementing Regulation](#) including an **annex to Regulation (EU) 2024/900** on the **transparency and targeting of political advertising**. The Implementing Regulation specifies the format, template and technical specifications for **labelling** and **transparency notices** related to political advertisements.

### eIDAS

- On **7 May 2025**, the following Commission Implementing Regulations were published: (i) "Commission Implementing Regulation (EU) 2025/846 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards cross-border identity matching of natural persons", [OJ L 2025/846](#); (ii) "Commission Implementing Regulation (EU) 2025/847 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reactions to security breaches of European Digital Identity Wallets", [OJ L 2025/847](#); (iii) "Commission Implementing Regulation (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties", [OJ L 2025/848](#); and (iv) "Commission Implementing Regulation (EU) 2025/849 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the submission of information to the Commission and to the Cooperation Group for the list of certified European Digital Identity Wallets", [OJ L 2025/849](#). These four implementing regulations establish and specify requirements and obligations concerning **European Digital Identity Wallets** within the meaning of [eIDAS](#).

### MiCAR

- On **10 June 2025**, the following three delegated regulations supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets [...] (**MiCAR**) were published: (i) "Commission Delegated Regulation (EU) 2025/1140 of 27 February 2025, supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the records to be kept in relation to all crypto-asset services, activities, orders, and transactions," [OJ L 2025/1140](#); (ii) "Commission Delegated Regulation (EU) 2025/1141 of 27 February 2025 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the requirements for conflict of interest policies and procedures for issuers of asset-

referenced tokens," [OJ L 2025/1141](#); and (iii) "Commission Delegated Regulation (EU) 2025/1142 of 27 February 2025 supplementing Regulation (EU) 2023/ 1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the requirements for conflicts of interest policies and procedures for crypto-asset service providers and the details and methods for the content of conflicts of interest disclosures," [OJ L 2025/1142](#). These three delegated regulations supplement **MiCAR** by establishing **technical regulatory standards** on **record-keeping obligations** and **conflicts of interest**. The record-keeping obligations cover both recording modalities and retention obligations.

## Austrian legal acts

### Ordinance on Itemised Bills 2025

- On **23 April 2025**, the "Ordinance of the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR-GmbH) specifying the level of detail and the format for itemised bills" ("Einzelentgeltnachweisverordnung 2025"; EEN-V 2025) was published in the [Federal Law Gazette II 2025/75](#). The **Ordinance on Itemised Bills 2025** regulates the format of **itemised bills** for charging the provision of **number-based interpersonal communication services** and **internet access services**. Number-based interpersonal communications services are fixed (land-line) and mobile telecommunication services, but also internet-based services that enable communication with a telephone number (e.g. Viber). Internet access services provide access to the internet (e.g. A1, Magenta and Hutchison Drei).

### Upper Austrian Information Technology Application Act

- On **12 June 2024**, the "*Upper Austrian Information Technology Application Act*" (Oö ITEG) was published in the [Provincial Law Gazette 2025/46](#). The aim is to promote digital transformation, the usage of **artificial intelligence** and **automated decisions** in the state parliament, the state court of audit, the state administrative court, and the authorities and agencies of the state of Upper Austria, the Upper Austrian municipalities and municipal associations, and other Upper Austrian public entities. In particular, participation in **AI regulatory sandboxes** is encouraged. In addition, decisions made by these entities as holders of private rights may be based on automated decisions.

### "ID Austria" mobile app

- On **20 June 2025**, the "**ID Austria**" mobile app (formerly "Digitales Amt") for digital identity was officially launched, enhancing eID, eSignature and qualified signature services (<https://secure.oesterreich.gv.at>). The login process has also been changed. Users can now choose between fingerprint or facial recognition or enter their device password or PIN code. ID Austria enables users to verify their identity to digital applications and authorities (digital identity) and meets the requirements of the eIDAS Regulation, making it legally valid throughout Europe.

### Austrian Accessibility Act

- The "**Austrian Accessibility Act**" (*Barrierefreiheitsgesetz* or BaFG) implementing Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the **accessibility requirements** for products and services, [OJ L 2019/151, 70](#), into Austrian law, was published in the [Federal Law Gazette I 76/2023](#) and will enter into force on **28 June 2025**. The Act establishes mandatory accessibility requirements for certain products and services provided to consumers, including, but not limited to, POS terminals, ATMs, e-readers, electronic communication services, audiovisual media services, banking services and e-commerce services. The Act contains provisions governing the obligations of producers, importers, distributors and service providers, as well as enforcement provisions for ensuring compliance.

### Austrian Data Access Act

- On **18 June 2025**, the Austrian National Council adopted the [government's bill](#) on the Austrian **Data Access Act** (*Datenzugangsgesetz*, DZG), implementing Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (**Data Governance Act**; [OJ L 2022/152](#)). The Act will establish a federal law governing data governance, providers of data intermediation services and data altruism organisations. Its aim is to introduce a uniform governance framework for the reuse of public sector data and data ecosystems, and to promote data altruism.

## **Bulgarian legal acts**

### Act on Accessibility Requirements for Products and Services

- On 11 April 2025, the Act on Accessibility Requirements for Products and Services, implementing Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services, [OJ L 2019/151, 70](#), and providing for measures for the implementation of Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products, [OJ L 2019/169](#), into Bulgarian law, was published in the [State Gazette No. 31/2025](#). The Act will enter into force on 28 June 2025. The Act regulates: (i) the accessibility requirements for certain products and services (e.g. audiovisual media services, consumer banking services, e-commerce services, etc.); (ii) the procedure for assessing the conformity of products with accessibility requirements; (iii) the obligations of economic operators making products available on the market or providing services; (iv) the supervision of products made available on the market and/or put into service; and (v) monitoring the compliance of the provided services with accessibility requirements.

### Act on Markets in Crypto-Assets

- On **20 June 2025**, the National Assembly adopted the **Act on Markets in Crypto-Assets**. The Act introduces the measures for the implementation of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (**MiCAR**), as well as the implementing acts related to the conditions and procedures for the licensing, operation and state supervision of crypto-asset issuers and crypto-asset service providers. The Act has not yet been published in the State Gazette but is expected imminently.

## Croatian legal acts

### Decision on the Publication of Price Lists and Quotation of Additional Prices Intended as a Measure of Direct Price Control in Retail Sale

- The Decision on the Publication of Price Lists and Quotation of Additional Prices Intended as a Measure of Direct Price Control in Retail Sale (the "**Decision**"), adopted by the Government of the Republic of Croatia and published in the [Official Gazette No. 75/2025](#), entered into force on **15 May 2025**. The Decision provides for mandatory online publication of retail prices for food-stuffs, drinks, cleaning products, toiletries and household items, and applies to all retailers categorised as supermarkets, hypermarkets, discount shops and cash & carry. The retailers are required to publish their price lists in digital, machine-readable format (.xml or .csv), compatible with software tools and automated programs designed to gather price data in real time. The price lists must be updated daily and accessible online for 30 days after publication.

### Act on Accessibility Requirements for Products and Services

- The Act on Accessibility Requirements for Products and Services (the "**Accessibility Act**"), implementing Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the **accessibility requirements** for products and services, [OJ L 2019/151, 70](#), into Croatian law, was published in the [Official Gazette No. 89/2025](#) and will enter into force on **28 June 2025**. The Act introduces mandatory accessibility requirements for certain products and services provided to consumers, including, but not limited to, POS terminals, ATMs, e-readers, electronic communication services, audiovisual media services, banking services and e-commerce services. The Act contains provisions governing the obligations of producers, importers, distributors and service providers, as well as enforcement provisions for ensuring compliance.

### Fiscalisation Act

- The **Fiscalisation Act**, published in the [Official Gazette No. 89/2025](#) and scheduled to enter into force on **1 September 2025**, is set to replace the current Act on the Fiscalisation of the Circulation of Cash. The new Act consolidates the existing rules on fiscalisation of cash transactions and electronic invoices in B2C relations and extends their application to all B2B relations and cashless transactions. The new legal framework is expected to reduce the administrative burden on taxpayers, as all electronic invoices will be automatically registered with the Tax Administration.

## Hungarian legal acts

### Act amending certain laws in connection with cash payment

- On **20 June 2025**, Act LXII of 2025 on the Amendment of Certain Laws in Connection with the Use of Cash (the "**Act**") was published in the [Hungarian Gazette No. 2025/74](#) and will enter into force on **1 July 2025**. Hungary has recently recognised **cash payment** as a **fundamental right**. In connection with this, the Act obligates businesses to **offer consumers the option to settle payments in cash**. Notably, the Act sets out certain exceptions, including online service contracts, cross-border online sales contracts and sales conducted in automated stores.



## Moldovan legal acts

### Law on Cybersecurity

- On **1 January 2025** the **Law on Cybersecurity** No.º48 dated 16 March 2023 (*Legea privind securitatea cibernetică*) entered into force, as published in [Official Gazette No.151-153 of 28 April 2023](#). It transposes Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (**NIS 2 Directive**). The law establishes the normative, organisational and cooperation framework for cybersecurity in Moldova, sets out the competences of public authorities and institutions in the field, defines the national crisis management framework for cybersecurity, and introduces requirements, measures and mechanisms to ensure the security of networks and IT systems essential for the functioning of society. It also provides for the management of cyber incidents at a national level.

### Law on Promoting Fairness and Transparency for Business Users of Online Intermediation Services

- On **22 April 2025** the **Law on Promoting Fairness and Transparency for Business Users of Online Intermediation Services** No.º53 dated 20 March 2025 (*Legea privind promovarea echităţii şi a transparenţei pentru întreprinderile utilizatoare de servicii de intermediere online*) was published in [Official Gazette No. 193-194](#) and will enter into force on 22 April 2026. The law partially transposes "Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services" (**P2B Regulation**). Its purpose is to ensure the smooth functioning of the market by establishing rules that guarantee an adequate degree of fairness, transparency and effective remedial measures for businesses using online intermediation services and professional website users in their interactions with online search engines.

### Law on Electronic Communications

- On **15 May 2025**, the **Law on Electronic Communications** No.º72 dated 10 April 2025 (*Legea comunicatiilor electronice*) was published in [Official Gazette No. 226-228](#), with entry into force slated for 1 January 2026. It partially transposes several European Union directives and regulations, including Directive (EU) 2018/1972 establishing the European Electronic Communications Code (Recast), Commission Delegated Regulation (EU) 2021/654 supplementing Directive (EU) 2018/1972, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, Commission Directive 2008/63/EC on competition in the markets in telecommunications terminal equipment, Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse. The law establishes the national regulatory framework for electronic communications networks and services, associated facilities and certain aspects of terminal equipment. It defines the responsibilities of relevant authorities, as well as the rights and obligations of natural and legal persons involved in the creation, management and use of electronic communications networks.

### Instruction regarding the procedure for stopping access to web pages containing information intended and used for preparing or committing crimes and for removing the respective content at the source

- On **28 May 2025**, the Government of the Republic of Moldova adopted Decision No.º317 on the approval of the **Instruction** regarding the procedure for stopping access to web pages containing information intended and used for preparing or committing crimes and for removing the respective content at the source. This decision was published in [Official Gazette No. 289-292](#) of **3 June 2025**. The instruction establishes the procedures for the identification of web pages containing information intended and used for preparing or committing crimes, for the implementation of the order to stop access to a web page or to remove online content at the source, as well as for the cooperation between the Ministry of Internal Affairs and/or the Information and Security Service and Internet access service providers, online content hosting service providers and/or content providers, in order to implement measures to stop access or removal of the content at the source.

## Polish legal acts

### Act amending the Act on Electronic Delivery

- On **1 January 2025**, the Act amending the **Act on Electronic Delivery** dated 18 November 2020 came into force. The amendment introduces a transitional period, which will last until 31 December 2025, during which public entities will be able to waive the service of correspondence to an electronic delivery address or using a public hybrid service due to organisational reasons assessed by the authority itself. The reason for the amendment is that some public entities are not ready to apply the solutions set out in the Act on Electronic Delivery, in particular with regard to the delivery of correspondence using the Public Registered Electronic Delivery Service (PURDE) or the Public Hybrid Service (PUH). The amended Act can be found [here](#).

### Guide to Data Protection Breaches (*Poradnik na gruncie RODO - Obowiązki administratorów związane z naruszeniami ochrony danych osobowych*)

- On **20 February 2025**, the President of the Personal Data Protection Office published an updated version of its **Data Protection Breaches Guide**. The guide is a source of knowledge for controllers and data protection officers. The latest version takes into account the current legislation, the experience from the past practice of applying the GDPR and the results of the public consultation. The guide was published on the [website of the President of the Personal Data Protection Office](#).

### Act on Accessibility Requirements for Products and Services

- By **28 June 2025**, businesses (excluding microenterprises) must adapt their products and services to meet EU accessibility requirements. The new **Act on Accessibility Requirements for Products and Services** will apply to manufacturers, importers, distributors and service providers. Products subject to accessibility requirements include computers and operating systems, payment and self-service terminals (e.g. ATMs, ticket machines), consumer end-user devices used to provide telecommunications and e-book readers. Services subject to accessibility requirements include telecommunications and audiovisual media services, passenger transport services (rail, air, road and water), retail banking, e-commerce and e-book services. The Act can be found [here](#).

## **Romanian legal acts**

Norm No. 14/2025 amending and supplementing Norm of the Financial Supervisory Authority No. 4/2018 on the management of operational risks generated by information systems used by entities authorised/approved/registered, regulated and/or supervised by the Financial Supervisory Authority ("Norm 14/2025")

- On **26 May 2025**, **Norm 14/2025** was published in the [Romanian Official Gazette No. 587 of 26 May 2025](#). It introduces slight amendments to the existing Norm 4/2018 in order to align with the provisions of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/101 (**DORA**) for entities regulated and/or supervised by the Romanian Financial Supervisory Authority.

Regulation No. 1/2025 on the amendment of certain legal acts issued by the National Bank of Romania ("Regulation 1/2025")

- The National Bank of Romania (NBR) made some amendments to its existing regulations to align with the **DORA** Regulation through Regulation 1/2025 (*Regulamentul nr. 1/2025 privind modificarea unor acte normative emise de Banca Națională a României*). The main amendments introduced by Regulation 1/2025 refer to the observance of the DORA requirements in the context of ICT activities and ICT incident reporting. Regulation 1/2025 was published in the [Romanian Official Gazette No. 489](#) on **26 May 2025**.

Law No. 232/2022 on accessibility requirements applicable to products and services ("Law 232/2022")

- [Law 232/2022](#) (*Legea nr. 232/2022 privind cerințele de accesibilitate aplicabile produselor și serviciilor*), which enters into force on **28 June 2025**, transposes the EU Accessibility Act into national law and sets specific requirements for products and services, including websites and apps, to ensure they are accessible to individuals with disabilities.

Draft Order on the approval of the requirements for the notification/registration process under NIS2

- On **30 April 2025**, the Romanian National Directorate for Cybersecurity (DNSC) published a [draft order](#) for approving the **requirements regarding the notification/registration process under the NIS2 Directive** (*Ordinul pentru aprobarea cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor*). The draft order establishes the registration process and an online platform where the companies that fall under the requirements of NIS2 must register as essential/important entities. The draft order is currently awaiting final approval following the public consultation.

Draft order on the approval of criteria and thresholds for determining the degree of disruption of a service and the methodology for assessing the risk level of entities under NIS2

- On **30 April 2025**, the DNSC also published a [draft order](#) regarding the **criteria and thresholds for determining the degree of disruption of a service and the methodology for assessing the risk level** of entities under NIS2 (*Ordinul pentru aprobarea criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și metodologia de evaluare a nivelului de risc al entităților*). The draft order establishes a set of criteria and a methodology that would help entities determine whether they qualify as essential or important entities under NIS2. The draft order is currently awaiting final approval following the public consultation.

## Slovenian legal acts

Act amending the Act on the Promotion of Digital Inclusion (*Zakon o spremembah Zakona o spodbujanju digitalne vključenosti*)

- On **13 February 2025**, the act on the promotion of digital inclusion underwent a minor amendment, predominantly eliminating a state-run mechanism that allowed rental of computer equipment. The act was published in the [Official Gazette of the Republic of Slovenia, No. 12/2025](#).

Act amending the Act on Prevention of Money Laundering and Terrorist Financing Act (*Zakon o spremembah Zakona o preprečevanju pranja denarja in financiranja terorizma*)

- On **29 March 2025**, the Prevention of Money Laundering and Terrorist Financing Act underwent an amendment following the transposition of **Directive 2015/849/EU** insofar as it relates to amendments to the crypto-asset market. Regulation 2020/2223/EU, which establishes **cooperation between the competent national authority and the European Anti-Fraud Office (OLAF)**, has also been implemented. The act was published in the [Official Gazette of the Republic of Slovenia, No. 17/2025](#).

Act amending the Banking Act (*Zakon o spremembah Zakona o bančništvu*)

- On **29 March 2025**, the Banking Act underwent an amendment following alignment with **Regulation 2023/1114/EU (MiCAR)** insofar as it relates to amendments to Directive 2013/36/EU. The act was published in the [Official Gazette of the Republic of Slovenia, No. 17/2025](#).

Act implementing Regulation (EU) on information accompanying the transfer of funds and certain crypto-assets (*Zakon o izvajanju uredbe (EU) o informacijah, ki spremljajo prenos sredstev in nekaterih kriptosredstev*)

- On **2 April 2025**, the act implementing **Regulation (EU) 2023/1113** of 31 May 2023 on information accompanying transfers of funds and certain cryptocurrencies and amending Directive (EU) 2015/849, entered into force. The act sets out the competent authorities for the supervision of payment service providers and intermediary payment service providers, cryptocurrency service providers and intermediary cryptocurrency service providers, the manner in which supervision is to be carried out, the supervisory measures, the procedure for imposing supervisory measures, and the offences and fines relating to the implementation of Regulation 2023/1113/EU. The act was published in the [Official Gazette of the Republic of Slovenia, No. 17/2025](#).

Regulation implementing Regulation (EU) on digital operational resilience for the financial sector (*Uredba o izvajanju uredbe (EU) o digitalni operativni odpornosti za finančni sektor*)

- On **26 April 2025**, the regulation implementing **Regulation (EU) 2022/2554 (DORA)** entered into force. Among other things, the regulation sets out the competent bodies overseeing compliance with DORA and fines for non-compliance, which may range up to EUR 500,000. The regulation was published in the [Official Gazette of the Republic of Slovenia, No. 25/2025](#).

Information Security Act (*Zakon o informacijski varnosti*)

- On **19 June 2025**, the amended **Information Security Act** entered into force. The act upgrades the national cybersecurity system and transposes the European **NIS2 Directive** (Directive 2022/2555/EU) into national legislation. The key new features include the introduction of a self-registration platform for entities covered by this law, a unified platform for incident reporting, and a platform for secure information exchange. The act was published in the [Official Gazette of the Republic of Slovenia, No. 40/2025](#).

## Turkish legal acts

### Compliance obligations for cross-border e-commerce products

- A new regulation issued by the Turkish Ministry of Trade to enhance product safety in e-commerce has officially entered into force. The Regulation on Market Surveillance of Products Offered through Remote Communication Tools (the "**Regulation**") was published in [Official Gazette No. 32707](#) on **30 October 2024** and became effective on **1 April 2025**. The Regulation sets out the conditions for offering products through remote communication tools and defines the obligations of economic operators and service providers, aiming to strengthen consumer protection, ensure that products sold online meet applicable safety standards and align national practices with EU market surveillance frameworks. Under the revised rules, appointing a responsible economic operator established in Türkiye has become a prerequisite for the sale of products procured from abroad through remote communication tools. These operators are responsible for preparing and retaining technical documentation, notifying the competent authority of non-compliant products in a timely manner and implementing corrective actions when necessary. The Regulation further requires that all product listings clearly include seller and manufacturer information, safety warnings in Turkish, conformity markings and accurate visuals and descriptions.

### Communiqué on keeping commercial books not related to the accounting of the business in electronic format

- A new Communiqué, published in [Official Gazette No. 32813](#) on **14 February 2025**, introduced the option and, in some cases, the obligation for companies in Türkiye to maintain non-accounting commercial books, such as share ledgers and board resolution books, in electronic form through the Electronic Bookkeeping System (EBS), integrated with Central Registration Systems (MERSIS). As of **1 July 2025**, all companies incorporated on or after **1 January 2026**, as well as specific regulated entities including banks, insurance firms, financial institutions and capital market players, are mandated to use the EBS. Voluntary transition is available for other companies, provided they digitise all relevant books.

### Implementation of the Centralised Crypto-Asset Reporting System by the Central Securities Depository of Türkiye

- On **27 May 2025**, the Central Securities Depository of Türkiye (MKK) initiated the implementation of a new digital infrastructure for crypto-asset data reporting (the "**System**"). This System has been developed pursuant to the Communiqué on the Principles of Establishment and Operation of Crypto-Asset Service Providers ([III-35/B.1](#)) and the Communiqué on the Operational Procedures and Capital Adequacy Requirements of Crypto-Asset Service Providers ([III-35/B.2](#)), both issued by the Capital Markets Board of Türkiye and published in [Official Gazette No. 32840](#) dated **13 March 2025**. The System is designed to ensure secure and standardised data flow between the MKK and platforms operating as crypto-asset service providers. These platforms will be required to report transaction-level information, such as purchase and sale operations, initial offerings or distributions, clearing and transfers, as well as custody records and customer balances, directly to the MKK. With the implementation, investors will be able to verify and compare platform records with those of the MKK through the e-YATIRIMCI (e-investors). The deadline for crypto service providers to complete their technical and integration applications to the MKK has been set for **20 June 2025**.

### Law on Cybersecurity

- Cybersecurity Law No.º 7545 (the "**Cybersecurity Law**"), which was published in [Official Gazette No. 32840](#) and entered into force on **19 March 2025**, establishes a national cybersecurity framework applicable to public institutions, private entities and individuals operating in cyberspace. The law grants extensive authority to the Cybersecurity Directorate, including the regulation and supervision of the sector, on-site inspections, imposition of administrative sanctions and development of standards for cybersecurity products and services. The Cybersecurity Law also imposes specific obligations on IT and cybersecurity companies, such as incident reporting, procurement of certified cybersecurity tools for use in public infrastructure and obtaining prior approval for certain transactions and exports.

to the point

# Digital Law Monitor. 3/2025

Welcome to the **3/2025 edition** of the **Digital Law Monitor**.

Keeping up with developments in digital law is becoming increasingly challenging. To assist you in navigating this area, we have created a comprehensive (though not exhaustive) overview of these developments, which we will update regularly. The overview includes **legal acts**, **draft legal acts**, **guidelines** and occasionally other legal materials. Please [subscribe](#) here.

For **weekly news**, please subscribe to the [Schönherr Datenschutzmonitor](#) for updates on legal acts and guidelines (in German).

For **detailed information** on digital law developments, check out our [technology & digitalisation news corner](#) and our periodic [technology & digitalisation newsletter](#).

Please also read our quarterly newsletter on [healthcare & life sciences](#), as well as our regular newsletter on [financial regulation](#).

## **EU legal acts**

### • **Regulations**

Corrigendum to Regulation (EU) 2024/2847 (Cyber Resilience Act)

Applicability of AI Act governance provisions

Applicability of the Data Act

Digital Omnibus (Call for evidence)

### • **Commission Guidelines**

General-Purpose AI Code of Practice

Explanatory Notice and Template for the Public Summary of Training Content for General-Purpose AI Models

General-Purpose AI Code of Practice

### • **European Data Protection Board**

Guidelines 3/2025 on the interplay between the DSA and the GDPR (2025)

### • **Commission Delegated and Implementing Regulations (incl. drafts)**

Open Internet Access Regulation (fair use)

Adequacy Decisions (UK, Patent Organisation)

Digital Services Act (data access portal)

Cybersecurity (certification)

Digital Operational Resilience Act (DORA)

Markets in Crypto-Assets Regulation (MiCA)

Regulation on the transparency and targeting of political advertising

Energy Performance of Buildings

Interoperable Europe Act

eIDAS

## **Austrian legal acts**

Amendment to the Universities Act 2002 and Education Documentation Act 2020

Guidelines on the Freedom of Information Act

Data Access Act

Freedom of Information Amendment Act

Amendment to the Banking Act (Banking Secrecy)

Amendment to the Criminal Code (Cyberflashing)

Amendment to the Number Portability Ordinance 2022

MiCA Issuer Reporting Ordinance

Applicability of the Freedom of Information Act

Data Governance Designation Ordinance

## **Bulgarian legal acts**

Act on Markets in Crypto-Assets

Decision on the management of the radio frequency spectrum for civil needs

Decision amending and supplementing the rules for the Free Use of the Radio Frequency Spectrum

Decision on the Rules for the Use of Radio Frequency Spectrum

Decree on the amendment and supplementation of the Ordinance on the register of base stations of terrestrial networks

#### **Croatian legal acts**

Act on the Implementation of the Data Governance Act

Ordinance on Authorisations for Crypto-Asset Service Providers

Decision on the Method of Exercising Supervision on MiCA

Decision on Reports for the Purpose of Supervising Issuers of Asset-Referenced Tokens

Decision on the Handling of Complaints against Issuers of Asset-Referenced Tokens and E-Money Tokens

Decision on the Implementation of Regulation (EU) 2024/1183 establishing the European Digital Identity Framework

Draft Act on Amendments to the Act on Administrative Cooperation in Tax Matters

Draft Act on Cross-Border Procurement of Electronic Evidence in Criminal Proceedings

Draft Act on the Amendment to the Electronic Communications Act

Draft Ordinance on the Payment of Fees for the Activities Conducted by Croatian Regulatory Authority for Network Industries

#### **Czech legal acts**

Amendment to the Electronic Communications Act

Act on the Digitalisation of the Financial Market

Act on the implementation of EU legislation in the field of financial market digitalisation and sustainability finance

Decree on categorisation of malicious calls or other malicious communications

Amendment to the Act on eHealth

Cybersecurity Act

Act amending certain laws in connection with the adoption of the Cybersecurity Act

Critical Infrastructure Act

#### **Hungarian legal acts**

Amendment to the implementing rules of the Cybersecurity Act

Amendment of certain cybersecurity-related SARA decrees

#### **Moldovan legal acts**

Law on digital economy and electronic services

Government Decision on Cybersecurity Obligations for Critical Sectors

#### **Polish legal acts**

Act on the National Cybersecurity Certification System

Draft Act on the Crypto-Asset Market

#### **Romanian legal acts**

DNCS Order on the approval of the requirements for the notification/registration process under NIS2 Directive and on the approval of criteria and thresholds

#### **Slovenian legal acts**

Media Act

Decision on establishing a list of categories of electronic communications and digital client devices intended for access to information society services or media

Decision on the application of ESMA Guidelines in accordance with the Markets in Crypto-Assets Regulation (MiCA)

#### **Turkish legal acts**

Communiqué on the Implementation Procedures and Principles of the Technology Move Programme

Technology Move Programme Implementing Procedures and Principles Communiqué

## EU legal acts

### Regulations

Corrigendum to Regulation (EU) 2024/2847 (Cyber Resilience Act)

- On **2 July 2025**, Art. 64(10) of Regulation (EU) 2024/2847 ([Cyber Resilience Act](#)) was **editorially corrected** in the English-language version, [OJ L 2025/90555](#).

Applicability of AI Act governance provisions

- On 2 August 2025, the governance provisions of the AI Act entered into force.

Applicability of the Data Act

- On **12 September 2025**, the **Data Act** ([2023/2854](#)) became directly applicable. It regulates, among other things, access to data generated by data-driven technologies (**Internet of Things**).

Digital Omnibus

- On **16 September 2025**, the Commission published a **call for evidence** regarding **omnibus rules for the digital sector**, [Ares\(2025\)7724296](#). The Commission aims to simplify the rules on **data, cybersecurity** and **artificial intelligence**.

### Commission Guidelines on the AI Act

- On **10 July 2025**, the "[General-Purpose AI Code of Practice](#)" was published. The Code of Practice is divided into three chapters: **Safety and Security**, **Transparency** and **Copyright**. The Code of Practice was prepared by independent experts.
- On **24 July 2025**, the **European Commission** published the "[Explanatory Notice and Template for the Public Summary of Training Content for general-purpose AI models](#)". In accordance with Art. 53(1)(d) **AI Act** (Regulation (EU) 2024/1689), **providers of general-purpose AI models** must draw up and make publicly available a sufficiently detailed summary of the content used to train the general-purpose AI model. In doing so, they must adhere to the **Template** provided by the **AI-Office**, which was established within the Commission. General-purpose AI models are used in applications such as ChatGPT, Microsoft Copilot and Google Gemini.
- On **1 August 2025**, the European Commission confirmed that the **Code of Practice for General-purpose AI** constitutes an appropriate voluntary tool for providers of GPAI models to demonstrate compliance with the [AI Act 2024/1689, Commission Opinion C\(2025\) 5361 final](#). The Code of Practice was developed at the EU level with the involvement of a broad range of stakeholders and consists of the following chapters: **Safety and Security**, **Transparency** and **Copyright**.

### European Data Protection Board (EDPB)

Guidelines 3/2025 on the interplay between the DSA and the GDPR (2025)

- On **12 September 2025**, the European Data Protection Board (EDPB) published the draft [Guidelines 3/2025 on the interplay between the DSA and the GDPR](#) for public consultation. The Guidelines of the EDPB address issues such as dark patterns, **transparency, recommender systems** and the **protection of minors**.

### Commission Delegated and Implementing Regulations

Open Internet Access Regulation

- On **23 June 2025**, the EU Commission published a [proposal for an implementing regulation](#) regarding the technical conditions for **fair use** (based on typical usage patterns) and **anti-fraud measures for international calls and text messages within the EU**. Intra-EU communications differ in nature from roaming and are intended for different types of use. Contrary to intra-EU communications, regulated roaming is a cross-border service intended for periodic travelling and not for permanent use. The proposed fair use policy should **provide consumers with appropriate volumes** of intra-EU calls and SMS messages, while also permitting for future adjustments based on market conditions and consumers' behaviour. Typical usage of intra-EU calls and SMS messages may vary depending on the type of consumer, the provider or the Member State. Therefore, typical usage conditions should give providers sufficient flexibility to establish a fair use policy



they deem appropriate, in compliance with the **Open Internet Access Regulation** (Regulation (EU) 2015/2120) and this proposed regulation, while also allowing for future adjustments. After the Commission's adoption, the draft act will **enter into force in the fourth quarter of 2025**.

#### Adequacy Decisions

- On **26 June 2025**, "Commission Implementing Decision (EU) 2025/1225 of 24 June 2025 amending Implementing Decision (EU) 2021/1773 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom", [OJ L 2025/1225](#), as well as "Commission Implementing Decision (EU) 2025/1226 of 24 June 2025 amending Implementing Decision (EU) 2021/1772 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom", [OJ L 2025/1226](#), were published. These Implementing Decisions extend the validity of the adequacy decisions applicable to the United Kingdom from 27 June 2025 until 27 December 2025, unless they are extended again.
- On **18 July 2025**, "Commission Implementing Decision (EU) 2025/1382 of 15 July 2025 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the **adequate protection** of personal data by the **European Patent Organisation**", [OJ L 2025/1382](#), was published. While the Commission has adopted adequacy decisions for more than a dozen third countries, the **European Patent Organisation** is the first international organisation to benefit from such a decision.

#### Digital Services Act

- On **1 July 2025**, the Commission adopted the draft "Delegated Regulation on data access under the **Digital Services Act (DSA)** 2022/2065", [C\(2025\) 4340 final](#). This Regulation establishes the **DSA data access portal**, through which vetted researchers may access specific data processed by very large online platforms (**VLOPs**) and search engines (**VLOSEs**).

#### Cybersecurity

- On **1 August 2025**, a **draft Commission Implementing Regulation** was published introducing a mechanism for the **peer review** of National Cybersecurity certification authorities in accordance with the **Cybersecurity Act** (Regulation (EU) 2019/881), [Ares\(2025\)6278765](#).
- On **1 August 2025**, a **draft Commission Implementing Regulation**, [Ares\(2025\)6278517](#), was published, aiming to add or update state-of-the-art documents for cybersecurity certification. State-of-the-art documents specify the evaluation methods, techniques and tools for cybersecurity certification.

#### Digital Operational Resilience Act (DORA)

- On **2 July 2025**, "Commission Delegated Regulation (EU) 2025/532 of 24 March 2025 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the elements that a financial entity has to determine and assess when **subcontracting ICT services** supporting critical or important functions", [OJ L 2025/532](#), was published. This Delegated Regulation supplements the Digital Operational Resilience Act (**DORA**) with regulatory technical standards governing the subcontracting of ICT services.

#### Markets in Crypto-Assets Regulation (MiCA)

- On **15 September 2025**, "Commission Delegated Regulation (EU) 2025/1125 of 5 June 2025 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information in an application for authorisation to offer asset-referenced tokens to the public or to seek their admission to trading", [OJ L 2025/1125](#), was published. With this Delegated Regulation, the Commission supplements "Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on **markets in crypto-assets** [...]" (**MiCA**) and specifies the information to be provided in an **application for authorisation** to offer **asset-referenced tokens** to the public.
- On **15 September 2025**, "Commission Implementing Regulation (EU) 2025/1126 of 5 June 2025 laying down implementing technical standards for the application of Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to the establishment of standard forms, templates and procedures for the information to be included in the application for authorisation to offer asset-referenced tokens to the public and to seek their admission to trading", [OJ L 2025/1126](#),

was published. This **Implementing Regulation** was also adopted based on **MiCA** and contains standard forms, templates and procedures for the **application for authorisation** to offer **asset-referenced tokens** to the public.

#### Regulation on the transparency and targeting of political advertising

- On **16 July 2025**, "Commission Implementing Regulation (EU) 2025/1410 of 9 July 2025 on the format, template and technical specifications of the labels and transparency notices of political advertisements in accordance with Articles 11 and 12 of Regulation (EU) 2024/900 of the European Parliament and of the Council", [OJ L 2025/1410](#), was published. This Implementing Regulation implements [Regulation \(EU\) 2024/900](#) by laying down **technical specifications** for the **labels and transparency notices of political advertisements**. Specific requirements are provided for advertisements on television and radio, as well as in printed and digital media.

#### Energy performance of buildings

- On **29 August 2025**, "Commission Implementing Regulation (EU) 2025/1328 of 30 June 2025 implementing Directive (EU) 2024/1275 of the European Parliament and of the Council by establishing common templates for the transfer of information from national **energy performance of buildings** databases to the EU Building Stock Observatory", [OJ L 2025/1328](#), was published. This Implementing Regulation implements [Directive \(EU\) 2024/1275 on the energy performance](#) of buildings and sets out **common templates** for **transferring information** from the **national databases** for the **energy performance of buildings** to the EU Building Stock Observatory. Prior to transmitting the information, Member States should anonymise **any personal data** by aggregation at country level. **Annex II** of the Commission Implementing Regulation contains formulas for **anonymisation**.

#### Interoperable Europe Act

- On **18 July 2025**, "Commission Implementing Regulation (EU) 2025/1420 of 17 July 2025 laying down rules for the application of Regulation (EU) 2024/903 of the European Parliament and of the Council, as regards the establishment and the operation of the **interoperability regulatory sandboxes**", [OJ L 2025/1420](#), was published. "[Regulation \(EU\) 2024/903 – Interoperable Europe Act](#)" aims to strengthen the cross-border interoperability of network and information systems used to provide or manage public services in the EU. This Implementing Regulation created the legal basis for the establishment and operation of **interoperability regulatory sandboxes**.

#### eIDAS

- On **30 July 2025**, (i) "Commission Implementing Regulation (EU) 2025/1566 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards **reference standards** for the **verification of the identity and attributes of the person** to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued", [OJ L 2025/1566](#), (ii) "Commission Implementing Regulation (EU) 2025/1567 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the **management of remote qualified electronic signature creation devices** and of **remote qualified electronic seal creation devices** as qualified trust services", [OJ L 2025/1567](#), (iii) "Commission Implementing Regulation (EU) 2025/1568 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards **procedural arrangements for peer reviews of electronic identification schemes** and for cooperation on the organisation of such reviews within the Cooperation Group and repealing Commission Implementing Decision (EU) 2015/296", [OJ L 2025/1568](#), (iv) "Commission Implementing Regulation (EU) 2025/1569 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards qualified **electronic attestations of attributes** and electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source", [OJ L 2025/1569](#), (v) "Commission Implementing Regulation (EU) 2025/1570 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards **notification of information** on **certified qualified electronic signature creation devices** and certified qualified **electronic seal creation devices**", [OJ L 2025/1570](#), (vi) "Commission Implementing Regulation (EU) 2025/1571 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the **formats and procedures** for annual reports by **supervisory bodies**", [OJ L 2025/1571](#), and (vii) "Commission Implementing Regulation (EU) 2025/1572 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014

of the European Parliament and of the Council as regards the **format and procedures** for the **notification of intention** and the review prior to the commencement of the provision of qualified trust services", [OJ L 2025/1572](#), were published. These **seven Commission Implementing Regulations** establish requirements, standards and procedures concerning the **European Digital Identity Wallets** under the [eIDAS](#) Regulation.

- On **20 August 2025**, the "Corrigendum to Commission Implementing Regulation (EU) 2025/1570 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notification of information on certified qualified electronic signature creation devices and certified qualified electronic seal creation devices", [OJ L 2025/90654](#), was published. The **Corrigendum** is of relevance because the date of **entry into force** of the corrected Implementing Regulation was brought forward from 19 December 2025 to **19 November 2025**.
- On **4 September 2025**, the draft Commission Implementing Regulations "laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards requirements for qualified trust service providers providing qualified trust services", [Ares\(2025\)7228840](#), and "laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the formats of advanced electronic signatures and seals to be recognised by public sector bodies and repealing Commission Implementing Decision (EU) 2015/1506", [Ares\(2025\)7228727](#), were published. Both drafts will further specify requirements under the [eIDAS](#) Regulation.

## Austrian legal acts

### Amendment to the Universities Act 2002 and Education Documentation Act 2020

- On **1 July 2025**, the "Federal Act amending the Universities Act 2002 and the **Education Documentation Act 2020**," [Federal Law Gazette I 2025/28](#), was published. This created the legal basis for the further development of the **data network for universities and higher education institutions** (DVUH) and the **Austrian Higher Education System Network** (AHESN), as well as for the establishment of a student register and the provision of **digital student ID cards**. The **Register and System Network** (RSV) will be connected to the Bundesrechenzentrum GmbH (BRZ).

### Guidelines on the Freedom of Information Act

- On **30 June 2025**, the Austrian Data Protection Authority (DSB) published its [guidelines on the Freedom of Information Act](#) ("*Informationsfreiheitsgesetz*"; "IFG"). In these guidelines, the DSB provides information on the relationship between **data protection law** and **freedom of information**. It embeds its explanatory considerations within the overall context of the Freedom of Information Act and the Federal Constitution.

### Data Access Act

- On **23 July 2025**, the **Data Access Act** ("*Datenzugangsgesetz*"), [Federal Law Gazette I 33/2025](#), was published. By this federal act, the **Data Governance Act (DGA)**, [Regulation \(EU\) 2022/868](#), is implemented into national law. The DGA governs the re-use of certain data held by public sector bodies. Implementation into national law is not required, as it is an EU Regulation. Under the Data Access Act, the **Federal Chancellor** acts as the competent authority for the registration of **data altruism organisations** and as the **single information point**. Furthermore, the DGA contains provisions on the allocation of data protection roles, penal provisions and an exemption from fees.

### Freedom of Information Amendment Act

- On **24 July 2025**, the "Federal Act adapting legislation to the **Freedom of Information Amendment Act**" ("*Informationsfreiheits-Anpassungsgesetz*"), [Federal Law Gazette I 50/2025](#), was published. With this omnibus amendment, 138 federal acts, including the acts on administrative procedure, are adapted to the new **fundamental right to information** and to the **Freedom of Information Act** ("IFG").

### Amendment to the Banking Act

- On **23 July 2025**, the "Federal Act amending the **Austrian Banking Act**", [Federal Law Gazette I 37/2025](#), was published. This amendment aligns the provisions on banking secrecy with the fundamental right to information and the Freedom of Information Act.

### Amendment to the Criminal Code

- On **24 July 2025**, the "Federal Act amending the **Criminal Code**", [Federal Law Gazette I 45/2025](#), was published. Under this amendment to the Criminal Code ("*Strafgesetzbuch – StGB*"), **cyber-flashing** – the unsolicited sending of images of genitals – becomes a criminal offence.

### Amendment to the Number Portability Ordinance 2022

- On **18 July 2025**, the "Ordinance of the Rundfunk und Telekom Regulierungs-GmbH amending the Number Portability Ordinance 2022" ("*Nummernübertragungsverordnung 2022*"), [Federal Law Gazette II 164/2025](#), was published. The amendment concerns the **continuation** of the contract with the **transferring provider** of a **mobile voice communications service**.

### MiCA Issuer Reporting Ordinance

- On **25 July 2025**, the "Ordinance of the Austrian Financial Market Authority (FMA) on reporting dates, reporting intervals, structure and content of reports pursuant to Regulation (EU) [2023/1114](#) on markets in crypto-assets concerning issuers of asset-referenced tokens and issuers of e-money tokens (**MiCA Issuer Reporting Ordinance – MiCAR-Emittenten-Meldeverordnung; MiCAR-E-MV**)", [Federal Law Gazette II 170/2025](#), was published. The **MiCAR-E-MV** determines, among other things, the content of reports to be submitted by issuers of **asset-referenced tokens** and issuers of **e-money tokens**.

#### Applicability of the Freedom of Information Act

- On **1 September 2025**, the **new fundamental right of access** to information and the **Freedom of Information Act** ("IFG") entered into force. **On the same day**, the availability of the information register was published by ordinance of the Federal Chancellor, [Federal Law Gazette II 2025/52](#). Information of general interest must therefore be made available at [www.data.gv.at](http://www.data.gv.at) no later than **1 December 2025**.

#### Data Governance Designation Ordinance

- On **26 August 2025**, the **Data Governance Designation Ordinance** ("*Daten-Governance-Benennungsverordnung*" - **DGBenV**), [Federal Law Gazette II 2025/186](#), was published. This ordinance designates the **Federal Institute "Statistics Austria"** as the **competent body** for access to the re-use of protected data in certain data categories pursuant to **Section 5(1) of the Data Access Act** (DZG).

## Bulgarian legal acts

### Act on Markets in Crypto-Assets

- On **4 July 2025**, the **Act on Markets in Crypto-Assets** was published in [State Gazette No. 54/2025](#). The Act introduces the measures for the implementation of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets ([MiCA](#)), as well as the implementing acts related to the conditions and procedures for the licensing, operation and state supervision of **crypto-asset issuers** and **crypto-asset service providers**.
- On **15 August 2025**, minor amendments and supplements to the **Act on Markets in Crypto-Assets** were published in [State Gazette No. 67/2025](#). The supplements mainly consist of a new competence of the **Financial Supervision Commission (FSC)**. The FSC may publish a list of websites offering **crypto-asset-related services** provided by persons who are not authorised to operate within the territory of the Republic of Bulgaria. The FSC has the right to submit a request to the Chairman of the Sofia District Court to order all undertakings providing **public electronic communications networks and/or services** to block access to these websites or to display an explicit warning to customers and crypto-asset holders when accessing them.

### Decision No. 213 of 26 June 2025 of the Communications Regulation Commission on the adoption of a Regulatory policy for the management of the radio frequency spectrum for civil needs

- The Decision was published in [State Gazette No. 59/2025](#) on **22 July 2025**. The regulatory policy for the management of **radio spectrum for civil needs** sets out the main objectives that the Communications Regulation Commission must pursue to promote the efficient and coordinated use of radio spectrum, support the establishment and development of pan-European networks, and ensure connectivity, wide availability and the use of very high-capacity networks.

### Decision No. 225 of 10 July 2025 of the Communications Regulation Commission, amending and supplementing the Rules for the Free Use of the Radio Frequency Spectrum

- The Decision was published in [State Gazette No. 60/2025](#) on 25 July 2025. The amendments to the rules are related to the implementation and incorporation into Bulgarian legislation of (i) Commission Implementing Decision (EU) 2024/3157 on the harmonised use of radio spectrum in the 5 945–6 425 MHz frequency band for the implementation of wireless access, systems including radio local area networks (WAS/RLANs); (ii) Commission Implementing Decision (EU) 2025/105 updating harmonised technical conditions in the area of radio spectrum use for short-range devices; and (iii) Commission Implementing Decision (EU) 2025/650 on the update of harmonised technical conditions for short-range devices within the 874-876 and 915-921 MHz frequency bands.

### Decision No. 237 of 17 July 2025 of the Communications Regulation Commission on the amendment and supplementation of the Rules for the Use of Radio Frequency Spectrum for Radio Equipment of the Amateur Radio Service

- The Decision was published in [State Gazette No. 64/2025](#) on 5 August 2025. The Rules introduce a ten-year validity period for personal identification marks of radio amateurs and clubs, personal listener marks, and identification marks of amateur repeaters, radio beacons and other types of automatic fixed radio stations. The relevant documents, including amateur radio operator licences, will be reissued *ex officio*.

### Decree No. 183 as of 12 September 2025 on the amendment and supplementation of the Ordinance on the content, conditions and procedure for keeping, maintaining and using the register of base stations of terrestrial networks

- The Decree of the Council of Ministers was published in [State Gazette No. 76/2025](#) on 16 September 2025. The amendments to the Ordinance aim to clarify its provisions to address practical issues that have arisen during the use of the register.

## Croatian legal acts

### Act on the Implementation of Regulation (EU) 2022/868 on European Data Governance (Data Governance Act)

- The Act on the Implementation of Regulation (EU) 2022/868 on European Data Governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (the "**Implementing Act**") was adopted by the Croatian Parliament on 26 September 2025 and is expected to enter into force on the eighth day after its publication in the Official Gazette. The Implementing Act determines the **national single information point** for the **reuse of protected data**, defines the procedure and fees for the reuse of protected data, and regulates the registration of data intermediation service providers and **data altruism organisations**.

### Ordinance on Authorisations for Crypto-Asset Service Providers, Qualifying Holdings Acquisition Assessment and Appointment Consents for Members of the Management Board

- The Ordinance on **Authorisations for Crypto-Asset Service Providers**, Qualifying Holdings Acquisition Assessment and Appointment Consents for Members of the Management Board (the "**Ordinance**"), adopted by the **Croatian Financial Services Supervisory Agency ("HANFA")** and published in [Official Gazette No. 95/2025](#), entered into force on **6 July 2025**. The Ordinance was adopted as part of a series of regulations implementing the Croatian Act on the Implementation of Regulation (EU) 2023/1114 on markets in crypto-assets. It lists the **required content of authorisation applications** submitted to HANFA by crypto-asset service providers, sets out the conditions for appointing management board members of such providers, and defines the method for assessing the good repute of acquirers of qualifying holdings in crypto-asset service providers.

### Decision on the Method of Exercising Supervision by the Croatian National Bank of the Implementation of Regulation (EU) 2023/1114 on Markets in Crypto-Assets and the Act Implementing that Regulation

- The Decision on the Method of Exercising Supervision by the Croatian National Bank of the Implementation of Regulation (EU) 2023/1114 on **Markets in Crypto-Assets** and the Act Implementing that Regulation (the "**Decision**"), adopted by the governor of the **Croatian National Bank** (the "**HNB**") and published in [Official Gazette No. 100/2025](#), entered into force on **17 July 2025**. The Decision defines the rules for the two supervisory methods applied by the HNB to persons seeking admission to trading of asset-referenced tokens and **e-money tokens**, namely the **continuous monitoring** of reports, data and documents, and the **direct supervision** of the persons concerned.

### Decision on Reports for the Purpose of Supervising Issuers of Asset-Referenced Tokens

- The Decision on Reports for the Purpose of Supervising Issuers of Asset-Referenced Tokens (the "**Decision**"), adopted by the governor of the **Croatian National Bank** (the "**HNB**") and published in [Official Gazette No. 100/2025](#), entered into force on **17 July 2025**. The Decision regulates the mandatory content and deadlines for submitting financial and supervisory reports as part of the HNB's supervision of issuers of asset-referenced tokens.

### Decision on the Handling of Complaints against Issuers of Asset-Referenced Tokens and E-Money Tokens

- The Decision on the Handling of Complaints against Issuers of Asset-Referenced Tokens and E-Money Tokens (the "**Decision**"), adopted by the governor of the **Croatian National Bank** (the "**HNB**") and published in [Official Gazette No. 105/2025](#), entered into force on **31 July 2025**. The Decision regulates the procedure adopted by HNB for handling consumer-filed complaints against issuers of asset-referenced tokens and e-money tokens.

### Decision on the Implementation of Regulation (EU) 2024/1183 establishing the European Digital Identity Framework

- The Decision on the Implementation of Regulation (EU) 2024/1183 establishing the European Digital Identity Framework (the "**Decision**"), adopted by the Government of the Republic of Croatia and published in [Official Gazette No. 121/2025](#), entered into force on **25 September 2025**. The Decision defines the responsibilities of various public bodies in the implementation of the **European Digital Identity Framework**. The principal implementing activities include the modification and

upgrade of the state information infrastructure and the development of the national European digital identity wallet.

#### Draft Act on Amendments to the Act on Administrative Cooperation in Tax Matters

- On **26 September 2025**, the Draft Act on Amendments to the Act on Administrative Cooperation in Tax Matters (the "**Draft Act**") completed its [first reading in the Croatian Parliament](#). The first draft of the Draft Act contains provisions governing the regulatory supervision of the fulfilment of **data-gathering and deep screening obligations** imposed on **crypto-asset service providers**.

#### Draft Act on Cross-Border Procurement of Electronic Evidence in Criminal Proceedings

- The e-public consultation for the [Draft Act on Cross-Border Procurement of Electronic Evidence in Criminal Proceedings](#) (the "**Draft Act**") ended on **30 August 2025**. The Draft Act is intended to implement Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for **electronic evidence in criminal proceedings** and for the execution of custodial sentences following criminal proceedings in the Croatian legal framework by designating the competent national bodies for the issuing of European production orders and European preservation orders.

#### Draft Act on the Amendment to the Electronic Communications Act

- The e-public consultation for the [Draft Act on the Amendment to the Electronic Communications Act](#) ("**Draft Act**") ended on **17 August 2025**. The Draft Act implements Regulation (EU) 2024/1309 on measures to reduce the cost of deploying gigabit electronic communications networks (**Gigabit Infrastructure Act**) by designating the competent national bodies for the implementation of the Regulation and establishing appropriate dispute resolution mechanisms.

#### Draft Ordinance on the Payment of Fees for the Activities Conducted by the Croatian Regulatory Authority for Network Industries

- The Croatian Regulatory Authority for Network Industries ("**HAKOM**") published the [Draft Ordinance on the Payment of Fees for the Activities Conducted by the Croatian Regulatory Authority for Network Industries](#) (the "**Draft Ordinance**"), with the subsequent e-public consultation ending on **10 September 2025**. The Draft Ordinance sets the **fees** payable by **electronic communications operators** used to fund the activities of HAKOM. These include the address and numbering space management fee, the radiofrequency spectrum management fee, and the fee for other activities in the field of electronic communications.



## Czech legal acts

### Amendment to the Electronic Communications Act

- On **7 February 2025**, the Amendment to the Electronic Communications Act, [Gazette No. 23/2025](#), was published. This amendment updates the **Electronic Communications Act** and related laws, including adjustments to the **Act on the Right to Digital Services**. It introduces stricter duties for providers (e.g. obligations on network operators regarding risk assessment, data handling and anti-fraud measures) and updates definitions and procedural rules. The Act also strengthens consumer protection – for instance, by limiting termination fees, ensuring non-discrimination in tariffs and mandating free access to emergency services – and revises enforcement and administrative structures. The main effects entered into force on **1 July 2025**.

### Act to the Digitalisation of the Financial Market

- On **14 February 2025**, the **Act on the Digitalisation of the Financial Market**, [Gazette No. 31/2025](#), was published. This Act establishes a national framework for **MiCA** and other EU digital-finance rules. It defines the rights and obligations of entities providing crypto-asset services and entrusts supervisory powers to the **Czech National Bank**. The Act introduces requirements for the licensing, governance and safeguarding of client assets.

### Act amending certain laws in the field of financial market digitalisation and sustainability finance

- On **14 February 2025**, the Act amending certain laws in connection with the implementation of EU legislation in the field of **financial market digitalisation** and sustainability finance, [Gazette No. 32/2025](#), was published. It updates numerous domestic laws, including the Trade Licensing Act, Banking Act, Act on Savings and Credit Cooperatives and Capital Markets Supervision Act, to accommodate requirements under **MiCA**, **DORA**, **green finance regulations** and related EU acts by inserting new types of regulated activities (e.g. issuing asset-backed tokens, crypto-asset services, crowdfunding services) and aligning oversight, reporting, sanction and procedural regimes.

### Decree on categorisation of malicious calls or other malicious communications

- On **27 March 2025**, the Decree on categorisation of malicious calls or other malicious communications, [Gazette No. 85/2025](#), was published. It sets out categories of malicious emergency-line communications and related blocking measures. The Decree implements Section 33(19) of the **Electronic Communications Act** and establishes specific procedural rules for the interruption of malicious communications.

### Amendment to the Act on eHealth

- On **15 July 2025**, the Amendment to the Act on eHealth, [Gazette No. 236/2025](#), was published. The amendment updates the **eHealth framework**, including electronic documentation, interoperability and data sharing.

### Cybersecurity Act

- On **4 August 2025**, the **Cybersecurity Act**, [Gazette No. 264/2025](#), was published. This new Act, effective as of 1 November 2025, transposes the **NIS-2-Directive** and introduces broad duties for regulated entities, which have 60 days to complete their registration with the National Cyber and Information Security Agency (NÚKIB). The number of regulated entities is expected to increase up to tenfold compared to the current regulation.

### Act amending certain laws in connection with the adoption of the Cybersecurity Act

- On **4 August 2025**, the Act amending certain laws in connection with the adoption of the **Cybersecurity Act**, [Gazette No. 265/2025](#), was published. It harmonises sanctions and procedures across the legal system in connection with the new Cybersecurity Act.

### Critical Infrastructure Act

- On **4 August 2025**, the **Critical Infrastructure Act**, [Gazette No. 266/2025](#), was published. It transposes the **CER Directive** and imposes new obligations on **digital-infrastructure operators**, among others.

## Hungarian legal acts

### Amendment to the implementing rules of the Cybersecurity Act

- On **3 July 2025**, Government Decree No. 189/2025. (VII. 3.) on the implementation of the **Act on Cybersecurity** of Hungary was published in [Hungarian Gazette No. 2025/80](#). The objective of the amendment is to further implement the **EU NIS-2-Directive** and to clarify provisions in light of practical experience gained during their application. Notably, the amendment **introduces new infringements** and **significantly increases the fines** that may be imposed by the competent authority. Read more about cybersecurity in Hungary here: <https://www.schoenherr.eu/content/cybersecurity-in-hungary-how-to-avoid-million-forint-fines-in-2025>.

### Amendment of certain cybersecurity-related SARA decrees

- On **21 August 2025**, Decree No. 8/2025. (VIII. 21.) of the President of the **Supervisory Authority for Regulated Activities (SARA)** on the amendment of certain decrees relating to **cybersecurity** and to sustainability-related due diligence obligations was published in [Hungarian Gazette No. 2025/96](#). The amendments concerning **cybersecurity-related** decrees include the extension of the scope of information that entities must provide during **registration with SARA**, as well as amendments to the requirements applicable to those authorised to **conduct vulnerability assessments**.

## Moldovan legal acts

### Law on amending certain normative acts (supporting the digital economy and electronic services)

- The **Law on amending certain normative acts (supporting the digital economy and electronic services)** No. 144 dated 19 June 2025 [*Legea pentru modificarea unor acte normative (sustinerea economiei digitale si a serviciilor electronice)*] was published in [Official Gazette No. 328](#) on **20 June 2025** and entered into force on **20 September 2025**. The main goal of the amendments is to promote the digital economy and align the Republic of Moldova with global trends in this domain. The key provisions of the law include: (i) allowing cash withdrawals at the point of sale, subject to limits; (ii) extending the **legal framework for digital nomads** to live and work remotely from Moldova under defined conditions; (iii) requiring fiscal receipts to be issued in **both paper and electronic formats**; (iv) **simplifying online registration** for legal entities and individual entrepreneurs; (v) updating the legal framework for **crowdfunding platforms**, including technical, operational and transparency requirements; (vi) aligning Moldovan regulations with EU standards, particularly **for cross-border communications and roaming**; and (vii) expanding the use of **electronic identification** for client verification, including for EU citizens with qualified digital certificates.

### Government Decision on Cybersecurity Obligations for Critical Sectors

- **Government Decision on Cybersecurity Obligations for Critical Sectors** No. 562 dated 3 September 2025 (Hotararea cu privire la modul de realizare a obligatiilor de asigurare a securitatii cibernetice de catre furnizorii de servicii in sectoarele critice) was published in [Official Gazette No. 467-470](#) on **5 September 2025** and entered into force on **5 October 2025**. The Government Decision establishes the regulatory framework for ensuring **cybersecurity** by providers of essential and important services in critical sectors. It partially transposes Commission Implementing Regulation (EU) 2024/2690, which implements the **NIS-2-Directive**, setting technical and methodological requirements for risk management and incident notification, and amends existing national legislation.

## Polish legal acts

### Act on the National Cybersecurity Certification System

- On **28 August 2025**, the [Act on the National Cybersecurity Certification System](#) came into force. The aim of the new regulations is to enhance the level of digital protection in Poland and enable the **issuance of European cybersecurity certificates** in the country, which will be automatically recognised by all EU Member States. The national cybersecurity certification system introduced by the Act is based on the **European Cybersecurity Act** and is intended to confirm that a given product or service meets specific security standards.

### Draft Act on the Crypto-Asset Market

- On **26 June 2025**, the Polish Parliament received a government-drafted Act on the crypto-assets market. The [proposed draft act](#) will transpose the EU's MiCA (Regulation (EU) 2023/1114) into national law. The draft act sets out, among other things, the conditions for the issuance and trading of crypto-assets, the regulatory framework for companies providing related services, as well as supervisory mechanisms for this sector. The draft Act can be found [here](#).

## Romanian legal acts

DNSC Order No. 1/2025 on the approval of the requirements for the notification/registration process under NIS2 Directive and Order No. 2/2025 on the approval of criteria and thresholds for determining the degree of disruption of a service and the methodology for assessing the risk level of entities under the NIS-2-Directive

- On **20 August 2025**, the following orders issued by the **National Directorate for Cyber Security (DNSC)** were adopted and published in the Romanian Official Gazette:
  - [Order No. 1/2025](#) on the requirements regarding the notification process for the registration of essential and important entities and the method of transmitting information (*Ordinul pentru aprobarea cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor*);
  - [Order No. 2/2025](#) on the criteria and thresholds for determining the degree of disruption of a service and the methodology for assessing the risk level of entities (*Ordinul pentru aprobarea criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și metodologia de evaluare a nivelului de risc al entităților*).
- Based on these acts, the obligation of DNSC notification for registration became effective. Essential and important entities were required to register with the DNSC within 30 days as of 20 August 2025 (respectively **until 22 September 2025**), via the [NIS2@RO Tool](#) available online (in Romanian and English).
- **Note:** Although the registration deadline has expired, essential and important entities under the NIS-2-Directive (as transposed by Romanian Government Emergency Ordinance No. 155/2025) are still obliged to notify the DNSC for registration. Failure to comply with this obligation constitutes a contravention and is punishable by fines of up to RON 500,000 (approx. EUR 100,000).

## Slovenian legal acts

### Media Act

- On **3 September 2025**, a **new Media Act** (*Zakon o medijih*; ZMed-1) was adopted ([Official Gazette of the Republic of Slovenia No. 69/2025](#)), introducing several fundamental improvements aimed at strengthening media transparency, digital development and journalistic protections. One of the key changes is the **requirement for greater transparency in media ownership and funding**, including mandatory disclosure of state advertising. The new Media Act also supports the digital transition by introducing **new financial schemes to assist in the digitalisation of print media** and to bolster the growth of digital media outlets. In response to the evolving media landscape, the new Media Act now **includes online platforms and influencers within its regulatory scope**, imposing higher legal and ethical responsibilities on them. Lastly, the new law aligns Slovenian media regulation with European standard, specifically the **European Media Freedom Act (EMFA)** and **Digital Services Act (DSA)**. It will enter into force on **27 September 2025**.

### Decision on establishing a list of categories of electronic communications and digital client devices intended for access to information society services or media

- On **4 September 2025**, the Government of the Republic of Slovenia adopted a "Decision on establishing a list of categories of electronic communications and digital client devices intended for access to information society services or media" (*Sklep o določitvi seznama kategorij elektronskih komunikacijskih in digitalnih odjemalnih naprav, ki so namenjene dostopu do storitev informacijske družbe ali medijev*) ([Official Gazette of the Republic of Slovenia No. 68/2025](#)). This decision outlines a **list of devices** that, pursuant to the Slovenian Act on the use of the Slovenian Language in Public, must make available the **Slovenian language** and **Slovenian orthography** to its users in such a way that the functionality of the device is equivalent to the functionality of the device in other available languages. The list of devices includes personal computers and laptops, electronic tablets and readers, smart mobile phones, smart TVs, connected cars and car parts (operating systems and graphical user interfaces), and interfaces for accessing IPTV (set-top boxes).

### DECISION on the application of ESMA Guidelines on supervisory practices of competent authorities for the prevention and detection of market abuse in accordance with the Markets in Crypto-Assets Regulation (MiCA)

- On **31 July 2025**, the **Slovenian Securities Market Agency** (*Agencija za trg vrednostnih papirjev*) adopted a Decision on the application of ESMA Guidelines on supervisory practices of competent authorities for the prevention and detection of market abuse in accordance with the Regulation on Markets in Crypto-Assets (MiCA) (*Sklep o uporabi Smernic ESMA o nadzornških praksah pristojnih organov za preprečevanje in odkrivanje zlorab trga v skladu z Uredbo o trgih kriptosredstev (MiCA)*), ([Official Gazette of the Republic of Slovenia No. 60/2025](#)). The Decision determines that the Agency will apply the ESMA guidelines when carrying out supervisory tasks under Articles 86 to 92 of the MiCA, with the aim of ensuring consistent and effective prevention, detection and enforcement against market abuse related to crypto-asset markets across the EU.

## Turkish legal acts

### Communiqué on the Implementation Procedures and Principles of the Technology Move Programme

- On 9 July 2025, the Ministry of Industry and Technology of the Republic of Türkiye issued a communiqué in the Official Gazette (No. 32951), amending the "[Technology-Oriented Industry Move Programme Implementing Procedures and Principles Communiqué](#)" (the "Communiqué"). The amendments, adopted under Presidential Decree No. 1 and Decision No. 9903, entered into force on the same date.

Among the notable revisions, the title of the original communiqué, previously published in the [Official Gazette dated 18 September 2019 \(No. 30892\)](#), has been changed from "Technology-Oriented Industry Move Programme Implementing Procedures and Principles Communiqué" (*Teknoloji Odaklı Sanayi Hamlesi Programı Uygulama Usul ve Esasları Tebliği*) to "Technology Move Programme Implementing Procedures and Principles Communiqué" (*Teknoloji Hamlesi Programı Uygulama Usul ve Esasları Tebliği*).

The revised Communiqué introduces several procedural and institutional changes to the incentive scheme designed to support investments in **medium-high** and **high-technology manufacturing sectors**. For applications to be considered for state support within the scope of [Presidential Decision No. 9903](#) and [Council of Ministers Decision No. 2016/9495](#), investors are required to submit the relevant forms and information, as set out under the applicable legislation, via the Programme Portal (*Program Portalı*). Upon submission, project evaluation committees assess the application files and provide a formal opinion to the Ministry regarding the project's eligibility for public support instruments.

### Technology Move Programme Implementing Procedures and Principles Communiqué

- The "Regulation on the Identification and Certification of Technology- and Innovation-Focused Enterprises" (*Teknoloji ve Yenilik Odaklı Girişimlerin Belirlenmesi ve Belgelendirilmesine Dair Yönetmelik*) (the "**Regulation**") was published in the [Official Gazette dated 3 July 2025](#), No. 32945, by the Ministry of Industry and Technology of the Republic of Türkiye, and entered into force on the same date.

The Regulation establishes the legal framework for identifying enterprises operating in Türkiye that engage in technology- and innovation-based activities and adopt scalable business models. Enterprises that meet the eligibility criteria may apply to receive the official **Tech-Entrepreneurship Badge (Teknogirişim Rozeti)**, which serves as a formal recognition of their innovative and scalable business structure. Eligibility requires, among other things, that the applicant be an SME (Small and Medium-sized Enterprise), have been established for no more than 15 years, and operate as an independent enterprise under Turkish law.

To better understand Türkiye's evolving digital legal framework, please see: <https://www.schoenherr.eu/content/turkiye-s-evolving-digital-legal-framework-regulatory-developments-in-innovation-and-data-protection>

# Digital Law Monitor. 4/2025

## **EU legal acts**

- **Regulations (incl. drafts)**

Regulation on the transparency and targeting of political advertising (TTPA)

Gigabit Infrastructure Act (GIA)

Digital Omnibus (AI and European Business Wallets)

Regulation on laying down additional procedural rules on the enforcement of the GDPR

- **Commission Guidelines**

Joint Guidelines on the Interplay between the DMA and the GDPR

- **European Council**

United Nations Convention against Cybercrime

- **European Data Protection Board**

Draft recommendations 2/2025 on e-commerce websites

- **Commission Delegated and Implementing Regulations (incl. drafts)**

Digital Services Act (DSA)

AI Act

Adequacy Decisions (UK)

Cyber Resilience Act (CRA)

Regulation on eCall systems

Markets in Crypto-Assets Regulation (MiCA)

eIDAS

TTPA

## **Bulgarian legal acts**

Law Amending and Supplementing the Electronic Communications Act

Law Amending and Supplementing the Competition Protection Act

Law Amending and Supplementing the Defence and Armed Forces of the Republic of Bulgaria Act

Instruction re processing personal data at the Ministry of Interior

Ordinance repealing Ordinance No. N-9 of 2020 re exchange of virtual assets

## **Croatian legal acts**

Act on the Implementation of the Data Governance Act

Act on Amendments to the Penal Code

Act on Control of Foreign Investments

Act on Amendments to the Act on Administrative Cooperation in Tax Matters

Act on Cross-Border Procurement of Electronic Evidence in Criminal Proceedings

Ordinance on Amendments to the Ordinance on Casino Online Games of Chance

Ordinance on Amendments to the Ordinance on Online Betting

Ordinance on Covert Surveillance of Crypto-Asset Service Providers

Ordinance on the Submission of Complaints against Offerers of Crypto-Assets

Decision on the Supervision Fee for Issuers of Asset-Referenced and Electronic Money Tokens

Ordinance on the Payment of Fees for the Activities Conducted by the Croatian Regulatory Authority for Network Industries

Ordinance on the Fiscalisation of Invoices Issued to End-Users

Ordinance on Prudential Requirements of Crypto-Asset Service Providers from Article 67 of Regulation (EU) 2023/1114

Ordinance on the Structure and Contents of Financial Statements of Crypto-Asset Service Providers

Ordinance on the Protection of Property of Clients using Crypto-Asset Services

Ordinance on the Scope of Revision of Crypto-Asset Service Providers

Ordinance on the Type and Amount of Fees levied by the Croatian Financial Services Supervisory Agency

Ordinance on the Calculation, Amount and Payment of Fees levied by the Croatian Financial Services Supervisory Agency in 2026

Ordinance on Amendments to the Ordinance on the Automatic Exchange of Information Relating to Taxes

## **Czech legal acts**

Cybersecurity Act

Decree on the Portal of the National Cyber and Information Security Agency

Decree on Regulated Services

Decree on Security Measures of Providers of Regulated Services under the Lower-Obligation Regime

Amendment to the Act on eHealth

### **Hungarian legal acts**

Act on the Hungarian implementation of the EU AI Act

Government Decree on the implementation of the Act on the Hungarian implementation of the EU AI Act

Amendment to the Act on Electronic Communications

NMHH Decree on the technical requirements of the civil alert system

Ministerial Decree on the specific rules governing the designation of bodies responsible for assessing compliance with the requirements applicable to high-risk AI systems

Act on the Hungarian implementation of the EU Cyber Resilience Regulation

### **Moldovan legal acts**

Government Decision on approval of Moldova's National Cybersecurity Programme

Government Decision on establishing the State Register of Cyber Incidents

Government Decision on the National Plan for response to cyber incidents and crises

Government Decision on coordinated disclosure of cybersecurity vulnerabilities

Government Decision on the regulatory framework in the field of cybersecurity by service providers in critical sectors

### **Polish legal acts**

Draft Act amending the Act on the Provision of Electronic Services and certain other acts

Draft Act amending the Act on the National Cybersecurity System and certain other acts

Draft regulation on telecommunications infrastructure necessary for defence, national security and public safety

Regulation on complaints concerning electronic communications services

### **Romanian legal acts**

National Directorate for Cybersecurity (DNSC) Order No. 3/2025 on the establishment of a framework for the cybersecurity of networks and information systems

Draft law on online majority age

### **Slovenian legal acts**

Act Amending and Supplementing the Financial Instruments Market Act

Act Amending and Supplementing the Investment Funds and Management Companies Act

Act Amending and Supplementing the Alternative Investment Fund Managers Act

Act Amending and Supplementing the General Administrative Procedure Act

Business Register Act

Act Amending and Supplementing the Electronic Identification and Trust Services Act

Act on the Implementation of the EU Regulation on Harmonised Rules for Artificial Intelligence

Exchange of Electronic Invoices and Other Electronic Documents Act

Exchange of Electronic Invoices and Other Electronic Documents Act

Act on the Digitalisation of Healthcare

Regulation on the training of responsible persons in the field of information and cybersecurity risk management

### **Turkish legal acts**

Draft Amendments on Artificial Intelligence Regulation in Türkiye

General Communiqué on the Tax Procedure Law

Amendments to the Presidential Decree on Cybersecurity

### **Austrian legal acts**

Critical Entities Resilience Act

Federal Act amending the SNG, SPG, TKG, BVwGG und RStDG (Federal Troja)

Criminal Law EU Adjustment Act 2025

Amendments to the Health Telematics Act

Network and Information Systems Security Act 2026 (NIS Act 2026)

Second EU Information Systems Adjustment Act

Second Transparency Database Query Ordinance 2025

## EU legal acts

### Regulations

#### Regulation on the transparency and targeting of political advertising (TTPA)

- On **10 October 2025**, "[Regulation \(EU\) 2024/900](#) of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising" became **applicable** in the Member States. Its objective is to ensure a uniform and high level of transparency in political advertising services across the EU. At the same time, it aims to counteract targeted manipulation of information and undue influence through political advertising. Political advertisements must be clearly identifiable as such.

#### Gigabit Infrastructure Act (GIA)

- On **12 November 2025**, the Gigabit Infrastructure Act (**GIA**, [Regulation \(EU\) 2024/1309](#)) became **applicable** in the Member States. It lays down rules on permit-granting procedures for the deployment of **fibre telecommunication networks**. For further information see [here](#).

#### Draft Regulations – Digital Omnibus, Digital Omnibus on AI and European Business Wallets

- On **19 November 2025**, the **European Commission** published proposals for (i) a "**Digital Omnibus**", [COM\(2025\) 837 final](#), (ii) a "**Digital Omnibus on AI**", [COM\(2025\) 836 final](#), and (iii) the establishment of "**European Business Wallets**", [COM\(2025\) 838 final](#). Among other things, the draft regulations are intended to simplify compliance with the **GDPR**, the **AI Act** and the **Data Act**. For further information see [here](#).

#### GDPR Procedural Regulation

- On **12 December 2025**, "[Regulation \(EU\) 2025/2518](#) of the European Parliament and of the Council of 26 November 2025 laying down additional procedural rules on the enforcement of Regulation (EU) 2016/679", [OJ L 2025/2518](#), was published. This Regulation lays down procedural rules for the conduct of investigations in **cross-border cases**. For further information see [here](#).

### Commission Guidelines

#### EDPB/Commission – Joint Guidelines on the Interplay between the DMA and the GDPR

On **9 October 2025**, the European Data Protection Board (EDPB) and the European Commission published a draft of [Joint Guidelines](#) on the **Interplay between the DMA and the GDPR**. The guidelines specifically address the processing of personal data of data subjects by gatekeepers within the meaning of the Digital Markets Act (DMA). The so-called "Pay or Consent" Model is considered arguably inapplicable where gatekeepers seek to rely on it. The guidelines also specify details on data portability as well as effective, continuous and real-time access to data generated by end users. Moreover, the responsibility for obtaining the end user's consent to access data by business users is clarified, and details on coordinated enforcement and consistent application by competent authorities are addressed.

### European Council

#### United Nations Convention against Cybercrime

- On **11 November 2025**, "[Council Decision \(EU\) 2025/2307](#) of 13 October 2025 on the **signing**, on behalf of the European Union, of the **United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes**", [OJ L 2025/2307](#), was published. The [United Nations Convention against Cybercrime](#) is intended to strengthen the fight against cybercrime and international cooperation in this field.

### European Data Protection Board

#### Draft recommendations 2/2025 on e-commerce websites

- On **3 December 2025**, the **EDPB** adopted the draft "[Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites](#)". The EDPB recommends allowing the use of e-commerce websites as a "**guest**".

### Commission Delegated and Implementing Regulations (incl. drafts)



## AI Act

- On **2 December 2025**, the draft "Commission Implementing Regulation (EU) laying down rules for the application of Regulation (EU) 2024/1689 of the European Parliament and of the Council as regards the establishment, development, implementation, operation and supervision of **AI regulatory sandboxes**", [Ares\(2025\)10569703](#), was published. This Implementing Regulation further specifies the use of **AI regulatory sandboxes** within the meaning of the [AI Act](#).

## Digital Services Act (DSA)

- On **9 October 2025**, "Commission Delegated Regulation (EU) 2025/2050 of 1 July 2025 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data with vetted **researchers**", [OJ L 2025/2050](#), was published. Pursuant to Art. 40(4) of Regulation (EU) 2022/2065 ([DSA](#)), providers of **very large online platforms** and of **very large online search engines** must provide **access to data** upon a reasoned request by the **Digital Services Coordinator** for the performance of **research** that contributes to the detection, identification and understanding of systemic risks. The Delegated Regulation lays down the procedure and technical conditions for granting access through a **data access portal**. The Commission is designated as the **data processor** of the DSA data access portal.

## Adequacy Decisions

- On **23 December 2025**, (i) "Commission Implementing Decision (EU) 2025/2571 of 19 December 2025 amending Commission Implementing Decision (EU) 2021/1773 pursuant to Directive (EU) **2016/680** of the European Parliament and of the Council on the **adequate protection of personal data** by the **United Kingdom**", [OJ L 2025/2571](#), and (ii) "Commission Implementing Decision (EU) 2025/2574 of 19 December 2025 amending Commission Implementing Decision (EU) 2021/1772 pursuant to Regulation (EU) **2016/679** of the European Parliament and of the Council on the **adequate protection of personal data** by the **United Kingdom**", [OJ L 2025/2574](#), were published. These Commission Implementing Decisions extend the validity of the adequacy decisions applicable to the **United Kingdom** from 27 December 2025 until **27 December 2031**.

## Cyber Resilience Act (CRA)

- On **16 October 2025**, the **draft** "Commission Delegated Regulation supplementing Regulation (EU) 2024/2847 of the European Parliament and of the Council by specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications", [Ares\(2025\)8809980](#), was published. This Delegated Regulation specifies **Cyber Resilience Act 2024/2847 (CRA)** by setting out the conditions under which the national Computer Security Incident Response Team (CSIRT) may, under exceptional circumstances, delay the dissemination of a security notification.

## Regulation (EU) 2015/758 (eCall systems)

- On **28 October 2025**, "Commission Delegated Regulation (EU) 2025/1871 of 23 July 2025 amending Regulation (EU) 2015/758 of the European Parliament and of the Council as regards the standards relating to **eCall** and amending Delegated Regulation (EU) 2017/79 as regards the technical requirements and test procedures for approval of motor vehicles equipped with **112-based eCall in-vehicle systems**", [OJ L 2025/1871](#), was published. This Delegated Regulation lays down **test procedures** concerning **eCall systems** within the meaning of [Regulation \(EU\) 2015/758](#) for new **types of vehicles**.

## Markets in Crypto-Assets Regulation (MiCAR)

- On **3 October 2025**, "Commission Delegated Regulation (EU) 2025/1264 of 27 June 2025 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the minimum contents of the liquidity management policy and procedures for certain issuers of asset-referenced tokens and e-money tokens", [OJ L 2025/1264](#), was published. This Delegated Regulation specifies the minimum contents of the **liquidity management** policy and procedures for certain issuers of **asset-referenced tokens** or **e-money tokens**.

## eIDAS

- On **30 September 2025**, (i) "Commission Implementing Regulation (EU) 2025/1942 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards **qualified validation services** for qualified electronic signatures and qualified validation services for qualified electronic seals", [OJ L 2025/1942](#), (ii) "Commission Implementing Regulation (EU) 2025/1943 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for **qualified certificates** for electronic signatures and qualified certificates for electronic seals", [OJ L 2025/1943](#), (iii) "Commission Implementing Regulation (EU) 2025/1944 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for processes for sending and receiving data in **qualified electronic registered delivery services** and as regards interoperability of those services", [OJ L 2025/1944](#), (iv) "Commission Implementing Regulation (EU) 2025/1945 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the **validation** of qualified electronic signatures and of qualified electronic seals and the validation of advanced electronic signatures based on qualified certificates and of advanced electronic seals based on qualified certificates", [OJ L 2025/1945](#), and (v) "Commission Implementing Regulation (EU) 2025/1946 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards **qualified preservation services** for qualified electronic signatures and for qualified electronic seals", [OJ L 2025/1946](#), were published. These **five Implementing Regulations** lay down **reference standards and specifications** under the [eIDAS](#).
- On **28 October 2025**, "Commission Implementing Regulation (EU) 2025/2160 of 27 October 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards **reference standards, specifications and procedures** for the management of risks to the provision of non-qualified trust services", [OJ L 2025/2160](#), and "Commission Implementing Regulation (EU) 2025/2162 of 27 October 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the **accreditation of conformity assessment bodies** evaluating qualified trust service providers and the qualified trust services they provide, the conformity assessment report and the conformity assessment system", [OJ L 2025/2162](#), were published. **These two Implementing Regulations** establish **reference standards and specifications**, as well as the **accreditation of conformity assessment bodies** under the [eIDAS](#).
- On **2 December 2025**, the draft "Commission Implementing Regulation (EU) laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards onboarding of users to the **European Digital Identity Wallets** by electronic identification means conforming to assurance level high or by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures where the combination meets the requirements of assurance level high", [Ares\(2025\)10575642](#), was published. This Implementing Regulation lays down reference standards for onboarding users to the European Digital Identity Wallet within the meaning of [eIDAS](#).
- On **17 December 2025**, (i) "Commission Implementing Regulation (EU) 2025/2527 of 16 December 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards **reference standards** for qualified certificates for **website authentication**", [OJ L 2025/2527](#), (ii) "Commission Implementing Regulation (EU) 2025/2530 of 16 December 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards requirements for **qualified trust service providers** providing qualified trust services", [OJ L 2025/2530](#), (iii) "Commission Implementing Regulation (EU) 2025/2531 of 16 December 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards **reference standards and specifications** for qualified **electronic ledgers**", [OJ L 2025/2531](#), and (iv) "Commission Implementing Regulation (EU) 2025/2532 of 16 December 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards **reference standards and specifications** for qualified **electronic archiving services**", [OJ L 2025/2532](#), were published. With these **four implementing regulations, reference standards and specifications**, as well as requirements for **qualified trust service providers**, are laid down under the [eIDAS](#).

## TTPA

- On **23 December 2025**, the **draft** "Commission Implementing Regulation (EU) ... setting out detailed arrangements for the provision of a common data structure, standardised metadata, standardised authentication and common application programming interface for the European

repository for online political advertisements in accordance with Regulation (EU) 2024/900 of the European Parliament and of the Council", [Ares\(2025\)11556145](#), was published. This Commission Implementing Regulation lays down standards to facilitate the inclusion of **political advertisements** within the meaning of the [TTPA \(EU\) 2024/900](#) in the **European repository**.

## Bulgarian legal acts

### Law Amending and Supplementing the Competition Protection Act

- By the Transitional and Final Provisions of the Law Amending and Supplementing the Competition Protection Act, published in the [State Gazette No. 95/2025](#) on **7 November 2025**, the Electronic Communications Act was amended to allow, where necessary, **the Commission on Protection of Competition (CPC) to obtain**, as provided by law, **data from undertakings providing public electronic communications networks and/or services** for the needs and purposes of proceedings under the Competition Protection Act.

### Law Amending and Supplementing the Electronic Communications Act

- **On 21 November 2025**, the Law Amending and Supplementing the Electronic Communications Act was published in the [State Gazette No. 99/2025](#). The adopted amendments ensure the application of the [Digital Services Act \(DSA\)](#). The amendments lay down the functions and powers of the national authorities, their competence to supervise providers of intermediary services for compliance with the DSA and introduce mechanisms for imposing the penalties and fines specified in the Regulation. Other amendments expressly **grant consumers the right**, without penalty, **to terminate their contract** for a publicly available electronic communications service, other than a number-independent interpersonal communications service, before the end of the agreed term **due to an imposed price increase** (price indexation).

### Law Amending and Supplementing the Defence and Armed Forces of the Republic of Bulgaria Act

- By the Transitional and Final Provisions of the Law Amending and Supplementing the Defence and Armed Forces of the Republic of Bulgaria Act, published in the [State Gazette No. 100/2025](#) on **25 November 2025**, Article 301, paragraph 3 of the Electronic Communications Act was supplemented to provide that **the Bulgarian Armed Forces may, by technical means, block the use of electronic communications services** when this is done for the purposes of using technical means for detecting and neutralising **unmanned systems** in the protection of military sites and garrison areas, as well as military units, equipment and military vessels located outside garrison areas, on the basis of procedures and rules approved by the Minister of Defence that take into account the use of such technical means.

### Instruction amending Instruction No. 81213-1280 of 7 October 2021 on the procedure for processing personal data at the Ministry of Interior

- The instruction amending Instruction No. 81213-1280 of 7 October 2021 on the procedure for processing personal data at the Ministry of Interior was published in the [State Gazette No. 114/2025](#) on **24 December 2025**. According to the amendment, when the Ministry of Interior processes personal data and where the time limits or circumstances for the erasure of personal data, or for the periodic review of the need for their retention, are not laid down in a normative act or by an order of the Minister of Interior, the retention period shall be **50 years** from the commencement of processing, and the period for periodic review shall be five years.

### Ordinance repealing Ordinance No. N-9 of 2020 on the terms and procedure for registration in the register of persons who, by way of business, provide services for exchange between virtual currencies and recognised currencies without gold backing, services for the transfer or exchange of virtual assets, services for the custody and management of virtual assets enabling control over such assets, and services related to the public offering of virtual assets, as well as of wallet providers offering custodial services

- The repealing Ordinance was published in the [State Gazette No. 114/2025](#) on 24 December 2025, and **the repeal of the said Ordinance has entered into force as of 28 December 2025**.

## Croatian legal acts

### Act on the Implementation of Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)

- The Act on the Implementation of Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (**Data Governance Act**), published in the Official Gazette No. 126/2025, entered into force on **11 October 2025**. The Act designates the national bodies competent for the implementation of the Data Governance Act, the procedure for the re-use of protected data, registration of data intermediation service providers and data altruism organisations, the competent national regulatory entities and the procedure and sanctions for breaches.

### Act on Amendments to the Penal Code

- The Act on Amendments to the Penal Code, published in the Official Gazette No. 136/2025, entered into force on **13 November 2025**. A new criminal offence was introduced which penalises the endangerment of life and property by means of an **artificial intelligence (AI) system**, with potential penalties reaching up to 15 years in prison.

### Act on Control of Foreign Investments

- The Act on Control of Foreign Investments, published in the Official Gazette No. 136/2025, entered into force on **13 November 2025**. The Act introduces **a prior and ex post facto control of foreign investments** in sectors potentially influencing national security and public order concerns, including in the digital sector. The exact affected sectors and the criteria for identifying individual obliged entities are yet to be defined by a separate Government regulation. For further information see [here](#).

### Act on Amendments to the Act on Administrative Cooperation in Tax Matters

- The Act on Amendments to the Act on Administrative Cooperation in Tax Matters, published in the Official Gazette No. 146/2025, entered into force on **11 December 2025**. The amendments regulate various obligations imposed on **crypto-asset service providers**, such as data-gathering, notification to tax authorities and deep screening of clients.

### Act on Cross-Border Procurement of Electronic Evidence in Criminal Proceedings

- The Act on Cross-Border Procurement of Electronic Evidence in Criminal Proceedings, published in the Official Gazette No. 151/2025, will enter into force on **18 February 2026**, with certain provisions entering into force only on **18 August 2026**. The Act implements Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for **electronic evidence in criminal proceedings** and for the execution of custodial sentences following criminal proceedings in the Croatian legal framework by designating the competent national bodies for the issuing of European production orders and European preservation orders.

### Ordinance on Amendments to the Ordinance on Casino Online Games of Chance accessed through Interactive Online Playing Sales Channels

- The Amendments to the Ordinance on Online Gambling in Casinos by means of Interactive Online Playing Sales Channels, published in the Official Gazette No. 129/2025, entered into force on **16 October 2025**. The amendments introduce more stringent criteria for **online identity verification and player exclusions** for online players.

### Ordinance on Amendments to the Ordinance on Online Betting

- The Amendments to the Ordinance on Online Betting, published in the Official Gazette No. 129/2025, entered into force on **16 October 2025**. The amendments introduce more stringent criteria for **online identity verification and player exclusions** for online bettors.

### Ordinance on Covert Surveillance of Crypto-Asset Service Providers

- The Ordinance on Covert Surveillance of Crypto-Asset Service Providers, adopted by the Croatian Financial Services Supervisory Agency (**HANFA**) and published in the Official Gazette No. 129/2025, entered into force on **23 October 2025**. The Ordinance contains procedural rules governing **mystery shopping with respect to crypto-asset service providers**.

Ordinance on the Submission of Complaints against Offerers or Persons Seeking Admissions to Trading of Crypto-Assets not considered Asset-Referenced Crypto-Assets or Electronic Money Tokens and Crypto-Asset Service Providers and the Complaint-Handling Procedure of the Croatian Financial Services Supervisory Agency

- The Ordinance on the Submission of Complaints to Offerers or Persons Seeking Admissions to Trading of Crypto-Assets not considered Asset-Referenced Crypto-Assets or Electronic Money Tokens and Crypto-Asset Service Providers and the Complaint-Handling Procedure of the Croatian Financial Services Supervisory Agency, adopted by HANFA and published in the Official Gazette No. 129/2025, entered into force on **23 October 2025**. The Ordinance regulates the form and content of **complaints against offerors, persons seeking admission to trading of crypto-assets and crypto-asset service providers**, as well as HANFA's procedure for handling submitted complaints.

Decision on the Supervision Fee for Issuers of Asset-Referenced and Electronic Money Tokens

- The Decision on the Supervision Fee for Issuers of Asset-Referenced and Electronic Money Tokens, adopted by the Croatian National Bank (**HNB**) and published in the Official Gazette No. 139/2025, entered into force on **20 November 2025**. The Decision sets the **fees payable by issuers of asset-referenced and electronic money tokens** for the regulatory supervision performed by the HNB.

Ordinance on the Payment of Fees for the Activities Conducted by the Croatian Regulatory Authority for Network Industries

- The Ordinance on the Payment of Fees for the Activities Conducted by the Croatian Regulatory Authority for Network Industries, adopted by the Croatian Regulatory Authority for Network Industries ("**HAKOM**") and published in the Official Gazette No. 154/2025, entered into force on **1 January 2026**. The Ordinance sets the **fees payable by electronic communications operators** used to fund the activities of HAKOM. These include the address and numbering space management fee, the radiofrequency spectrum management fee, and the fee for other activities in the field of electronic communications.

Ordinance on the Fiscalisation of Invoices Issued to End-Users

- The Ordinance on the Fiscalisation of Invoices Issued to End-Users, published in the Official Gazette No. 153/2025, entered into force on **1 January 2026**. The Ordinance contains detailed technical provisions on the implementation of **mandatory fiscalisation of all end-user invoices**.

Ordinance on Prudential Requirements of Crypto-Asset Service Providers from Article 67 of Regulation (EU) 2023/1114

- The Ordinance on Prudential Requirements of Crypto-Asset Service Providers from Article 67 of Regulation (EU) 2023/1114, published in the Official Gazette No. 153/2025, entered into force on **1 January 2026**. The Ordinance regulates the contents, form and statutory deadlines for submitting **reports on satisfaction of prudential requirements set by the MiCAR**.

Ordinance on the Structure and Contents of Financial Statements of Crypto-Asset Service Providers

- The Ordinance on the Structure and Contents of Financial Statements of Crypto-Asset Service Providers, published in the Official Gazette No. 153/2025, entered into force on 1 January 2026. The Ordinance regulates the **structure, contents and statutory deadlines for submitting financial statements of crypto-asset service providers** to HANFA.

Ordinance on the Protection of Property of Clients using Crypto-Asset Services

- The Ordinance on the Protection of Property of Clients using Crypto-Asset Services, published in the Official Gazette No. 157/2025, entered into force on 1 January 2026. The Ordinance imposes various **regulatory obligations on crypto-asset services providers** connected with the protection of property of their clients' crypto assets.

#### Ordinance on the Scope of Revision of Crypto-Asset Service Providers

- The Ordinance on the Scope of Revision of Crypto-Asset Service Providers, published in the Official Gazette No. 157/2025, entered into force on **1 January 2026**. The Ordinance regulates the **scope of the financial revision of crypto-asset service providers**, as well as the **grounds for rejection of the revised annual financial statements and revised reports on satisfaction of prudential requirement**.

#### Ordinance on the Type and Amount of Fees levied by the Croatian Financial Services Supervisory Agency

- The Ordinance on the Type and Amount of Fees levied by HANFA, published in the Official Gazette No. 157/2025, entered into force on **1 January 2026**. The Ordinance defines the corresponding amounts of various **fees levied by HANFA for regulatory services provided in the field of crypto-assets**.

#### Ordinance on the Calculation, Amount and Payment of Fees levied by the Croatian Financial Services Supervisory Agency in 2026

- The Ordinance on the Calculation, Amount and Payment of Fees levied by the Croatian Financial Services Supervisory Agency in 2026, published in the Official Gazette No. 157/2025, entered into force on **1 January 2026**. The Ordinance defines various **annual fees levied by HANFA for regulatory services provided in the field of crypto-assets**.

#### Ordinance on Amendments to the Ordinance on the Automatic Exchange of Information Relating to Taxes

- The Ordinance on Amendments to the Ordinance on the **Automatic Exchange of Information Relating to Taxes**, published in the Official Gazette No. 158/2025, entered into force on **1 January 2026**. The amendments contain detailed provisions on the implementation of legislative changes introduced by the amended Act on Administrative Cooperation in Tax Matters (see above).

## Czech legal acts

### Cybersecurity Act

- The **Cybersecurity Act**, published in the [Official Gazette No. 264/2025](#), entered into force on **1 November 2025**. The Act transposes the **NIS2 Directive** and introduces broad duties for regulated entities, which have 60 days to complete their registration with the National Cyber and Information Security Agency (NÚKIB). The number of regulated entities is expected to increase up to tenfold compared to the current regulation.

### Decree on the Portal of the National Cyber and Information Security Agency

- The Decree on the Portal of the National Cyber and Information Security Agency, published in the [Official Gazette No. 334/2025](#), entered into force on **1 November 2025**. This Decree regulates the operation of the **online portal of the NÚKIB** and sets out technical and procedural requirements for selected electronic acts carried out via the portal, incl. identification, authentication, submission of data, and communication with NÚKIB. The Decree supports the digitalisation of cybersecurity supervision and standardises how regulated entities fulfil certain statutory obligations electronically.

### Decree on Regulated Services

- The Decree on Regulated Services was published in the [Official Gazette No. 408/2025](#) on **14 October 2025**. This new Decree, effective as of **1 November 2025**, implements and elaborates provisions of the new Cybersecurity Act (Act No. 264/2025 Coll.) by defining the **list of "regulated services"**, the criteria for determining when a service provider is significant, and the classification of service providers into regulatory regimes (higher vs. lower obligations). It sets out how providers should assess whether they fall within the scope of the Act's obligations and clarifies which regulatory regime applies to them under the Czech cybersecurity framework aligned with the NIS2 Directive.

### Decree on Security Measures of Providers of Regulated Services under the Lower-Obligation Regime

- The Decree on Security Measures of Providers of Regulated Services under the Lower-Obligation Regime was published in the [Official Gazette No. 410/2025](#) on **14 October 2025**. This Decree, effective as of **1 November 2025**, specifies a proportionate set of baseline technical and organisational cybersecurity measures for providers subject to a reduced regulatory regime, focusing on risk management, incident handling and basic protection of information systems. The Decree aims to ensure an **adequate level of cybersecurity** while limiting the administrative burden for smaller or lower risk regulated service providers under the supervision of the NÚKIB.

### Amendment to the Act on eHealth

- The Amendment to the Act on eHealth, published in the [Official Gazette No. 236/2025](#), entered into force on **1 January 2026**. The amendment updates the **eHealth framework**, including electronic documentation, interoperability and data sharing.



## Hungarian legal acts

### Act on the Hungarian implementation of the EU AI Act

- On **31 October 2025**, Act LXXV of 2025 on the implementation in Hungary of the European Union's Regulation on **Artificial Intelligence Act** was published in the [Hungarian Gazette No. 2025/127](#). The Act establishes the national framework for implementing the EU AI Act in Hungary, including defining the core competences and procedural rules of the national **AI notifying authority** and the **AI market surveillance authority**, and establishing the **Hungarian Artificial Intelligence Council** to promote the uniform application of the law. The Act aims to ensure fundamental rights-respecting use of AI, promote consistent enforcement through the issuance of guidance, and support the development of a national AI strategy and cooperative domestic AI ecosystem.

### Government Decree on the implementation of the Act on the Hungarian implementation of the EU AI Act

- On **31 October 2025**, Government Decree No. 344/2025. (X. 31.) on the implementation of Act LXXV of 2025 on the implementation in Hungary of the European Union's Regulation on **Artificial Intelligence** was published in the [Hungarian Gazette No. 2025/127](#). The Decree lays down detailed procedural rules and designates the bodies responsible for carrying out the tasks of the **AI notifying authority** and the **AI market surveillance authority**.

### Amendment to the Act on Electronic Communications

- On **28 November 2025**, Act LXXXVII of 2025 on the amendment of Act C of 2023 on **Electronic Communications** was published in the [Hungarian Gazette No. 2025/142](#). The new provisions support the implementation of EU and national objectives aimed at ensuring that all households have access to **gigabit-capable internet connections** by 2030. The amendment sets out detailed rules within the competence of EU Member States, including the introduction of additional **exemptions from licensing procedures**.

### NMHH Decree on the technical requirements of the civil alert system for defence and security purposes

- On **10 December 2025**, Decree No. 11/2025. (XII. 10.) of the President of the National Media and Infocommunications Authority (NMHH) on the technical requirements of the **civil alert system for defence and security purposes** was published in the [Hungarian Gazette No. 2025/151](#). The Decree establishes the technical requirements that enable the near-simultaneous transmission of alert messages to devices located within a designated alert area using **mobile radio-telephone technology**.

### Ministerial Decree on the specific rules governing the designation of bodies responsible for assessing compliance with the requirements applicable to high-risk AI systems, the activities of such designated bodies, and the administrative service fees payable for the designation procedure

- On **23 December 2025**, Decree No. 44/2025. (XII. 23.) of the Minister for National Economy on the specific rules governing the designation of bodies responsible for assessing compliance with the requirements applicable to **high-risk AI systems**, the activities of such designated bodies, and the administrative service fees payable for the designation procedure was published in the [Hungarian Gazette No. 2025/157](#). The Decree aims to establish detailed rules concerning the designation of organisations **certifying the preliminary technical compliance** of high-risk AI systems. It sets out specific procedural provisions, including requirements related to **liability insurance** and the **administrative service fees** applicable to the designation process.

### Act on the Hungarian implementation of the EU Cyber Resilience Regulation and the amendment of certain cybersecurity provisions

- On **29 December 2025**, Act CXXXV of 2025 on the implementation in Hungary of the European Union's Regulation on **Cyber Resilience** and amendment of certain cybersecurity provisions was published in the [Hungarian Gazette No. 2025/158](#). The Act establishes the domestic legal framework for implementing Regulation (EU) 2024/2847 and clarifies certain cybersecurity provisions. Notably, it amends the **scope of the Hungarian Cybersecurity Act**.

## Moldovan legal acts

### Government Decision on approval of Moldova's National Cybersecurity Programme for 2026–2030

- On **29 December 2025**, Government Decision No. 821 on approval of **Moldova's National Cybersecurity Programme** for 2026–2030 was published in the [Official Gazette No. 656-658](#) dated 31 December 2025. The programme responds to threats and capability gaps, setting strategic objectives and practical measures to achieve and maintain a high level of network and information system security, and to strengthen national capacity for prevention, detection, response and recovery in the face of cyber incidents.

### Government Decision on establishing the State Register of Cyber Incidents

- On **29 December 2025**, Government Decision No. 822 on establishing the **State Register of Cyber Incidents** was published in the [Official Gazette No. 646-650](#) dated 30 December 2025. The decision approves both the concept and the regulation on how the State Register of Cyber Incidents is to be maintained, designating the Cybersecurity Agency to create, implement, operate and develop the system.

### Government Decision on approval of the Regulation governing the development, updating and implementation of the National Plan for response to cyber incidents and crises

- On **29 December 2025**, Government Decision No. 823 on approval of the Regulation governing the development, updating and implementation of the **National Plan for response to cyber incidents and crises** was published in the [Official Gazette No. 656-658](#) dated 31 December 2025. The Regulation sets principles (legality, coordination/cooperation, responsibility), mandates alignment with the National Crisis Management Plan, and assigns roles and responsibilities at strategic, operational and tactical levels for unified and timely responses.

### Government Decision on approval of the Regulation on coordinated disclosure of cybersecurity vulnerabilities

- On **29 December 2025**, Government Decision No. 824 on approval of the Regulation on coordinated disclosure of **cybersecurity vulnerabilities** was published in the [Official Gazette No. 646-650](#) dated 30 December 2025. The Regulation establishes the substantive and procedural legal framework for the notification, assessment, remediation and coordinated disclosure of vulnerabilities in information and communications technology products and services to improve cybersecurity.

### Government Decision on approval of the Regulation on state supervision and control over compliance with the regulatory framework in the field of cybersecurity by service providers in critical sectors

- On **29 December 2025**, Government Decision No. 825 on approval of the Regulation on state supervision and control over compliance with the regulatory framework in the field of **cybersecurity by service providers in critical sectors** was published in the [Official Gazette No. 656-658](#) dated 31 December 2025. The Regulation establishes the legal, organisational and procedural framework for the exercise by the **Cybersecurity Agency** of the function of state supervision and control of the way service providers in critical sectors ensure compliance with the provisions of the regulatory framework in the field of cybersecurity.

## Polish legal acts

### Draft Act amending the Act on the Provision of Electronic Services and certain other acts

- The draft act concerns the adjustment of Polish regulations to Regulation (EU) 2022/2065 of the European Parliament and of the Council on the Digital Single Market (**Digital Services Act**). This will create a modern system in Poland for effectively combating illegal content and disinformation, which will protect online users and ensure transparent operating rules for internet platforms. On **19 December 2025**, the Polish Parliament completed work on the draft act and submitted it to the Polish president for signature. On **9 January 2026**, the Polish president did not sign the bill and exercised his veto, arguing that some of the solutions presented in the draft act are harmful to ordinary citizens. As a result, the draft act returned to the parliament for amendments to the provisions indicated by the president.

### Draft Act amending the Act on the National Cybersecurity System and certain other acts

- The Draft Act amending the Act on the National Cybersecurity System and certain other acts was submitted to the Polish Parliament on **7 November 2025**, and the first reading of the bill took place on **5 December 2025**. The draft act concerns the implementation of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (**NIS2 Directive**) (OJ EU L 333 of 27 December 2022, p. 80). The new provisions provide, among other things, for the extension of the list of entities covered by the national cybersecurity system to include new sectors of the economy (wastewater, ICT management, space, postal services, manufacturing, chemical production and distribution, food production and distribution), the purchase of equipment and modernisation of infrastructure, the creation of cybersecurity incident response teams, increased responsibility for persons managing enterprises and institutions covered by the national cybersecurity system, and the introduction of mandatory reporting of network incidents.

### Draft regulation of the Minister of Digital Affairs on the scope of data on telecommunications infrastructure necessary for the preparation of communications systems for the purposes of defence, national security and public safety and order

- On **14 October 2025**, the Minister of Digital Affairs presented the draft regulation to the Polish government. The draft regulation covers issues related to **data on telecommunications infrastructure** for the preparation of **communications systems for defence and security purposes**. Until now, these issues have been regulated by a document issued by the Minister of Infrastructure 15 years ago, and the changes were prompted by the Electronic Communications Law passed in 2024. The President of the Office of Electronic Communications will continue to be responsible for obtaining data from telecommunications operators. Until now, he has requested entities to provide the required information within 30 days. The new regulation reverses this situation: now operators will have until 31 March to submit data on infrastructure as at the end of the previous year. One of the most important points of the draft are the provisions including the Minister of National Defence and the minister responsible for internal affairs among the entities involved. The President of the Office of Electronic Communications will make the collected data available to them for the purpose of planning activities related to security, public order and defence.

### Regulation of the Minister of Digital Affairs of 29 September 2025 on complaints concerning electronic communications services or optional account charging services

- On **14 March 2026**, a new regulation of the Minister of Digital Affairs **on complaints about electronic communications services** will come into force. The Regulation will enter into force in connection with the implementation of Article 378(7) of the Electronic Communications Law, pursuant to which the Minister of Digital Affairs will specify, by way of a regulation, the detailed complaint procedure and the elements that should be included in a response to a complaint about an electronic communications service or an optional billing service, taking into account the necessary protection of the end user's interests, the maximum simplification of the complaint procedure and ensuring its transparency.

## Romanian legal acts

DNSC Order No. 3/2025 approving the Norms for supervision, verification and control of compliance with Government Emergency Ordinance No. 155/2024 on the establishment of a framework for the cybersecurity of networks and information systems in the national civil cyberspace and the Methodology for risk-based prioritisation of supervision, verification and control activities ("Order 3/2025")

- On **11 December 2025**, [Order 3/2025](#) issued by the National Directorate for Cybersecurity (DNSC) was published in the Romanian Official Gazette and entered into force, thereby approving two legal acts:
  - the **Norms** for supervision, verification and control of compliance with Government Emergency Ordinance No. 155/2024 on the establishment of a framework for the cybersecurity of networks and information systems in the national civil cyberspace. The norms establish the procedural framework for oversight, verification and control of compliance with Romania's cybersecurity regime under Government Emergency Ordinance (GEO) 155/2024, which transposed the NIS2 Directive at the national level. They define the roles and powers of the DNSC, including the authority to request documents and data, perform non-intrusive proactive scans, order ad-hoc cyber audits, access premises and systems during controls, and coordinate with sectoral authorities.
  - the **Methodology** for risk-based prioritisation of supervision, verification and control activities. The methodology complements the above-mentioned norms by setting out how the DNSC ranks entities for supervision and control activities based on cybersecurity risk, in order to allocate oversight resources proportionately and efficiently.

### Draft law on online majority

- The [draft law on online majority age](#) was approved by the Romanian Senate on **6 October 2025**. The draft law aims to protect minors from harmful online content and sets an "online majority" at age 16. Until said majority age, minors may access online services or create accounts only with verifiable parental consent. If adopted, the law would apply broadly to online services, including social media, streaming, e-commerce, gaming, banking and mobile apps, but would not apply to online learning platforms authorised at the national level by the Ministry of Education and Research or at the European level by the competent authorities. The status of the adoption process may be tracked [here](#).

## Slovenian legal acts

### Act Amending and Supplementing the Financial Instruments Market Act

- The Act Amending and Supplementing the Financial Instruments Market Act was adopted on **25 September 2025** and entered into force on 22 October 2025. The amendment aligns Slovenian financial markets law with EU digital regulation by implementing **DORA** and strengthening **ICT security, digital operational resilience** and **algorithmic trading controls** for investment firms and regulated markets. It also introduces new digital reporting and machine-readable disclosure obligations in support of the European Single Access Point (ESAP), enhancing transparency and data accessibility across the EU.

### Act Amending and Supplementing the Investment Funds and Management Companies Act

- The Act Amending and Supplementing the Investment Funds and Management Companies Act was adopted on **25 September 2025** and entered into force on 22 October 2025. The amendment aligns Slovenian fund management legislation with the EU digital regulation by transposing Directive (EU) 2022/2556 and applying **DORA** requirements to **management companies' ICT systems**. It establishes a unified framework for ICT risk management, cybersecurity and digital operational resilience in the asset management sector.

### Act Amending and Supplementing the Alternative Investment Fund Managers Act

- The Act Amending and Supplementing the Alternative Investment Fund Managers Act was adopted on **25 September 2025** and entered into force on 22 October 2025. The amendment aligns Slovenian law on alternative investment fund managers with the EU digital regulation by transposing Directive (EU) 2022/2556 and applying **DORA** requirements to their **ICT systems**. It establishes a unified framework for ICT risk management, cybersecurity and digital operational resilience in the asset management sector.

### Act Amending and Supplementing the General Administrative Procedure Act

- The Act Amending and Supplementing the General Administrative Procedure Act was adopted on **23 October 2025** and will enter into force on 6 February 2026. The amendment mandates, among other things, **electronic service of documents** for all business entities, public institutions and professionals, using secure electronic mailboxes provided by the Ministry of Digital Transformation or official registers. It also introduces shorter service fiction periods, prolongs deadlines for appeals, and modernises electronic and physical document delivery to improve efficiency and digital procedural resilience.

### Business Register Act

- The new **Business Register Act** was adopted on **23 October 2025**. The act entered into force on 21 November 2025 but will begin to apply on 21 November 2027 (the provision relating to the processing of data on the addresses of secure electronic mailboxes for the purpose of service under the general administrative procedure act will begin to apply on 21 November 2026). The new act was adopted with the aim of a comprehensive legal, substantive and technical overhaul of the Slovenian Business Register. The new act introduces, among other things, mandatory registration of a **secure electronic mailbox** address in the Business Register to enable electronic service of documents in administrative, judicial and other proceedings. It strengthens digital-by-default communication between public authorities and companies, enhancing procedural efficiency, legal certainty and digitalisation of public administration.

### Act Amending and Supplementing the Electronic Identification and Trust Services Act

- The Act Amending and Supplementing the **Electronic Identification and Trust Services Act** was adopted on **23 October 2025** and entered into force on 21 November 2025. The amendment strengthens the security and proper use of electronic identification of trust services, including qualified certificates, by clearly defining holder responsibilities, preventing unauthorised use and expanding access points for digital authorisation. It also introduces an official electronic registry of authorisations and aligns national rules with the revised EU **eIDAS** Regulation, while updating sanctions for non-compliant service providers.

#### Act on the Implementation of the EU Regulation on Harmonised Rules for Artificial Intelligence

- The new Act on the Implementation of the EU Regulation on Harmonised Rules for **Artificial Intelligence** was adopted on **23 October 2025** and entered into force on 21 November 2025. The new act adapts Slovenian law to Regulation (EU) 2024/1689 by designating competent authorities, establishing oversight and enforcement mechanisms, and defining sanctions for AI non-compliance. It also sets the legal framework for AI regulatory sandboxes, high-risk system registries, market supervision and ethical oversight, supporting trustworthy and human-centric AI across the EU.

#### Exchange of Electronic Invoices and Other Electronic Documents Act

- The new **Business Register Act** was adopted on **23 October 2025**. The act entered into force on 6 December 2025 but will mostly begin to apply on 1 January 2028. It mandates the use of **electronic invoices** for all domestic B2B transactions in Slovenia, ensuring secure, automated and traceable exchange through regulated e-invoice service providers. It also aligns national law with EU Directive 2025/516, promotes digitalisation of business processes, and strengthens legal certainty, efficiency and cybersecurity in electronic invoicing.

#### Act on the Digitalisation of Healthcare

- The new Act on **Digitalisation of Healthcare** was adopted on **21 November 2025** and entered into force on 19 December 2025. This Act regulates the establishment and maintenance of **public central information and communication infrastructure** in the field of **healthcare** in Slovenia, the processing of data and databases in the field of healthcare and compulsory health insurance, their controllers, contractual processors, data users, and the use of data for the purposes of healthcare and compulsory health insurance, public health, development, research and statistical purposes.

#### Regulation on the training of responsible persons in the field of information and cybersecurity risk management

- The Regulation on the **training** of responsible persons in the field of information and **cybersecurity risk management** was adopted on **9 October 2025** and entered into force on 25 October 2025. The regulation, adopted on the basis of the Information Security Act, sets out the programme and methods of training for responsible persons of essential or important entities in managing information and cybersecurity risks and their impact on the activities or services performed by the entity, with the aim of ensuring a high level of security of networks and information systems and protection against cyberthreats.

## Turkish legal acts

### Draft Amendments on Artificial Intelligence Regulation in Türkiye

- On **7 November 2025**, [the Draft Law on Amendments to Turkish Criminal Code and Certain Laws](#) was submitted to the Grand National Assembly of Türkiye with the aim of introducing a regulatory framework for **artificial intelligence**. The Draft proposes to insert definitions, obligations and enforcement mechanisms into existing legislation, including Law No. 5651, the Turkish Criminal Code, the Personal Data Protection Law, the Electronic Communications Law and the Cybersecurity Law. It introduces obligations on labelling deepfake and AI-generated content, accelerated content removal and access-blocking for harmful AI content, data governance and non-discrimination requirements for training datasets, and technical and organisational safeguards for high-risk systems, as well as criminal and administrative liability regimes for users and developers.

### General Communiqué on the Tax Procedure Law

- On **27 November 2025**, the [General Communiqué on the Tax Procedure Law \(Serial No. 585\)](#) was published in the Official Gazette, announcing a revaluation rate of 25.49 % for 2026. In line with this rate, the **administrative fines** set out under Article 18 of the Turkish Data Protection Law No. 6698 were increased as of 1 January 2026. As a result, the upper limit of administrative fines applicable to certain infringements, in particular breaches of data security obligations, failure to comply with Personal Data Protection Board decisions and failure to register with the Data Controllers' Registry (*Veri Sorumluları Sicili, VERBİS*), has exceeded TRY 17m. Breach of the information obligation may result in administrative fines ranging from approximately TRY 85,000 to TRY 1.7m, while failure to implement adequate technical and organisational data security measures may give rise to fines of up to approximately TRY 17m. Similarly, failure to comply with decisions or instructions of the Personal Data Protection Board and failure to register with or notify the Data Controllers' Registry, where required, may each result in administrative fines of up to approximately TRY 17m. In addition, failure to notify the Board of standard contractual clauses used for cross-border data transfers may lead to fines of up to approximately TRY 1.8m.

### Amendments to the Presidential Decree on Cybersecurity

- On **25 December 2025**, [the Presidential Decree Amending the Presidential Decree on Cybersecurity was published in the Official Gazette No. 33118](#), introducing structural and functional changes to the Cybersecurity Directorate. The Decree expands the Directorate's mandate, including its role in coordinating the alignment of national legislation with international regulatory frameworks, and assigns new responsibilities relating to electronic (**E-devlet**) and digital government infrastructure, data governance principles for **artificial intelligence**, common data space infrastructure and data quality standards. It also authorises the establishment of new organisational units and entities both domestically and abroad.

## Austrian legal acts

### Critical Entities Resilience Act

- On **16 October 2025**, the Federal Act adopting the Federal Act ensuring a high level of resilience of critical entities (Critical Entities Resilience Act – **RKEG**) and amending the Expungement Act 1972, [Federal Law Gazette I 2025/60](#), was published. The RKEG transposes Directive (EU) 2022/2557 on the **resilience of critical entities** ([CFR Directive](#)) into national law. The **Federal Minister of the Interior** is designated as the competent authority and as the controller within the meaning of data protection law.

### Federal Act amending the SNG, SPG, TKG, BVwGG and RStDG

- On **29 September 2025**, the Federal Act amending the **State Protection and Intelligence Service Act**, the Security Police Act, the Telecommunications Act 2021, the **Federal Administrative Court Act** and the Judicial and Public Prosecutor Service Act, [Federal Law Gazette I 2025/54](#), was published. This Act creates a legal basis for the surveillance of **end-to-end encrypted communication** (such as via WhatsApp or Signal) for the purpose of combating threats relevant to the protection of the constitution. The **Federal Administrative Court** (BVwG) is competent for the **authorisation** of investigative measures.

### Criminal Law EU Adjustment Act 2025

- On **31 October 2025**, the **Criminal Law EU Adjustment Act 2025**, [Federal Law Gazette I 2025/65](#), was published. With this omnibus amendment, [Regulation \(EU\) 2019/816](#) "establishing a centralised system for the identification of Member States holding **conviction information on third-country nationals and stateless persons** (ECRIS-TCN)..." is implemented into Austrian law. The act regulates, among other things, the taking and processing of **fingerprints** in **criminal records** and the obtaining of **criminal records** from other EU Member States and the UK.

### Amendment to the Health Telematics Act

- On **3 November 2025**, the Federal Act amending the **Health Telematics Act 2012** and the General Social Insurance Act, [Federal Law Gazette I 2025/71](#), was published. This amendment creates a legal bases for cross-border health applications (**MyHealth@EU, ePrescription service, EU patient summary**).
- On **23 December 2025**, an amendment to the **Health Telematics Act 2012**, [Federal Law Gazette I 2025/93](#), was published. The amendment concerns a **retention period**, which is extended from ten to **30 years**.

### Second EU Information Systems Adjustment Act

- On **12 December 2025**, the **Second EU Information Systems Adjustment Act**, [Federal Law Gazette I 2025/87](#), was published. By this omnibus amendment, interoperability between **EU information systems** is established and the European Travel Information and Authorisation System (**ETIAS**) is set up.

### Second Transparency Database Query Ordinance 2025

- On **19 December 2025**, the **Second Transparency Database Query Ordinance 2025**, [Federal Law Gazette II 2025/313](#), was published. The ordinance governs **read permissions** for service offerings containing **sensitive data** in the **Transparency Database**.

### Network and Information Systems Security Act 2026 (NIS Act 2026)

- On **23 December 2025**, the "Federal Act enacting the Federal Act to ensure a high level of cybersecurity of network and information systems (Network and Information Systems Security Act 2026 – **NIS Act 2026**) and amending the Telecommunications Act 2021 and the Health Telematics Act 2012", [Federal Law Gazette I 2025/94](#), was published. The new NIS Act 2026 transposes the NIS2 Directive into Austrian law and also implements [Regulation \(EU\) 2021/887](#) establishing the European Cybersecurity Competence Centre. The NIS Act 2026 will enter into force on **1 October 2026**. The Telecommunications Act 2021 and the Health Telematics Act 2012 were aligned with the NIS Act 2026. For further information see [here](#).