Bird & Bird

NIS2 Directive

EU co-legislators reach a provisional agreement

June 2022

NIS2 Directive

EU co-legislators reach a provisional agreement

On 13 May 2022, the European Parliament and EU Member States reached a provisional agreement on the Directive on measures for a high common level of cybersecurity across the Union ("**NIS2 Directive**"). This act will repeal the current directive on security of network and information systems ("**NIS Directive**"), amending the rules on the security of network and information systems.

In summary, the NIS2 Directive is part of a package of instruments and initiatives to further improve the resilience of public and private entities against cybersecurity threats. It sets rules to ensure protection and smooth uninterrupted functioning of services which are critical for the society. To this aim, it modernises the existing legal framework built on the NIS Directive, in particular expanding its scope as well as strengthening and streamlining security and reporting requirements. The act furthermore introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States.

Importantly, despite ensuring a higher level of harmonisation than the current rules, the NIS2 Directive does not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with their obligations under Union law. This means that, depending on the national implementation of the NIS2 Directive, there will be still divergencies with respect to security, incident reporting and other requirements. This needs to be considered by organisations when implementing new requirements.

The rules will be of relevance both for the entities directly falling under the new Directive (in conjunction with its future local implementation) as well as, though itself not in scope, dealing with the organisations covered by the NIS2 Directive.

Once formally approved by the co-legislators and published in the Official Journal, the NIS2 Directive will enter into force 20 days after publication. Member States will then have 21 months to transpose the Directive into national law. In Germany, for example, following the IT Security Act 2.0, the legislator will have to deal with an IT Security Act 3.0.

This article describes the key takeaways of the provisional agreement. Although this may change during the legislative process, the outline of the provisions is clear and is summarized below.

1.) Widening of the scope of the rules

The NIS2 Directive provides for a much broader scope of application than the current NIS Directive:

- **Size-cap rule**: While under the current NIS Directive member states were responsible for determining which entities would meet the criteria to qualify as operators of essential services, the new NIS2 Directive introduces a size-cap rule. This means that all public as well as private medium-sized and large entities of a type referred to in Annex I and Annex II providing their services or carrying out their activities within the Union are covered by the Directive.

  There are, however, certain exceptions: Regardless of their size, the NIS2 Directive also applies to essential and important entities where for example the services are provided by providers of public electronic communications networks, publicly available electronic communications services, top-level domain name registries, trust service providers, or where the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities (cf. Art. 2(2)).

- **Essential and important entities**: Entities falling within the scope of the new Directive are essential entities and important entities operating in the following sectors as specified in annexes to the Directive (see the table below):

Essential entities	Important entities

• Energy
• Transport
• Banking
• Financial market infrastructures
• Health
• Drinking water
• Waste water
• Digital infrastructure
  – Internet Exchange Point providers
  – DNS service providers, excluding operators of root name servers
  – TLD name registries
  – Cloud computing service providers
  – Data centre service providers
  – Content delivery network providers
  – Trust service providers
  – Providers of public electronic communications networks or providers of electronic communications services
• ICT-service management (B2B)
  – Managed service providers (MSP)
  – Managed security service providers (MSSP)
• Public administration entities (excluding the judiciary, parliaments and central banks) and
• Space
	• Postal and courier services
	• Waste management
	• Manufacture, production and distribution of chemicals
	• Food production, processing and distribution
	• Manufacture of medical devices, electronic products and transport
	• Digital providers
	  – Providers of online marketplaces
	  – Providers of online search engines
	  – Providers of social networking services platform
	• Research

The text also clarifies that the Directive will not apply to entities carrying out activities in areas such as defence or national security, public security, law enforcement and the judiciary. Parliaments and central banks are also excluded from the scope.

2.) Relation of the NIS2 Directive to sector-specific acts

The European Parliament and the Council have aimed to align the text with sector-specific legislation, in particular the regulation on digital operational resilience for the financial sector (DORA) and the directive on the resilience of critical entities (CER), to provide legal clarity and ensure coherence between the NIS2 Directive and these acts:

As set out in the NIS2 Directive, 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 this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid, shall not apply to such entities. If, however, sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive shall continue to apply to the entities not covered by those sector-specific provisions (cf. Art. 2b(1)).

In Art. 2b(2) NIS2 Directive, it has been thereby clarified which aspects should be considered when determining the equivalent effect of requirements set out in the sector specific provisions of a Union legal act.

The Commission shall within six months after the entry into force of this Directive, issue guidelines clarifying the application of the afore mentioned provisions.

As a result, entities should verify whether national horizontal law regulations implementing the NIS2 Directive will apply, in addition to sector specific legal acts.

3.) Territorial scope

As to the territorial scope, essential and important entities under this Directive should fall under the jurisdiction of the Member State in which they are established, except:

- Providers of public electronic communications networks or providers of electronic communications services (which shall be deemed to be under the jurisdiction of the Member State in which they provide their services);
- DNS service providers, TLD name registries, and entities providing domain name registration services for the TLD, cloud computing services providers, content delivery network providers, managed service providers and managed security service providers as well as digital providers (which shall be under the jurisdiction of the Member State in which they have their main establishment in the Union);
- Public administration entities (which shall be deemed under the jurisdiction of the Member State which established them).

In addition, if an entity referred to in the list set out above is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under Article 24, any Member State in which the entity provides services may take legal actions against the entity for non-compliance with the obligations under the NIS2 Directive.

4.) Strengthened cybersecurity risk and incident management

The revised Directive aims to remove divergences in cybersecurity as well as reporting requirements and in their implementation in different member states. To achieve this, it sets out minimum rules for a regulatory framework in this regard. Essential and important entities will be subject to the same cybersecurity and reporting requirements.

a) Cybersecurity risk management

Similar to the current NIS Directive, essential and important entities will be required to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Apart from this general requirement, cybersecurity risk management measures have been specified in more detail in the new Directive.

Such measures shall be based on an all-hazards approach aiming to protect network and information systems and their physical environment from incidents, and shall include at least the following:

- risk analysis and information system security policies;
- incident handling;
- business continuity, such as backup management and disaster recovery, and crisis management;
- supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- policies and procedures to assess the effectiveness of cybersecurity risk management measures;
- basic computer hygiene practices and cybersecurity training;
- policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- human resources security, access control policies and asset management;
- the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate (cf. Art. 18(2)).

b) Incident management

The two co-legislators have also streamlined the reporting obligations in order to avoid causing over-reporting and creating an excessive burden on the entities covered (cf. Art. 20).

In the context of reporting, the NIS2 Directive makes a differentiation between an incident (meaning "*any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the*

services offered by, or accessible via, network and information systems", cf. Art. 4 no. 5) and a cyber threat (meaning "*a cyber threat within the meaning Article 2(8) of the Cybersecurity Act*[1]", i.e. "*any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons*", cf. Art. 4 no. 7):

aa) With regard to reporting obligations in the context of an incident having a significant impact on the provision of the services of essential or important entities, the Parliament has asserted itself with a graduated approach: The entities concerned shall submit to the CSIRT or, where relevant, the competent authority

- an initial notification of the significant incident;
- upon request of a CSIRT or the competent authority, an intermediate report including indicators of compromise on relevant status updates;
- a final report not later than one month after the submission of the initial notification under first bullet point, including at least the following: a detailed description of the incident, its severity and impact; the type of threat or root cause that likely triggered the incident; applied and ongoing mitigation measures.

In cases of ongoing incidents at the time of the submission of the final report, entities would need to provide a comprehensive report at that time and a final report within one month after the incident has been handled. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of those incidents that are likely to adversely affect the provision of that service.

bb) With respect to reporting obligations in the context of a significant cyber threat: Where applicable, essential and important entities shall communicate, without delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the threat itself.

5.) Express governance requirements

In addition, the NIS2 Directive sets out express governance requirements (cf. Art. 17). The management bodies of essential and important entities will be on this basis required

- to approve the cybersecurity risk management measures taken by those entities in order to comply with cybersecurity risk measures,
- to oversee its implementation and
- can be held liable for non-compliance by the entities with the obligations under this Article.

Member States shall also ensure that the members of the management body of essential and important entities are required to follow training and shall encourage essential and important entities to offer similar training to all employees on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the services provided by the entity.

The non-compliance liability of management bodies and training obligations requires companies to appoint a 'cybersecurity officer' at board level, to ensure compliance oversight and to reassess company and management assurance conditions in terms of liability risk mitigation.

6.) Cybersecurity certification

For the purposes of demonstrating compliance with cybersecurity risk management measures and in the absence of appropriate European cybersecurity certification schemes adopted in accordance with the Cybersecurity Act, Member States may require entities to use particular ICT products, services and processes, either developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Art. 49 of the Cybersecurity Act. Furthermore, Member States shall encourage essential and important entities to use qualified trust services.

For suppliers, it will be important to verify whether the Member States in which they operate will mandate the use of certified products, services or processes.

In this context, the Commission's power to determine the sectors in which cybersecurity certification should be mandated through secondary legislation was contentious. Now, it has been agreed upon that these certifications are introduced via delegated acts, which gives the Commission more leeway, as opposed to the implementing acts required by the Council, which give governments more control: The Commission is empowered to adopt delegated acts specifying which categories of essential or important entities shall be required to use certain certified ICT

[1] Regulation (EU) 2019/881.

products, services and processes or obtain a certificate under which European cybersecurity certification schemes adopted pursuant to Art. 49 of the Cybersecurity Act. The adoption of such delegated acts shall be preceded by an impact assessment and stakeholder consultation.

7.) Sanctions

The NIS2 Directive furthermore provides for remedies and sanctions to ensure enforcement. Organisations that do not comply with the new cybersecurity measures will face fines. Managing directors will be held personally liable.

a) Supervision and enforcement

Competent authorities will be required to supervise the entities under the scope of the NIS2 Directive. The NIS2 Directive distinguishes between an ex-ante supervisory regime for essential entities (Art. 29) and an ex-post supervisory regime for important entities (Art. 30). In the latter case, competent authorities will need to take action when provided with evidence or indication, or information that an important entity is allegedly not in compliance with the obligations laid down in this Directive, and in particular the security and incident notification requirements.

b) Administrative fines

The Directive also requires Members States to impose administrative fines to essential and important entities and defines certain maximum fines. There will be a differentiation for important entities on the one side and essential entities on the other side with respect to the amount of the fines in case of infringements of the cybersecurity risk management (Art. 18) or reporting (Art. 20) obligations. Member States may furthermore provide for the power to impose periodic penalty payments in order to force an essential or important entity to cease an infringement in accordance with a prior decision of the competent authority.

c) Temporary ban from exercising managerial functions

In the context of supervision and enforcement for essential entities, under certain circumstances, the competent authorities will have the power to request the imposition by the relevant bodies or courts in accordance with national law of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity from exercising managerial functions in that entity (Art. 29(5) lit. b)).

Such temporary bans shall be applied only until the entity concerned takes the necessary action to remedy the deficiencies or complies with the requirements of the competent authority for which such sanctions were applied. In addition, the imposition of such temporary bans shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection, due process, presumption of innocence and right of defence.

Member States shall further ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.

8.) What companies should already do now

We have highlighted above some actions organisations should have in place when national implementation acts pursuant to the Directive come into force. In addition, organisations are advised to act now and assess the following:

- whether the organisation falls/might fall within the scope of the new Directive;
- what new requirements would need to be implemented by the organisation directly falling within the scope of the new legislation;
- if the organisation is not directly covered by the act, whether it deals with suppliers or customers subject to the new rules;
- what obligations do organisations need to attribute to their suppliers or business customers in their contractual arrangements, in order to facilitate a seamless, cybersecurity compliant supply chain. Therefore, insight into the regulatory obligations will be also relevant for organisations not directly covered by the new act; and
- whether there are any related or additional local IT security requirements, which still or would potentially need to be implemented due to any national legislation, and to steer for a coordinated approach in terms of implementation.

Your Contacts

Dr. Fabian Niemann

Partner

fabian.niemann@twobirds.com

Dr. Natallia Karniyevich

Associate

natallia.karniyevich@twobirds.com

Mr. Feyo Sickinghe

Of Counsel

feyo.sickinghe@twobirds.com

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw