TaylorWessing

NIS2 Directive: New IT Security Requirements on an EU level

With the so-called **NIS2 Directive**, the EU has updated its IT security requirements. Compared to the former NIS("1") Directive, the NIS2 Directive contains far more specific **IT security requirements** and the **scope** of covered entities has been **widened** to a significant extent. Therefore, companies should thoroughly check whether they are subject to the NIS2 Directive and what measures they must implement. Key elements of the NIS2 Directive are:

1 **Comprehensive regulation of IT security obligations on an EU level** shall lead to greater harmonization across the European Union and improved IT security

2 **A wide coverage of economic sectors** shall ensure extensive IT security in critical areas of society in the face of current risks

3 **Affected industries** subject to the NIS2 Directive are:

- **Energy** (electricity, district heating and cooling, oil, gas and hydrogen), e. g. electricity suppliers, electricity producers or transmission and distribution system operators
- **Transport** (air, rail, water, road)
- **Banking and financial market infrastructures**
- **Health** (e. g. hospitals, laboratories, research facilities, manufacturers of pharmaceutical products)
- **Drinking and waste water**
- **Digital infrastructure:**
  - Cloud computing
  - Data centres
  - Trust service providers
  - Internet infrastructure (IXP, DNS, TLD, CDN)
  - Telecommunication and internet service providers
  - Managed service and managed security service provider (even if these services are just provided as a 'shared service' within corporate groups)
- **Public administration**
- **Space**
- **Postal and courier services**
- **Waste management**
- **Manufacture, production and distribution of chemicals**
- **Industrial production, processing and wholesale distribution of food**
- **Manufacturing:**
  - Medical devices and in vitro diagnostic medical devices
  - Computer, electronic and optical products, electrical equipment
  - Machinery and equipment
  - Motor vehicles, trailers and semi-trailers
  - Other transport equipment
- **Digital services** (online marketplaces, online search engines, social networking services platforms)
- **Research organisations**

4 **Size-thresholds:** In general, entities that engage in the afore-mentioned sectors are only subject to the NIS2 Directive either

- if they employ at least 50 persons (FTE) or
- if both their annual turnover and annual balance sheet exceed 10 Mio. EUR.
- **Exception for negligible activities:** An activity that is insignificant compared to the entity's overall business activities may be disregarded under certain conditions.
- **Attribution within corporate groups:** The thresholds generally apply to corporate groups as a whole, not just to individual subsidiaries.

5 **Registration obligation:** Submit your registration at the competent supervisory authority within three months after becoming subject to the NIS2 Directive

6 **Representative:** If your company has no establishment within the EU and provides certain digital and IT services in the EU, you may be obliged to designate a representative in one EU Member State where you offer these services. Your company shall then fall under the jurisdiction of the Member State where that representative is established.

7 **The requirement to implement comprehensive cybersecurity risk-management measures includes** taking appropriate and proportionate technical, operational and organizational measures with respect to:

- Risk analysis and information security concepts (including development of evaluation processes for effectivity of the risk management measures implemented)
- Supply chain security
- Incident handling
- Business continuity (including backup management)
- Processes for cyber hygiene and trainings for IT security
- Security measures for the acquisition, development and maintenance of network and information systems
- HR security (including access control and facility management)
- Encryption strategies
- Crisis management
- Use of multi-factor or continuous authentication solutions, secure voice, video and text communication channels as well as secure emergency communication systems

Your expert

Dr Paul Voigt, Lic. en Derecho, CIPP/E
Partner, Berlin
+49 30 885636-408
p.voigt@taylorwessing.com

8 **Stricter incident notification requirements:** Submit to the competent authority

- an early warning of a security incident within 24 hours
- a notification within 72 hours, including an initial assessment
- a final report within one month after the notification

9 **Potential information obligations towards contractual partners and users with respect to:**

- significant cyber threats (including potential protective or remedial measures to be taken)
- significant security incidents (authorities may additionally disclose an incident in case of public interest)

10 **Liability of the management bodies and specific obligations:**

- Liability of an entity's management bodies (also towards the entity) for the compliant implementation of cybersecurity risk-management measures, including selection and monitoring of supervising personnel
- Obligation to receive IT security trainings on a regular basis

11 **Executive powers of supervisory authorities include amongst other rights regarding:**

- Audits and inspections
- Information requests
- Designation of a monitoring officer
- Temporary suspension of certifications or authorisations concerning a part or all of the services provided by an entity that fall under the NIS2 Directive
- Request of a temporary prohibition for persons responsible for discharging managerial responsibilities at chief executive officer level in an entity to exercise managerial functions in that entity

12 **Fines:** up to 10 Mio. EUR (in Germany: up to 20 Mio. EUR) or 2 % of total annual turnover, whichever is higher