Baker McKenzie.

Legal Update

February 2025

European Union: Who does NIS2 apply to and what are the key obligations?

In brief

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union ("**NIS2 Directive**") entered into force on 16 January 2023. It had to be transposed into national law by 17 October 2024. Only a small number of member states (among them Hungary, Belgium and Croatia) have transposed the provisions of the NIS2 Directive into national law so far, and it is likely that a significant number of member states will need some time. Nevertheless, companies are well advised to familiarize themselves with the new requirements and to provide for their implementation.

The NIS2 Directive extends the scope of application of security requirements for networks and information systems (NIS) to include numerous additional sectors compared to the previous NIS Directive (Directive (EU) 2016/1148). It also extends the range of obligations for public and private institutions. This means that companies that fall within the scope of the NIS2 Directive are subject to extensive new obligations.

The extended personal scope of application means that under the NIS2 Directive, significantly smaller companies than before are subject to NIS security requirements. Similar to other regulations such as the GDPR, the NIS2 Directive foresees severe sanctions for certain breaches, with enforcement powers assigned to the member states.

Contents

Recommended actions

Due to the extensive obligations and the potentially severe consequences in the event of non-compliance, companies should take the following steps as a matter of priority:

- Check whether the NIS2 Directive is applicable to the company and if so, make the topic of cybersecurity and risk management a "top priority";
- Compare existing measures with the requirements of the NIS2 Directive and take or supplement risk management measures;
- Create or adapt processes to comply with reporting obligations for significant security incidents; and
- Monitor local laws of the member states transposing the NIS2 Directive.

In depth

1. Which companies are covered by the NIS2 Directive?

The NIS2 Directive generally applies to companies that

- belong to a "high criticality sector" (Annex I of the NIS 2 Directive) or an "other critical sector" (Annex II of the NIS 2 Directive),

- are at least so-called medium-sized enterprises within the meaning of EU Recommendation 2003/361/EC, i.e., (i) employ at least 50 persons and/or (ii) have an annual turnover of at least EUR 10 million or an annual balance sheet total of at least EUR 10 million, and

- provide their services in the Union or carry out their activities there.

Furthermore, certain types of companies, such as for instance providers of publicly available electronic communication services or networks as well as companies that are identified as critical entities by individual member states under the Critical Entities Resilience (CER) Directive (Directive 2022/2557) are covered by the NIS2 Directive, regardless of their size. The same applies to qualified trust service providers and top-level domain name registries as well as DNS service providers.

However, companies may also be excluded - either in whole or in part – from the scope of the NIS2 Directive, e.g., by sector-specific legal acts of the Union (see below).

Annexes 1 and 2 of the NIS2 Directive – Sectors of high criticality and other critical sectors

Annex I lists "high criticality sectors" including subsectors and, in certain instances, detailed criteria on the types of entities covered. Annex II lists "other critical sectors" including subsectors and, in certain instances, detailed criteria on the types of entities covered.

High criticality sectors	Other critical sectors
• energy	• postal and courier services
• transport	• waste management
• banking	• manufacture, production, and distribution of chemicals
• financial market infrastructures	• production, processing and distribution of food
• health	• manufacturing of certain goods (e.g., medical devices; computer, electronic products, motor vehicles, other transport equipment)
• drinking water	• providers of digital services (online marketplaces, online search engines, platforms for social network services)
• waste water	• research
• digital infrastructure	
• ICT service management (B2B)	
• public administration	
• space	

The comprehensive IT security requirements of the NIS2 Directive therefore now also apply to sectors that were not subject to the obligation under the previous NIS Directive, e.g., parts of the automotive industry and mechanical engineering.

Essential and important entities

The new directive divides entities into essential and important entities. This distinction is relevant, primarily in the context of supervisory and enforcement measures and fines. These are typically stricter for essential entities. In general, essential entities are subject to a comprehensive *ex ante* and *ex post* supervisory regime, while important entities are subject only to a light *ex post* supervisory regime. For example,

- Essential entities are subject to both regular and targeted security audits, while important entities are subject only to targeted security audits;

- Authorities may impose binding instructions on both essential and important entities, but may impose specific measures necessary to prevent a potential incident only on essential entities; and

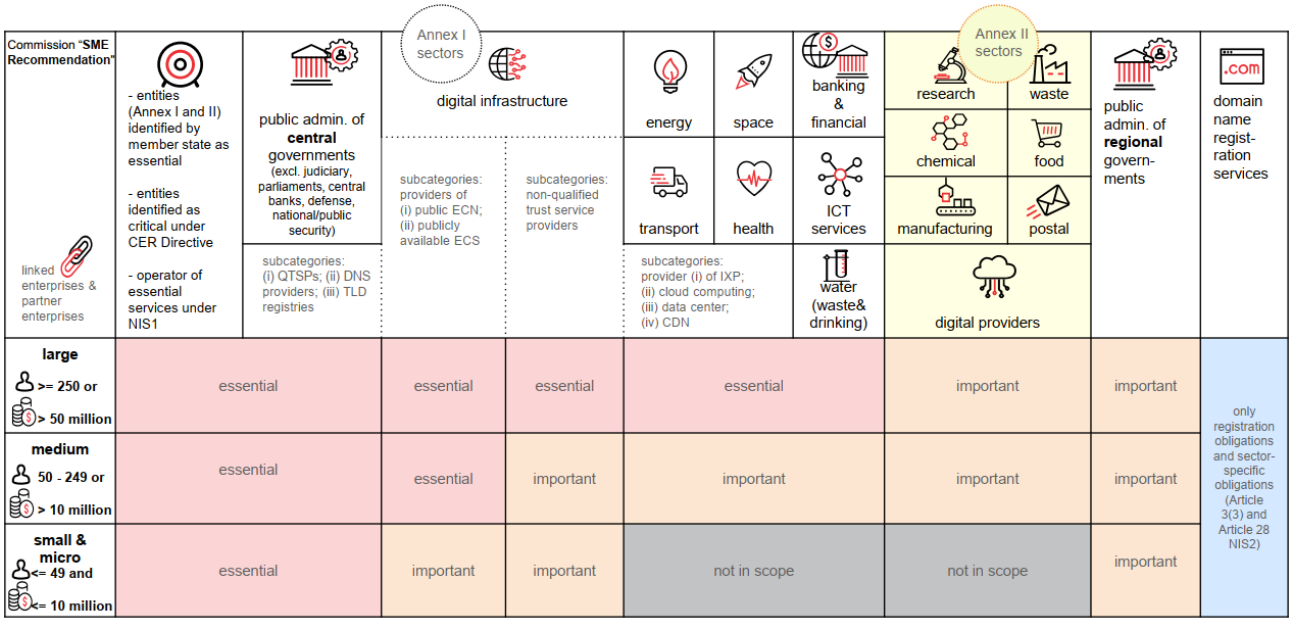
- Persistent non-compliance by essential entities may even result in the temporary disqualification of CEOs and legal representatives from exercising management functions and to the temporary suspension of certifications/authorizations (e.g., business licenses) for services and activities provided by the essential entity.

Essential entities are:

- Entities from the sectors listed in Annex I ("high criticality sectors") that exceed the ceilings for medium-sized companies, i.e., are no longer medium-sized companies;
- providers of public electronic communications networks and publicly available electronic communications services that are at least medium-sized enterprises;
- qualified trust service providers and top level domain name registries and DNS service providers, regardless of their size;
- public administration entities of central governments as defined in accordance with national laws regardless of their size; and
- other entities listed in Annexes I and II that a Member State has designated as essential entities, entities that have been designated as critical entities, and entities which have been identified as operators of essential services under NIS1.

Important entities are:

Entities listed in Annexes I and II that are not considered essential entities and entities that a Member State has designated as such.



2. What are the obligations for companies?

The NIS2 Directive provides for a comprehensive program of obligations. This includes the following obligations in particular:

Registration obligation

The NIS2 Directive foresees that essential and important entities as well as entities providing domain registration services must register with the competent authority. Certain entities, such as cloud computing service providers or providers of online marketplaces shall be required to submit additional information.

Governance

The NIS2 Directive aims to ensure a high level of accountability for cybersecurity risk management measures and reporting obligations for essential and important entities.

Therefore, the NIS2 Directive stipulates that the management bodies of significant and important entities must approve the cybersecurity risk-management measures taken, oversee their implementation and can be held liable for infringements by the entities. The NIS2 Directive foresees that management bodies must participate in trainings and that essential and significant entities offer regular trainings to their employees, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Risk management measures

The EU legislature considers the responsibility for ensuring the security of network and information systems to lie largely with essential and important entities. Because of this responsibility, it wants to promote a "risk management culture". This also includes the application of risk management measures in the area of cyber security that are appropriate to the respective risks.

Essential and important entities must therefore take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems they use for their operations or for the provision of their services and to prevent or minimize the impact of security incidents. The measures must take into account the state of the art and must be appropriate to the risks posed.

The risk management measures include at least policies on risk analysis and information security, incident handling, business continuity, such as backup and crisis management and disaster recovery, supply chain security, policies and procedures to assess the effectiveness of cybersecurity risk management measures, and, where appropriate, multi-factor authentication.

Threats to the security of network and information systems may have different causes. Therefore, risk management measures must be based on an all-hazards approach to protect the network and information systems and their physical environment from incidents. The decision as to which risk management measures should be taken must be adapted to the degree of risk exposure of the essential or important entity, the size of the entity and the likelihood of occurrence of incidents and their severity, including their social and economic impact.

For certain entities, e.g., cloud computing service providers, online marketplace providers, online search engines and social network service platforms and trust service providers, the European Commission has adopted implementing acts on 17 October 2024 to specify technical and methodological requirements for risk management measures.

Reporting obligations

The NIS 2 Directive imposes the following obligation on essential and important entities: They must notify the competent Computer Security Incident Response Team (CSIRT, which will be implemented at Member State level) or, where applicable, the competent authority without undue delay of any incident that has a significant impact on the provision of their services.

An incident is an event that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the services offered by, or accessible via, network and information systems.

An incident is significant if (i) it has caused or is capable of causing severe operational disruption of services or financial loss for the entity concerned. It is also classified as "significant" if it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Multi-stage reporting process

The reporting process is multi-stage:

- **Early warning**: Essential and important entities must submit an early warning without undue delay and in any event within **24 hours** of becoming aware of the significant incident. It shall indicate, whether the significant incident is suspected of being caused by unlawful or malicious acts or could have cross-border impact.

- **Incident notification**: Without undue delay and in any event within **72 hours** of becoming aware of the significant incident, essential and important entities must submit an incident notification. This must update information as appropriate and include an initial assessment of the significant incident, including its severity and impact, and, where available, the indicators of compromise.

- **Final report**: No later than **one month** after submitting the incident notification, essential and important entities must submit a final report. This shall contain (i) a detailed description of the incident, including its severity and impact, (ii) the type of threat or root cause that is likely to have triggered the incident, (iii) applied and ongoing mitigation measures and (iv) where applicable, the cross-border impact of the incident.

The multi-stage approach is designed to enable the right balance between, on the one hand, timely notifications that counteract the potential spread of significant incidents and enable essential and important entities to receive support, and, on the other hand, detailed notifications where lessons can be learned from security incidents and entire sectors can improve their cyber resilience.

Essential and important entities shall also, where appropriate, inform the recipients of their services without undue delay of these significant incidents that are likely to adversely affect the provision of the services. Also, the NIS2 Directive foresees a notification requirement concerning significant cyber threats.

3. Sector-specific rules and possible effects of minimum harmonization

The NIS2 Directive seeks to provide for minimum, not full harmonization, i.e., it does not prevent member states from adopting or maintaining provisions that ensure a higher level of cybersecurity than those set out in the NIS2 Directive.

This means that the national laws at Member State level, which transpose the NIS2 Directive, may differ significantly between the member states. One area, where Member State laws take different approaches to implementing the NIS2 Directive is the handling of requirements applicable to providers of publicly available electronic communication services and public electronic communication networks, with some member states maintaining (parts of) sector specific regulation in the national telecommunications laws (which can lead to additional obligations applicable to providers and parallel competence of several authorities) and other member states centralizing relevant requirements in one single NIS2 implementation law.

Providers should therefore not base their compliance efforts solely on the provisions as set out in the NIS2 Directive, but also assess local implementation. This is in particular key where they are subject to the jurisdiction of more than one Member State (as is the case for providers of publicly available electronic communication services and public electronic communication networks, see also below).

With regard to the relationship to the EU's Digital Operational Resilience Act (DORA) for the financial sector, the NIS2 Directive stipulates that where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in the NIS2 Directive, the relevant provisions of NIS2 Directive shall not apply (Art. 4 NIS 2 Directive). DORA stipulates that, with regard to financial entities identified as "essential or important entities" pursuant to national laws transposing the NIS2 Directive, DORA "shall be considered a sector-specific Union legal act for the purposes of Article 4 of that Directive" (Art. 1 para. 2 DORA).

4. What are the sanctions in the event of a breach?

According to the NIS2 Directive, violations can have significant consequences:

member states should provide for administrative fines of a maximum amount of at least EUR 10 million or 2% of the total worldwide turnover in the preceding financial year, whichever is higher, against essential entities that do not take sufficient risk management measures or violate reporting obligations.

For important entities that do not take sufficient risk management measures or violate reporting obligations, the member states should provide for administrative fines with a maximum amount of at least EUR 7 million or 1.4% of the total worldwide turnover in the preceding financial year, whichever is higher.

The competent authorities should also be able to take measures such as on-site inspections, targeted security audits, issue warnings or order entities concerned to implement the recommendations provided.

5. Jurisdiction and territoriality

Entities that are subject to the requirements of the NIS2 Directive fall under the jurisdiction of the Member State in which they are established (country of origin), except in the case of:

- providers of public electronic communications networks or providers of publicly available electronic communications services, which fall under the jurisdiction of the Member State in which they provide their services;
- DNS service providers, top-level domain (TLD) name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which fall under the jurisdiction of the Member State in which they have their main establishment in the Union (an entity shall be considered to have its main establishment in the EU in the Member State (i)

where decisions related to the cybersecurity risk-management measures are predominantly taken, and (ii) if such Member State cannot be determined or decisions are not taken in the EU, where cybersecurity operations are carried out, and (iii) if that cannot be determined, where the entity concerned has the establishment with the highest number of employees in the EU); and

- public administration entities, which shall be considered to fall under the jurisdiction of the Member State which established them.

If an entity listed in the second bullet point above is not established in the Union, but offers services within the Union, such entity must designate a representative in the Union.

6. What should companies do now?

Due to the extensive obligations and the potentially severe consequences in the event of non-compliance, companies should take the following steps as a matter of priority:

- Check whether the NIS2 Directive is applicable to the company and if so, make the topic of cybersecurity and risk management a "top priority";
- Compare existing measures with the requirements of the NIS2 Directive and take or supplement risk management measures;
- Create or adapt processes to comply with reporting obligations for significant security incidents; and
- Monitor local laws of the member states transposing the NIS2 Directive.

Contact Us

Dr. Lukas Feiler
Partner
lukas.feiler@bakermckenzie.com

Dr. Michaela Nebel
Partner
michaela.nebel@bakermckenzie.com

Caroline Heinickel LL.M.
Counsel
caroline.heinickel@bakermckenzie.com

Silvia Grohmann
Associate
silvia.grohmann@bakermckenzie.com