in short

NISG 2026

schönherr

in short

NISG 2026

*On 20 November 2025, the Austrian Federal Government presented the government bill for the Network and Information Systems Security Act 2026 (Netz- und Informationssystemsicherheitsgesetz – "**NISG 2026**"), which serves as Austria's implementing legislation for the NIS 2 Directive.*

The NISG 2026 implements the NIS 2 Directive in a highly comprehensive manner, significantly strengthening **supervisory powers**, raising **cybersecurity requirements** to a new level, and establishing **clear reporting and documentation obligations**. At the same time, it remains a **government bill**, meaning that amendments are **still possible** during the parliamentary process.

Institutional framework

The NISG 2026 establishes the **Federal Office for Cybersecurity** as a monocratic authority under the Ministry of the Interior (BMI), designated as the "**Cybersecurity Authority**" (*Bundesamt für Cybersicherheit*). The computer security incident response teams ("**CSIRTs**") will continue to serve as key pillars in the operational defence against cybersecurity incidents.

Classification

Essential entities	Important entities
Size-independent: including qualified trust service providers, TLD name registries, DNS service providers	**Size-independent:** including providers of public electronic communications networks or publicly available communications services (unless already classified as essential)
Size-dependent: entities of the type stated in Appendix 1 that operate a large enterprise	**Size-independent:** entities of the type stated in Appendices 1 and 2 that operate a large or medium-sized enterprise
Size-dependent: entities that operate a medium-sized enterprise and are providers of public electronic communications networks or providers of publicly accessible electronic communications services	**Size-dependent**: state administration entities

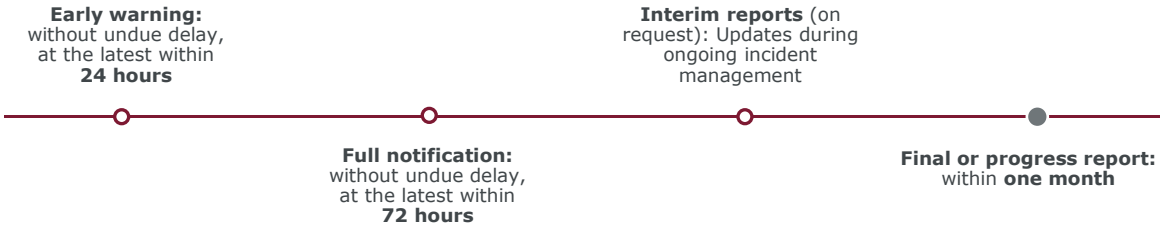
The Cybersecurity Authority may also **designate** entities listed in Annexes 1 or 2 that do not qualify as essential or important based on their size as "essential entities" or "important entities", respectively, if **certain conditions** specified in more detail in the NISG 2026 are met.

Governance

According to the NISG 2026, executive bodies bear **personal** responsibility for risk management and must **actively** supervise its implementation. This includes mandatory **cybersecurity training** for themselves as well as regular training for employees. Only natural persons at the **management or executive board level** are considered to be executive bodies; authorised signatories or functions such as the CISO are generally not included in this definition.

Notification

(exception: trust service providers, which are subject to special rules)



Supervision and measures

Essential entities are subject to **ex ante supervision**, whereas **important entities** are primarily subject to ad hoc **ex post supervision**. The range of supervisory measures extends from disclosure and submission obligations to ad-hoc audits and security scans, and may include the appointment of a supervisory officer. In **severe cases**, business licences may be revoked and the exercise of managerial functions may be temporarily prohibited.

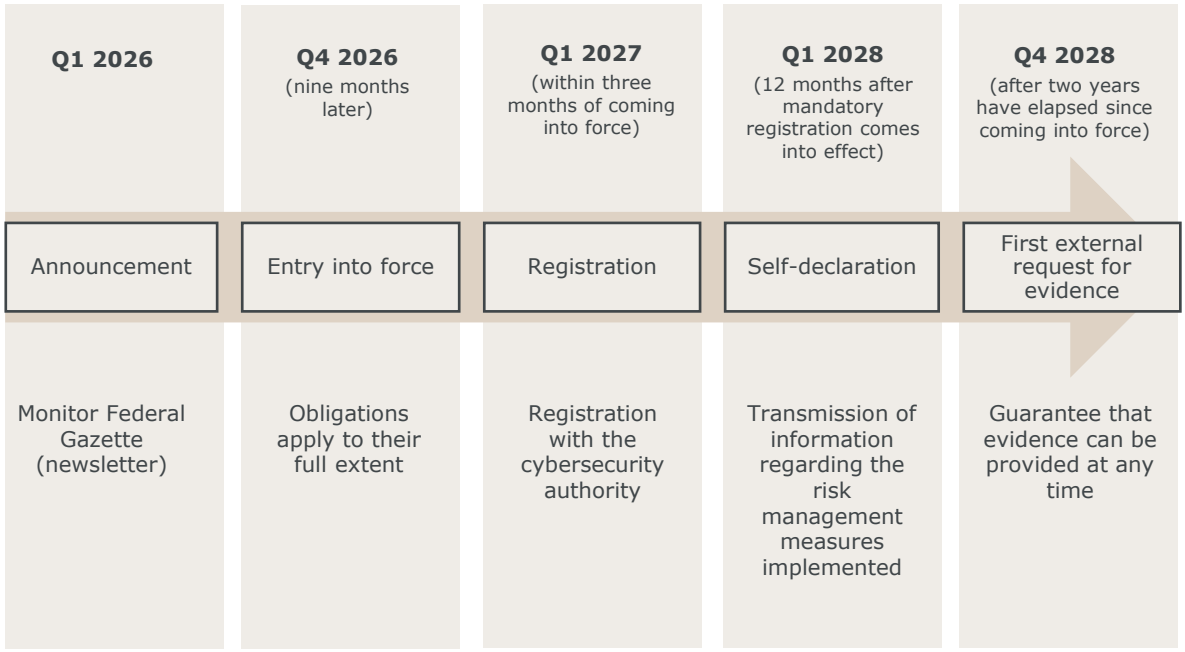
Essential and important entities must provide evidence of the technical, operational and organisational implementation of risk management measures within two years of a request from the Cybersecurity Authority; operational and organisational measures may also be demonstrated through valid certifications, such as ISO/IEC 27001. For **essential entities**, the deadline for submitting evidence of operational and organisational measures is reduced to **two months**.

Penalties

- **Essential entities:** up to EUR 10 million or 2% of global turnover from the previous year
- **Important entities:** up to EUR 7 million or 1.4% of global turnover from the previous year
- **Public authorities:** no system involving fines – alternative sanctioning regime ("*naming and shaming*" solution)
- **No double penalty** for simultaneous violation of the GDPR

in short

Schedule for the NISG 2026 (subject to announcement in Q1 2026)



Practical consequences for businesses and public authorities

Evaluation of classification	**Gap analysis of risk management measures**	**Strengthening of the notification framework**
Based on the size of the company and type of activity in accordance with Appendices 1 and 2 – entity "**essential**" or "**important**"	**Focus areas** including information security, supply chain security, incident handling, identity and access management with multi-factor authentication, emergency and recovery plans as well as training	Processes, tools and responsibilities must ensure that **early warnings** can be issued within 24 hours and **full notifications** within 72 hours
Prepare for **registration** in good time	Particular focus on the **quality of the risk analysis** and **documentation of effectiveness controls** (self-declaration and audit report)	Public administration should review internal precautionary measures in light of its **function as a role model** (high level of cybersecurity)

contact

Felix Schneider

Attorney at Law, Austria

T: +43 1 534 37 50213
E: f.schneider@schoenherr.eu

Christopher Drolz

Associate, Austria

T: +43 1 534 37 50356
E: ch.drolz@schoenherr.eu

www.schoenherr.eu