EU-Directive

NETWORK AND INFORMATION SECURITY (NIS 2.0)

cep**PolicyBrief** No. 2021-13

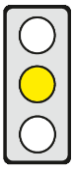
Centrum für Europäische Politik
FREIBURG | BERLIN

KEY ISSUES

Background: The applicable NIS Directive has shown several shortcomings, which the Commission wants to address.

Objective of the Directive: The EU Commission wants to improve the overall level of cybersecurity in the EU.

Affected parties: Essential and important private and public entities, EU and national cybersecurity authorities and bodies.



Pro: (1) Cybersecurity requirements for entities that are crucial to society are appropriate because the economic incentives to invest in cybersecurity are inadequate and the costs to society of cyber incidents affecting essential and important entities are particularly high.

(2) The new notification procedures increase legal clarity and the single-entry point for notifications reduces the administrative burden for notifying entities.

Contra: (1) The new responsibilities of essential and important entities to consider supply chain risks should be limited to risks affecting suppliers of ICT products and services that are deemed security relevant for the entities' business.

(2) The duty to notify incidents within 24 hours may prove to be too challenging for smaller entities.

The most important passages in the text are indicated by a line in the margin.

CONTENT

Title

Proposal COM(2020) 823 of 16 December 2020 for a **Directive on measures for a high common level of cybersecurity across the Union,** repealing Directive (EU) 2016/1148

Brief Summary

- **Context and objectives**
  - The current Directive on the security of network and information systems ["NIS 1.0", (EU) 2016/1148, see cep**PolicyBrief**], in particular, [p. 1]
    - requires Member States to adopt national cybersecurity strategies and appoint cybersecurity authorities,
    - establishes different forums to enhance cybersecurity cooperation between Member States,
    - requires Member States to establish mandatory cybersecurity risk management rules and
    - requires Member States to introduce obligations to notify cybersecurity incidents.
  - According to the Commission, since the entry into force of the Directive, cybersecurity resilience in the EU has significantly improved. However, it has also identified several remaining shortcomings, e.g.: [Recital 2, p. 5]
    - the scope of the Directive is "too limited" and "not sufficiently clear";
    - Member States' discretion, when transposing the requirements for security risk management and incident notification, is too wide; and
    - supervision and enforcement are "ineffective".
  - The proposed Directive "NIS 2.0" addresses these shortcomings and repeals the existing NIS Directive.

- **Scope**
  - The Directive applies to all public and private entities, with more than 50 employees or an annual turnover or balance sheet sum of at least € 10 million, that qualify as either (full list see cep**Document**) [Art. 2 (1)]
    - "essential", e.g. electricity and water suppliers, oil producers, banks, or
    - "important", e.g. manufacturers of medical devices, producers of food or providers of online marketplaces.
  - Regardless of their size, the Directive applies to "essential" or "important" public and private entities that are [Art. 2 (2)]
    - providers of public electronic communication networks and services, trust services related, inter alia, to electronic signatures or top-level domain (TLD) name registries and systems,
    - public administrations at the level of central governments, major socio-economic and basic regions that, inter alia, have legal personality, are established for meeting needs in the general interest, and exercise administrative or regulatory powers affecting the freedom of movement of persons, goods, services and capital (four freedoms),
    - the sole provider of a service in a Member State,

Authors: Philipp Eckhardt and Dr. Martina Anzini | eckhardt@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Germany | Telephone + 49 761 38693-107 | www.cep.eu

- providers of services,
  - the disruption of which could endanger public safety, public security, public health or cross-border systemic stability, or
  - that are specifically critical at regional or national level, or
  - that are designated by Member States as "critical", i.e. essential for providing vital economic and social functions, under the proposed Directive on the resilience of critical entities [COM(2020) 829].
- The risk management and reporting requirements of the Directive do not apply where other EU regulations provide for stricter requirements [Art. 2 (6)]. This applies, inter alia, to financial sector entities that are subject to the proposed Digital Operational Resilience Act [COM(2020) 595, see cep**PolicyBrief**] [Recital 13].

- **Cybersecurity risk management by essential and important entities**
  - Essential and important entities must take "appropriate and proportionate technical and organisational measures" to manage risks posed to the security of the network and information systems (NIS) they use to provide their services. This must include at least the analysis of risks, information system security policies, incident handling, business continuity, the security of supply chains and the use of encryption. [Art. 18 (1) and (2)]
  - Regarding the security of their supply chains, essential and important entities must consider the vulnerabilities specific to each supplier, the quality of the products and cybersecurity practices of those suppliers [Art. 18 (3)].
  - The management bodies of essential and important entities must approve the risk management measures and supervise their implementation. They are accountable for any non-compliance with the Directive and must conduct regular training on cybersecurity risks and their impact on the entity. [Art. 17]
  - The Commission may adopt implementing acts laying down "technical and methodological specifications" on the risk management measures, and delegated acts extending the list of measures [Art. 18 (5) and (6)].
  - The Commission may – via delegated acts – decide that certain categories of essential entities must obtain a certificate for ICT products, services or processes under a "European cybersecurity certification schemes" as developed by the European Agency for Cybersecurity (ENISA) (see also cep**PolicyBrief**). Member States may, in addition, require individual essential and important entities to do so. [Art. 21]

- **Notification of incidents and cyber threats to authorities and customers**
  - Incidents are events that compromise data or services offered by, or accessible via, NIS [Art. 4 (5)]. Cyber threats, on the other hand, are events that could damage, disrupt or adversely impact NIS, their users or other persons [Art. 4 (7)].
  - Essential and important entities must notify national competent authorities or national computer security incident response teams (CSIRTs), without undue delay, of any [Art. 20]
    - significant incidents, i.e. such incidents, that may lead to substantial operational disruptions or financial losses for the entity or considerable material or non-material losses for other natural or legal persons, and
    - significant cyber threats which they identify that could have potentially resulted in a significant incident.
  - Significant incidents must be reported, in general, within 24 hours, indicating whether an incident is "presumably caused by unlawful or malicious action" [Art. 20 (4)].
  - An intermediate report with status updates must be submitted upon the request of a competent authority or CSIRT [Art. 20 (4)].
  - A final report must be submitted within one month of the incident, indicating its severity and impact, the type of threat, its root cause and applied mitigation measures [Art. 20 (4)].
  - Essential and important entities must, without undue delay, notify their customers, [Art. 20 (1) and (2)]
    - where appropriate, of incidents that are likely to adversely affect the provision of their services, and
    - where applicable, of significant cyber threats, and the measures they can take in response to those threats.
  - The competent authority or CSIRT must respond within 24 hours, provide initial feedback and, upon request by the entity, guidance on mitigation measures [Art. 20 (5)].
  - The competent authority or CSIRT may inform the public about the incident, or require the concerned entity to do so, if public awareness may prevent or manage the incident, or is in the public interest [Art. 20 (7)].
  - Member States are encouraged to establish a national single entry point for all notifications, also covering notifications, e.g., of breaches under the General Data Protection Regulation [GDPR, (EU) 2016/679] and the ePrivacy Directive [2002/58/EC] [Recital 56].

- **Supervision, enforcement and sanctions**
  - The competent national authorities must be granted a minimum of supervisory powers, inter alia for on-site inspections, security audits. Essential entities may be checked ex-ante and ex-post, important entities only ex-post. [Art. 29 (2) and 30 (2)]
  - The competent authorities must be granted a minimum of enforcement powers, inter alia for issuing warnings and instructions. They can be addressed to both essential and important entities. [Art. 29 (4) and 30 (4)]
  - If entities do not comply with enforcement actions, the authorities may apply sanctions.
    - Sanctions may be imposed on both [Art. 29 (5)]
      - the entity – e.g. suspension of certifications – and
      - the individuals responsible for its management – e.g. temporary ban on exercising managerial functions.

Main changes to the Status quo

- NIS 2.0 covers a number of entities and sectors that were not covered by NIS 1.0, e.g., operators of hydrogen production, wastewater companies and manufacturers of motor vehicles (see cep**Document**).
- NIS 1.0 differentiates between operators of essential services and digital service providers; and Member States have wide discretion to define these entities. NIS 2.0 differentiates between essential and important entities and sets a uniform criterion in the form of a size-cap.
- In NIS 1.0, the scope of necessary cybersecurity risk management measures is vague, and Member States have wide discretion. NIS 2.0 provides more detail and puts a stronger focus on supply chain risks.
- In NIS 1.0, the scope of notification requirements is vague. NIS 2.0 provides for clearer rules on which, when and how incidents must be notified. It introduces a notification requirement for cyber threats.
- In NIS 1.0, supervision is less harmonised and enforcement is not equally effective across the EU. NIS 2.0 provides for a minimum list of supervisory and enforcement powers and a more detailed sanctions regime.

Statement on Subsidiarity by the Commission

EU intervention is justified by the cross-border nature of NIS-related threats, its means for improving and facilitating effective and coordinated national policies and its capacity for coordinated action to protect data and privacy.

Policy Context

The proposed Directive complements the proposed Directive on the resilience of critical entities [COM(2020) 829], which revises the Council Directive on the identification and designation of European critical infrastructures [2008/114/EC] and the Cybersecurity Act [Regulation (EU) 2019/881, see cep**PolicyBrief**].

Legislative Procedure

16 December 2020	Adoption by the Commission
Open	Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

Options for Influencing the Political Process

Directorates General:	Connect
Committees of the European Parliament:	ITRE (leading), Rapporteur: Angelika Niebler (EPP, Germany)
Federal Germany Ministries:	Interior, Building and Community
Committees of the German Bundestag:	Internal Affairs and Community
Decision-making Mode in the Council:	Qualified majority (acceptance by 55% of Member States which make up 65% of the EU population)

Formalities

Competence:	Art. 114 TFEU (Internal Market)
Type of Legislative Competence:	Shared competence (Art. 4 (2) TFEU)
Procedure:	Art. 294 TFEU (ordinary legislative procedure)

ASSESSMENT

Economic Impact Assessment

Cybersecurity requirements for entities that are crucial to society are appropriate: Entities already have a vested interest in protecting their network and information systems against cyber incidents and threats since a failure to do so may cause significant revenue losses and reputational damage. Nevertheless, although they are associated with considerable costs and limit entrepreneurial freedom, common European requirements for "appropriate technical and organisational measures" regarding NIS are justified because **the economic incentives to invest in cybersecurity are inadequate**. This is firstly because entities often do not have to bear the full costs caused by cyber incidents **and** can shift some of the costs onto third parties, e.g. their clients. Secondly, entities can free-ride on the cybersecurity investments made by others as these investments often not only enhance the investor's NIS-resilience but indirectly also that of others. **Furthermore, the costs to society of cyber incidents affecting essential and important entities are particularly high.**

By contrast with the existing Directive, the new definition of the scope of the Directive increases legal clarity and limits regulatory arbitrage and hence distortions of competition. However, the scope of the Directive is too broad: it encompasses many entities which do not provide products or services that are crucial for the functioning of a society, e.g. car manufacturers which should therefore be left out. Moreover, it is questionable whether the competent authorities would be able to adequately supervise all the entities that fall under the Directive – e.g. all "important" manufactures,

i.e. 31,000 medium and large-sized manufacturers [SWD(2020) 345, page 63]. Also, the size as sole criterion is inappropriate as size alone does not necessarily indicate a higher cybersecurity risk. Other criteria such as the number of customers should be added.

The new responsibilities of essential and important entities to consider supply chain risks to a larger extent than under the current Directive, as part of their cybersecurity risk management, may increase the general cybersecurity level in the EU. However, they **should be limited to risks affecting suppliers of ICT products and services that are deemed security relevant for the entities' business.** Furthermore, the burden should not lie solely on the essential and important entities at the end of the supply chains. There should also be requirements for the suppliers within the supply chains to ensure their ICT-products and -services, if delivered to essential and important entities, are cyber secure.

Entities have few incentives to report cyber incidents and threats, given the reporting costs and potential reputational damage. At the same time, notifications help others to identify and close security loopholes. Notification of cyber incidents and threats therefore gives rise to substantial external benefits, so forcing entities to report is appropriate. **The new notification procedures increase legal clarity and the single-entry point for notifications reduces the administrative burden for notifying entities. The** envisaged **duty to notify incidents** and supply meaningful information **within 24 hours may prove to be too challenging** to comply with, especially **for smaller entities.** Such fast notifications may also tie up resources of entities that could be better used to tackle the incident.

Legal Assessment

Legislative Competence of the EU

The Directive is rightly based on Art. 114 TFEU. This also applies to the inclusion into its scope of those public administrations that issue administrative or regulatory decisions affecting the four fundamental freedoms. In fact, measures based on Art. 114 TFEU must genuinely aim to improve the conditions for the establishment and functioning of the internal market by eliminating either obstructions of the fundamental freedoms or significant distortions of competition [Judgement of 3 September 2015, C-398/13 P, Inuit Tapiriit Kanatami and Others v Commission, EU:C:2015:535, para 26]. Establishing common rules that improve the cybersecurity of public administrations will meet the above criteria if such common rules cover national authorities upon which legal and natural persons depend to exercise their rights to the movement of persons, goods, services or capital. This could be the case where a supervisory authority issues an authorisation allowing market players to offer their services throughout the whole internal market. In fact, in such cases, the fitness of public administrations to perform their tasks in a continuous and secure fashion is a condition which must be met in order for all persons, whether natural or legal, to effectively exercise the aforesaid rights.

Subsidiarity

Unproblematic, given the cross-border nature of NIS-related threats and incidents.

Proportionality with Respect to Member States

Member States retain the power to regulate the cybersecurity regime applicable to entities not covered by the Directive. Also, they retain some leeway when deciding upon the appropriateness and proportionality of the technical and organisational risk management measures. Finally, the Directive brings about minimum harmonisation [Art. 3] and therefore enables Member States to establish a higher level of cybersecurity if they so wish.

Summary of the Assessment

Cybersecurity requirements for entities that are crucial to society are appropriate because the economic incentives to invest in cybersecurity are inadequate and the costs to society of cyber incidents affecting essential and important entities are especially high. The new responsibilities of essential and important entities to consider supply chain risks should be limited to risks affecting suppliers of ICT products and services that are deemed security relevant for the entities' business. The new notification procedures increase legal clarity and the single-entry point for notifications reduces the administrative burden for notifying entities. The duty to notify incidents within 24 hours may prove to be too challenging for smaller entities.