GLI GLOBAL LEGAL INSIGHTS

AI, Machine Learning & Big Data

2023

Fifth Edition

Contributing Editor: **Charles Kerrigan**

glg global legal group

CONTENTS

Austria

Veronika Wolfbauer & Tullia Veronesi
Schoenherr Attorneys at Law

Trends

Artificial intelligence (AI) is often seen as having great potential for practical use across a wide range of industries. Accompanied by big expectations, opportunities and risks, AI is making its way into corporate practice in Austria. The domain of AI's applicability is steadily expanding and, particularly in industry, its potential is being clearly demonstrated. However, AI is of little interest to small and medium-size companies in Austria. This is principally due to the fact that such organisations either have too little know-how or the acquisition costs are too high.[1] Ignorance about the possibilities and use cases of AI systems is another reason why SMEs are less enthusiastic about adopting AI than larger companies. AI is currently relevant mostly in those sectors that use advanced manufacturing and key enabling technologies. Sectors with high productivity and a significant degree of technological embedding and digitalisation have the most use cases. Other use cases can be found, for example, in the medical field, where virtual online health assistants and chatbots provide patients with information about their medical requests. In (online) retail, the focus is on marketing and individual customer recommendations. Banks and insurance companies rely on AI to simplify complex risk assessments or fraud detection procedures. In Austria, there is an increasing trend towards the utilisation of AI, machine learning (ML) and big data. These technologies are, in summary, gaining popularity in the country.

The persistent spotlight on AI motivated the Austrian government to revamp its AI strategy. Accordingly, in 2021, the government issued its federal strategy on AI – the Artificial Intelligence Mission Austria 2030 (AIM AT 2030)[2] – which will ensure that AI systems are only deployed in a safe environment and for purposes that serve public interests. The strategy also aims to establish Austria as an industrial hub for AI and, moreover, strengthen the country's competitiveness with respect to the development and expansion of this technological area.

Key legal issues

Like many other economies, Austria has recognised the potential of AI and – as a Member State of the EU – is investing and working on suitable framework conditions. It is imperative for Europe to create suitable and agile framework conditions in which innovative companies with AI applications can develop. So far, Europe has only been moderately successful in this endeavour, which explains Austria's 16th place ranking among Organisation for Economic Co-operation and Development (OECD) countries in the Government AI Readiness Index by Oxford Insights.[3]

AI must be designed, developed and deployed in a responsible manner. In order to establish a "social license to operate" for such systems, ethical frameworks are necessary to build public trust at every level. The responsible design, development and deployment of AI also ensures its sustainable use and facilitates the realisation of its many benefits. Thus, the European Commission is currently working intensively on a coherent and holistic AI legal framework.

The AI Act

The AI Act, taking a "horizontal" approach, sets out harmonised rules for developing AI, placing it on the market and using it in the EU. The Act draws heavily on the model of "safe" product certification used for many non-AI products in the new regulatory framework. It is part of a series of draft EU proposals to regulate AI, including the Machinery Regulation and product liability reforms. The law needs to be read in the context of other major packages announced by the EU, such as the Digital Services Act, the Digital Markets Act and the Digital Governance Act. The first two are primarily concerned with the regulation of very large commercial online platforms. The AI Act does not replace the protections offered by the General Data Protection Regulation (GDPR), but will overlap with them. However, the scope of the former is broader and is not limited to personal data. The AI Act also draws on the Unfair Commercial Practices Directive for parts relating to manipulation and deception. Existing consumer law and national laws, such as tort law, are also relevant.

In a nutshell, the AI Act aims to govern the development and utilisation of AI systems deemed as "high risk" by setting standards and responsibilities for AI technology providers, developers and professional users. Certain harmful AI systems are also prohibited under the Act. The Act encompasses a broad definition of AI and distinguishes it from traditional IT. There is ongoing debate in the EU Parliament on the need for a definition for General Purpose AI. The Act is designed to be technologically neutral and future-proof, potentially affecting providers as greatly as the GDPR did. Non-compliance with the Act could result in penalties of up to EUR 30m or 6% of the provider's or user's worldwide revenue for violations of prohibited practices.

Businesses need to determine if their AI systems fall within the scope of the legislation and conduct risk assessments of their AI systems. If they are using high-risk AI systems, they must establish a regulatory framework, including regular risk assessments, data processing impact assessments and detailed record-keeping.

The AI systems must also be designed for transparency and explainability. The terms of use for these systems are deemed crucial for regulating high-risk AI systems, requiring a review of contracts, user manuals, end-user licence agreements and master service agreements in light of the new legislation.

The Regulatory Framework defines four levels of risk in AI:

- Unacceptable risk.
- High risk.
- Limited risk.
- Minimal or no risk.

The AI Act splits AI into four different bands of risk based on the intended use of the systems in question. Of these four categories, the AI Act is most concerned with high-risk AI, but it also contains a number of "red lines". These are AIs that should be banned because they pose an unacceptable risk. Prohibited systems are considered unacceptable insofar as the product of their functionality conflicts with the values of the Union, for example, through the violation of fundamental rights. These include AI that uses subliminal techniques to

significantly distort a person's behaviour in a way that causes or is likely to cause physical or psychological harm, and AI that enables manipulation, social scoring and "real-time" remote biometric identification systems in "public spaces" used by law enforcement.

The Act follows a risk-based approach and implements a modern enforcement mechanism, where stricter rules are imposed as the risk level increases. The EU AI Act establishes a comprehensive "product safety framework" based on four levels of risk. It requires the certification and market entry of high-risk AI systems through a mandatory CE-marking process and extends to ML training, testing and validation datasets. For certain systems, an external notified body may participate in the conformity assessment evaluation. Simply put, high-risk AI systems must go through an approved conformity assessment and comply with the AI requirements outlined in the EU AI Act throughout their lifespan.

Limited-risk AI systems, such as chatbots, must adhere to specific transparency obligations. The AI systems in this category must be clear about the fact that the person is interacting with an AI system and not a human being. The providers of such systems must make sure to notify its users of this.

Product liability and AI liability

The EU Commission has published two proposals for directives aimed at adapting product liability rules to the digital age. The first proposal (Product Liability Directive (PLD))[4] modernises, expands and clarifies the outdated PLD to include AI systems. Proposal number II (AI Liability Act)[5] introduces liability rules for damage caused by AI systems. Specifically, the AI Liability Act establishes new procedural rules for the application of existing Member State non-contractual civil liability rules for harm caused by AI systems.

The EU Commission justifies its need for action, among other factors, with the existing uncertainties among companies and the fear of a premature legal development by national legislators or even by independent legislative measures of the Member States. If a legislator were confronted today with special characteristics of AI, it would have to find an *ad hoc* solution by interpreting the existing regulations.[6] This legal uncertainty also inhibits innovation, because it is difficult for companies to predict how existing liability rules will be applied. This makes it almost impossible to assess one's own liability risk and take hedging measures. The result of a survey conducted by the EU Commission shows that companies consider liability for potential damages, standardisation of data and regulatory barriers (each with around 30%) as major challenges for the adoption of AI.[7] Legislative measures taken hastily by Member States would also lead to fragmentation and, ultimately, legal uncertainties.

The proposed directives are intended to complement each other and the AI Act.[8] The PLD deals with the "strict" liability of a manufacturer for defective products (including AI) and their related damages. The AI Liability Act, on the other hand, deals with liability for "wrongful conduct" by AI systems.

AI-related changes of the revised PLD

- Extension of the product definition: The definition of the term "product" will also include software and digital construction documents. Digital construction documents aim at 3D printing.[9] Software should be understood as a product regardless of how it is delivered or used (i.e. including cloud applications).[10] The product definition does not refer to AI specifically, but to software in general, with the exception of open source software.[11] Free and open source software that is developed and provided non-commercially should be excluded from the scope of the PLD, in order to not prevent the pursuit of

research and innovation. In addition, the Directive specifies when a connected service is considered part of a product, extending strict liability to certain digital services, provided they are equally fundamental to the safety of the product. However, this only applies if the connected services are under the control of the manufacturer of the product, i.e. if they are provided by the manufacturer itself or the manufacturer recommends them or otherwise influences their provision by a third party.

- Extension of the liability reasons (redefinition and extension of the concept of fault): A product is defective if it does not meet the justified safety expectations of the average consumer. The assessment in each individual case depends on the objectively justified safety expectations and presentation of the product. So far, so well known. In the future, however, other factors will also have to be taken into account. The networking and self-learning functions of products are explicitly mentioned in the draft PLD, but also the requirements for the cybersecurity of the product.[12] This change pays tribute to digitalisation and is particularly relevant to the use of neural networks and self-learning algorithms as embedded software.
- Extension of the material scope of protection: Up to now, personal injury (life, body, health) and damage to property, insofar as it occurred to a movable physical object *different* from the product, led to a claim for compensation. Pure financial losses, however, are not eligible for compensation. This restriction to fault-related violations of legal rights is maintained in principle, but the PLD provides for certain extensions. For example, the "*loss or corruption of data not used exclusively for professional purposes*" is defined as "damage" in the product liability regime. In relation to AI systems, this proposal means that in the case of damage caused by faulty AI systems, such as physical damage, damage to property or loss of data, the provider of the AI system or any manufacturer who integrates an AI system into another product can be held responsible and, regardless of fault, compensation can be claimed.
- Disclosure obligations/easier evidence for injured parties: The plaintiff bears the burden of proving the damage, the defectiveness of a product and the causal connection between the two. To do so, the plaintiff must present facts and evidence that sufficiently support the plausibility of the damages claim. Due to the information deficit that consumers naturally have when using products *vis-à-vis* their manufacturers, the EU Commission's draft provides for "access to evidence". According to this, the defendant must "produce relevant evidence within their control". If the defendant does not comply with this court order or does not do so completely, there is a high risk of losing the case, because the defectiveness of the product is then presumed by law.[13] However, this disclosure is still to be preceded by a proportionality test, which is also intended to protect trade secrets, among other things.

The key topics of the AI Liability Act

- Addressees and material scope of application: Both providers of AI systems and, in certain cases, their users can be liable parties according to the meaning of the draft AI Liability Act. The definitions[14] refer to the definitions in the AI Act. Accordingly, the "provider" is the natural or legal person, authority, institution or other body that develops an AI system or has it developed with a view to placing it on the market or putting it into operation in its own name or under its own brand (in short: the manufacturer). A "user" is a person who uses an AI system under his or her own responsibility, in the context of a professional activity (in short: a professional user). The material scope of application is limited to non-contractual fault-based civil damages claims and extends primarily to high-risk AI systems and to "other" AI systems.

- Access to evidence: Member State courts are granted the power to order the disclosure of evidence by the provider/user if the latter has already refused to comply with the direct request of a "potential claimant" (injured party or another person entitled to make a claim). This only applies to the use of high-risk AI, and only if the high-risk AI is suspected of having caused harm.[15] To obtain this order, the potential claimant must have "made all reasonable efforts" to obtain the evidence from the defendant.[16] This draft also obliges the courts to take into account the legitimate interests of all parties in their orders to disclose or preserve evidence and to limit them to a necessary and proportionate extent.[17] Particular consideration is to be given to the protection of trade secrets, leaving it to national courts to balance disclosure against such protection in individual cases. Courts should be empowered to take specific measures to protect the confidentiality of trade secrets, for example, by restricting access to documents containing trade secrets to a limited number of persons. If the defendant fails to comply with the disclosure or seizure order, it can be assumed that the defendant has breached a relevant duty of care. However, this presumption can be challenged or disproven.[18] The problem with this broad formulation ("relevant due diligence") is that it is unclear whether this provision is limited to the obligations under the AI Act or also includes breaches of other (national) laws, such as the GDPR, or general due diligence obligations. The wording of the standard rather argues for a limitation to "relevant due diligence obligations" in the sense of those obligations under the AI Act that affect high-risk AI system providers. The related recital 26 of the AI Liability Act, on the other hand, allows for a broader understanding ("*In addition, the fault of users of high-risk AI systems may be established against the backdrop of Article 29(2) [of the AI Act] if other duties of care set out in Union or national law have been breached*").
- Presumption of causality: As mentioned, one aim of the draft is to relieve injured parties of causality issues when claiming damages in connection with non-compliance with the AI Act, in order to create an incentive to comply with the AI Act. Specifically, the (rebuttable) presumption of causality[19] is intended to make it easier for the plaintiff to prove the causal link between the defendant's fault and the output produced by the AI system that caused the damage. These presumption rules are important because, without them, establishing causality would likely require a plaintiff to conduct a "review of the AI decision", which can be nearly impossible to do. However, the presumption of causality only applies if, in the opinion of the court, it is "excessively difficult" for the plaintiff to demonstrate the veracity of this presumption of causality.[20] The plaintiff must also ensure that the following conditions are met:
  - the plaintiff has proven the defendant's fault or the defendant's fault is presumed due to non-compliance with a duty of care;
  - the circumstances of the case make it sufficiently probable that the defendant's fault influenced the AI output (the "behaviour of the AI system"); and
  - the plaintiff has proven that the AI output caused the damage.

In addition, differentiated rules are provided for high-risk AI systems, whereby the application of the presumption of causality in relation to high-risk AI systems is to be limited to non-compliance with certain obligations under the AI Act. In addition, the presumption of causality will not apply if the defendant proves that the plaintiff had sufficient evidence and expertise to establish such a connection.[21]

It should be emphasised, however, that the draft does not contain an all-encompassing presumption of causality (no reversal of the burden of proof), but that the causality between

the breach of duty of the provider and the AI output is presumed (under the outlined conditions). Hence, the injured party must still prove the existence of damage, the causal connection between the output and such damage, etc.

Austrian perspective

In Austria, the proposal of those draft legal frameworks has been reflected in and monitored by the media. However, since those drafts are still subject to discussion and frequent amendment, the media contented itself with reporting rather than explaining the proposal's potential impact.

The proposed regulations will have a significant impact and will affect many stakeholders. Depending on the outcome of the discussions about the definition of AI, the framework will certainly encompass impacts on companies and stakeholders beyond those dedicated groups that are already actively working with AI systems.

Depending on the outcome of the discussions about the definition of AI, companies using software that makes predictions or decisions that guide or provide options to individuals will also be subject to the proposed regulation. This includes commonly used tools such as telematic software in cars, e-learning tools in work environments and self-creating content in private cloud solutions. There is also an expected strong merger of AI regulation and data protection regulation, as AI involves software, which entails the processing of data. The proposed AI regulation aims to regulate both the providers and users of AI, in order to protect individuals impacted by the deployed AI. A speedy resolution on the definition of AI and the establishment of a final legal framework would be beneficial for Europe, while failure could result in the continent losing its competitive edge.

* * *

Endnotes

1. Frauenhofer Austria KI-Study, *Künstliche Intelligenz in Österreichs Unternehmen*, 2022; (https://publica.fraunhofer.de/entities/publication/33a3eab0-210e-4991-9489-9fb4d39226f4/details).
2. The AIM AT 2030 paper is available for download at https://www.bmk.gv.at/dam/jcr:8acef058-7167-4335-880e-9fa341b723c8/aimat_ua.pdf (German-English).
3. Oxford Insights, *Government AI Readiness Index*, 2022; (https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/639b495cc6b59c620c3ecde5/1671121299433/Government_AI_Readiness_2022_FV.pdf).
4. Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products, COM (2022) 495 final.
5. Proposal for a Directive of the European Parliament and of the Council adapting the rules on non-contractual civil liability to artificial intelligence (AI Liability Directive), COM (2022) 496 final.
6. AI Liability Directive-E, 2.
7. European enterprise survey on the use of technologies based on artificial intelligence, IPSOS 2020, Final Report, 12, available at https://op.europa.eu/en/publication-detail/-/publication/f089bbae-f0b0-11ea-991b-01aa75ed71a1 (accessed 3.1.2023).
8. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI Act) and amending certain Union acts, COM(2021) 206 final; for more details see Herst, AI Regulation Act – the Regulation of Artificial Intelligence in this issue.

9. Recital 14.
10. Recital 12.
11. Recital 13.
12. Art 6, Rec 23.
13. Art 9 para 2.
14. Art 2.
15. Art 3 para 1.
16. Art 3 para 2.
17. Art 3 para 4.
18. Art 3 para 5.
19. Art 4.
20. Art 4 para 5.
21. Art 4 para 4.

Veronika Wolfbauer
Tel: +43 1 53437 50791 / Email: v.wolfbauer@schoenherr.eu

Veronika Wolfbauer has been with Schoenherr since 2013, having become an attorney at law in 2016 and counsel in February 2019. Prior to joining Schoenherr, she gained experience at well-known national law firms in Vienna and was legal counsel at a gas trading hub. Veronika is part of the firm's IP & technology and regulatory practices, a leading member of its privacy and data protection team, and the head of the technology regulation and audio-visual media law team. She provides strategic and legal advice to national as well as international corporate clients and also lectures in those areas. In addition, she leads administrative proceedings before the DP regulator and appeal proceedings, including addressing the Austrian Highest Administrative Court, the Austrian Constitutional Court and the European Court of Justice.

Tullia Veronesi
Tel: +43 1 53437 50310 / Email: tu.veronesi@schoenherr.eu

Tullia Veronesi has been with Schoenherr since 2021 and is an attorney at law. Her main areas of practice are IT, blockchain, cryptocurrencies, AI, E-commerce, digitalisation, start-ups, cyber security as well as intellectual property and data protection law. Before joining Schoenherr, Vienna, she practised with another international law firm as an associate and as a CLO in the new tech area. Tullia graduated from the University of Linz (Mag. iur. 2017) and from the University of Vienna (LL.M. 2018). She regularly lectures and has published articles in the field of crypto and data protection, as well as a book and a podcast on blockchain technology and is a jury and board member in various committees.

Schoenherr Attorneys at Law

Schottenring 19, 1010 Vienna, Austria
Tel: +43 1 534 370 / URL: www.schoenherr.eu

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

Banking Regulation
Blockchain & Cryptocurrency
Bribery & Corruption
Cartels
Corporate Tax
Employment & Labour Law
Energy
Fintech
Fund Finance
Initial Public Offerings
International Arbitration
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Pricing & Reimbursement

GLI GLOBAL LEGAL INSIGHTS