TaylorWessing

# NIS2 Directive: New IT Security Requirements for the energy sector

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**, covering a significant part of companies within the energy sector. Therefore, companies within the energy sector 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 companies in the energy sector** shall ensure extensive IT security in the critical area of energy supply in the face of current risks

**3** **Players within the energy sector** subject to the NIS2 Directive are:

- **Electricity:**
  - Electricity suppliers
  - Distribution system operators
  - Transmission system operators
  - Electricity producers
  - Nominated electricity market operators
  - Market participants providing electricity aggregation or demand response or energy storage services
  - Operators of recharging points provided towards end users
- **Gas:**
  - Gas suppliers
  - Distribution system operators
  - Transmission system operators
  - Storage system operators
  - LNG system operators
  - Natural gas undertakings involved in the production, transmission, distribution, supply, purchase or storage of natural gas
  - Operators of natural gas refining and treatment facilities
- **Hydrogen production, storage and transmission**
- Due to the energy sector's high degree of divided responsibilities it can be particularly difficult to determine which enterprise is actually addressed by NIS2 (e.g. if one entity owns an energy plant that is operated by another entity).

**4** **Size-Thresholds:** In general, entities that engage in the afore-mentioned activities in the energy sector 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:** NIS2 does not apply to companies in Germany if their activities within the NIS2 sectors are negligible (compared to the company's overall business activities).
- **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** **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

## 7

**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

## 8

**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)

## 9

**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

## 10

**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

## 11

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

## Your expert

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