Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations

Thomas Sievers

Received: 6 August 2021 / Accepted: 13 August 2021 / Published online: 20 September 2021
© Springer Fachmedien Wiesbaden GmbH 2021

Abstract The proposal for a Network and Information Systems (NIS) Directive 2.0 aims to broaden the scope of the current NIS Directive by covering more companies in existing sectors as well as including additional sectors. The present categories of operators of essential services and digital service providers are to be replaced by important and essential entities. Currently, companies subject to NIS obligations are identified by decisions of national competent authorities. In contrast, the proposal introduces a single criterion for companies in the listed sectors, according to which they are to be primarily identified *ipso iure*—a company’s size. The author gives an overview of the main provisions and highlights the principal challenges associated with the proposed changes to the NIS regulatory regime.

Keywords NIS Directive 2.0 · NIS2 · NIS · Directive (EU) 2016/1148 · Network and Information Systems Directive · Size-cap rule · KRITIS

The author is a policy officer with the German Federal Ministry of the Interior, Building and Community. Any views and opinions expressed in this contribution are solely those of the author.

Thomas Sievers (✉)
Berlin, Germany
E-Mail: thomas.sievers@me.com

Vorschlag für eine NIS-Richtlinie 2.0 – vom erweiterten Anwendungsbereich erfasste Unternehmen und ihre Verpflichtungen

1 Introduction and context

In the last couple of years, cybersecurity incidents have become a virtually ubiquitous item in the daily news, with ransomware attacks gaining notoriety with double-digit million dollar claims.¹ This impression is supported by cyber threat landscape reports.² In light of the increased digitalization of the economy and dependency on digitalization amplified by the Covid-19 pandemic, the European Commission (EC) in its Cybersecurity Strategy reiterated the call to revise the EU's cybersecurity legislation.³

The Network and Information Security Directive (NIS1)⁴ was the first piece of EU legislation on cybersecurity. Its specific aim was to achieve a high common level of cybersecurity across all EU Member States. Among other things, the regulatory regime established by NIS1 required EU Member States to make an assessment of which “entities” provide in their economy “a service which is essential for the maintenance of critical societal and/or economic activities” in certain sectors of the economy and identify the respective operators of essential services (OES). National legislation transposing NIS1 was to subject these OES to cybersecurity requirements as well as notification obligations with respect to cybersecurity incidents.⁵

The proposal by the EC for a revised NIS Directive⁶ (NIS2) greatly widens the scope of application of NIS1 to cover more entities in existing sectors of the economy as well as including new sectors. Like NIS1, the NIS2 text speaks of “entities” as regulatory subjects. While in practice most will be companies, natural persons would

¹ A high profile example of Summer 2021 includes the *Colonial Pipeline* incident, cf. *NYT*, Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity (08.06.2021), accessible at <https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html>.

² For a situational report of cybersecurity in Germany (in German), cf. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2020 (20.10.2020), accessible at <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.html>.

³ cf. *European Commission/High Representative of the Union for Foreign Affairs and Security Policy*, Joint Communication to the European Parliament and the Council—The EU's Cybersecurity Strategy for the Digital Decade (16.12.2020), EU-doc. JOIN (2020) 18 final, p. 1 and 5.

⁴ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.07.2016, p. 1—so called “NIS Directive” or “NIS1” for short.

⁵ Germany, for example, has primarily transposed NIS1 in the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik—BSI-Gesetz*), BGBl. I 2009 p. 2821; for a comprehensive overview (in German) cf. *Beucher/Fromageau* in Kipker (Ed.), *Cybersecurity*, 2020, p. 358 *et. seq.*

⁶ Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148—EU-doc. COM (2020) 823 final, dated 16 December 2020—so called “NIS Directive 2.0” or “NIS2” for short.

also be included in this definition.⁷ This contribution will focus on those provisions of NIS2 that address the question of which entities are in its scope of application and which kinds of obligations these entities will face. Other matters included in NIS2, namely obligations for EU Member States and cooperation amongst Member States or between them and the EC or the European Network and Information Security Agency (ENISA), will not be addressed in this contribution.

The implementation period of NIS1 was 22 months, and EU Member States had an additional six months to identify OES, i.e. until 9 November 2018.⁸ The EC carried out an evaluation of the functioning of NIS1 starting in mid-2019.⁹ Among its findings were that the scope of NIS1 was not covering all sectors providing key services to economy and society. Furthermore, NIS1 was deemed to have granted too wide powers of a discretion for EU Member States to mandate the kinds of cybersecurity and incident reporting requirements for OES, and NIS1 was considered not to include effective supervision and enforcement. Thus, the EC's main objectives for NIS2 are to cover a larger share of the economy and society by including more sectors, to replace the identification process established in NIS1, and to create a higher level of harmonization regarding security requirements and reporting obligations.¹⁰

2 The proposed revision to the NIS regulatory regime

In a first step, it will be examined which entities are in the scope of NIS2. In a second step, the obligations of those entities and their supervision will be considered.

2.1 Identification and new categories

2.1.1 Self-identification

By design, NIS2 does not contain a mechanism like Article 5 NIS1 that enabled EU Member States to identify those entities that are to fall within the scope of the directive pursuant to a set of criticality criteria.¹¹ According to the evaluation of NIS1 performed by the EC, the EU Member States carried out the identification process with employing varying amounts of resources. This led to different “levels

⁷ According to the newly included definition in Article 4 no. 24 NIS2, the term “entity” means “any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations”.

⁸ Cf. Article 25 para. 1 NIS1 (transposition period) and Article 5 para. 1 NIS1 (identification deadline).

⁹ Cf. EC, Evaluation Report, Annex 5 to Impact Assessment Report, EU-doc. SWD (2020) 345 final, Part 2/3, p. 81 *et seq.*

¹⁰ Cf. EC, NIS2 Explanatory Memorandum, EU-doc. COM (2020) 823 final, p. 7.

¹¹ Germany, for example, has enshrined the criteria (or thresholds) by which OES are determined in the ordinance on the determination of critical infrastructures pursuant to the act on the Federal Office for Information Security (*Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz—BSI-KritisV*).

of maturity in dealing with cybersecurity risks”.¹² Furthermore, the EC considers the NIS1 identification process to be “complex”.¹³ Therefore, the scope of NIS2 is determined by a single criterion that is to be applied across all EU Member States. This criterion was determined to be an entity’s size. While the EC itself admits that this criterion is “not necessarily an ideal stand-alone criterion to determine the importance and/or criticality” of an entity, the EC nevertheless reasons it to be a “meaningful proxy” in order to determine whether certain entities have key roles for society and economies.¹⁴

Pursuant to the central provision of Article 2 para. 1 NIS2, a company is within the scope of the directive if it belongs to one of the economic sectors listed in its Annexes I and II—see “Important and Essential Entities” below for further details—and is not considered a micro or small enterprise. This generally leads to the exclusion of any entity that employs fewer than 50 employees and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.¹⁵ This so-called “size-cap rule”¹⁶ would require companies to determine for themselves whether they are in the scope of NIS2, as a determination by the national competent authority (NCA)¹⁷ is no longer required.

Some entities excluded by the size-cap rule may still be in the scope of application. Article 2 para. 2 NIS2 lists five types of entities for which the size-cap rule does not apply at all (letters a, b, and g) and four non-cumulative criteria (letters c through f), in which case a company is in the scope of NIS2 regardless of the size-cap rule.¹⁸ While the types of entities are straightforward, the criteria (letters c through f) are less so. Article 2 para. 2 (c) NIS2, for example, could potentially result in the inclusion of such producers with only few employees and an annual turnover below 10 million who—while being the sole producer of a good in an EU Member State—produce a good that would generally not be considered as critical.

¹² See EC, NIS2 Explanatory Memorandum, EU-doc. COM (2020) 823 final, p. 5.

¹³ See EC, NIS2 Explanatory Memorandum, EU-doc. COM (2020) 823 final, p. 8.

¹⁴ Cf. EC, Impact Assessment Report, EU-doc. SWD (2020) 345 final, Part 1/3, p. 60.

¹⁵ See Article 2 para. 1 sentence 2 NIS2 together with Article 2 para. 2 in Annex to Commission Recommendation 2003/361/EC of 6 May 2003, OJ L 124, 20.05.2003, p. 36. Since the original purpose of the recommendation was to support SMEs, subsidiaries are effectively excluded from being considered micro or small enterprises. For example, in the case of a company where 25% or more of the capital or voting rights are held by a parent company, then the headcount and financials are generally determined by the consolidated accounts, cf. Article 3 para. 2 and Article 6 para. 2 in Annex to Commission Recommendation 2003/361/EC.

¹⁶ The term was coined in Recital 8 NIS2 and is also widely used in the EC’s impact assessment on NIS2, cf. EC, Impact Assessment Report, EU-doc. SWD (2020) 345 final, Part 1/3, p. 59.

¹⁷ EU Member States are required by Article 8 para. 1 NIS1 (see also Article 7 para. 4 NIS2) to designate an NCA. In Germany, the designated NCA is the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*—BSI).

¹⁸ While EU Member States are to compile a “list of the entities identified” pursuant to the criteria according to Article 2 para. 2 sentence 2, the wording of Article 2 para. 2 sentence 1 appears to clearly suggest that NIS2 is to apply *ipso iure* to such companies (“this Directive also applies”). This is supported by Recital 9 NIS2.

The extension of NIS2 to more sectors, together with the size-cap rule, leads to a significant increase in the number of entities covered. This increase is estimated to be seven-fold.¹⁹

2.1.2 Important and essential entities

The NIS1 terms OES and digital service providers (DSPs) are completely replaced by the two NIS2 categories called “important entities” and “essential entities”. The allocation of an entity to either category is determined by the sector being listed in Annex I (essential entities) or Annex II (important entities). Therefore, all entities belonging to a sector are automatically allocated to that category. The kinds of sectors and sub-sectors in NIS2 were expanded in comparison to NIS1; for an overview please refer to Table 1 below.

The annexes include references to EU legislation containing the definition of a certain group of entities. Although this may be burdensome to the legal practitioner to find the referenced definitions, it does have the advantage that such definitions are—in most cases—established and quite clear. By way of deletion in other legal acts, cybersecurity requirements and notification obligations for trust service providers in eIDAS and electronic communication providers²⁰ in EECC are

Table 1 Comparison of sectors under NIS1 (not in bold) and NIS2 (in bold); sub-sectors in parenthesis. The order of the listed (sub-)sectors corresponds to the one in the NIS2 Annexes

Essential entities	Important entities
<ul style="list-style-type: none"> – Energy (electricity—now including production; aggregation; demand response and energy storage; electricity markets—; district heating; oil; gas and hydrogen) – Transport (air; rail; water; road) – Banking – Financial market infrastructures – Health (healthcare; EU reference labs; research and manufacturing of pharmaceuticals and medical devices) – Drinking water – Waste water – Digital infrastructure (IXP; DNS; TLD; cloud; data centre service providers; CDN; trust service providers; electronic communications) – Public administrations – Space 	<ul style="list-style-type: none"> – Postal and courier services – Waste management – Chemicals (manufacture; production; distribution) – Food (production; processing; distribution) – Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment) – Digital providers (online marketplaces; search engines; social networks)

¹⁹ The EC’s impact assessment gives the current number of OES identified by EU Member States as roughly 15,500 and estimates the number of companies in the scope of NIS2 as roughly 110,000 across the entire EU, cf. EC, Impact Assessment Report, EU-doc. SWD (2020) 345 final, Part 1/3, p. 20, 70.

²⁰ In this regard also in this issue of ICLR: Gruber A, Ségur-Cabanac N (2021) Necessary or premature? The NIS 2 Directive from the perspective of the telecommunications sector.

transferred to NIS2.²¹ However, in some sectors the definitions chosen could be considered quite broad.²²

2.2 Obligations and supervision

Having established the entities in the scope of NIS2, this contribution will now consider what cybersecurity requirements and reporting obligations the entities newly in scope will face, as well as what will change for entities currently in scope in this regard. Furthermore, the supervision and sanction provisions will be summarized.

2.2.1 Cybersecurity requirements and reporting obligations

Recital 11, Article 18 and 20 NIS2 make it clear that entities in both categories—important entities and essential entities—are subject to the same cybersecurity requirements and reporting obligations.²³ Article 18 para. 1 NIS2 closely resembles Article 14 para. 1 NIS1 and also references “appropriate and proportionate” measures as well as the standard of “state of the art”. A novelty in comparison to NIS1 is the inclusion of a catalogue of the measures that entities will have to observe at a minimum in Article 18 para. 2. They include (a) risk analysis and information system security policies; (b) incident handling (prevention, detection, and response to incidents); (c) business continuity and crisis management; (d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services; (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; (f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures; and (g) the use of cryptography and encryption. Also new in the NIS regulatory regime is the responsibility and accountability of management bodies and their members for the compliance with cybersecurity requirements.²⁴ In order

²¹ Article 39 and 40 NIS2 delete the sector-specific cybersecurity requirements and reporting obligations for trust service providers under Article 19 of Regulation (EU) No 910/2014 (so-called “eIDAS”) and electronic communication providers under Articles 40 and 41 of Directive (EU) 2018/1972 (so-called “European Electronic Communications Code” or “EECC” for short) respectively. Thereby the cybersecurity requirements and reporting obligations of NIS2 will apply for these types of entities as they are listed in Annex I, no. 8, dash 7 and 8 respectively.

²² For example, the term “food business” in the meaning of the EU legislation referenced in Annex II point 4 NIS2 is defined as “any undertaking, whether for profit or not and whether public or private, carrying out any of the activities related to any stage of production, processing and distribution of food”. On the other hand, under the NIS1 transposition act currently in force in Germany, the food supply sector only covers such entities that pass the listed thresholds for food and beverages, cf. section 4 para. 3 and Annex 3 part 3 BSI-KritisV. For example, a production plant will need to produce at least 434,500 tons of food or 350 million litres of beverages annually in order to be in scope, cf. Annex 3 part 3 no. 1.1.1 BSI-KritisV.

²³ The difference between the two categories lies only in supervisory and penalty regimes, see “Supervision and Sanction” below.

²⁴ While the general rule is included in Article 17 NIS2, the provision on respective sanctions will be considered in “Supervision and Sanction” below.

to demonstrate compliance with certain cybersecurity requirements, EU Member States may, pursuant to Article 21 para. 1 NIS2, require essential and important entities to have certain information and communications technology (ICT) products, services and processes certified in accordance with the cybersecurity certification schemes adopted pursuant to Art. 49 CSA. This also includes products and services furnished by third parties. The EC is empowered under Article 21 para. 2 NIS2 to specify which types of essential and important entities must obtain certification in accordance with para. 1.

With regard to reporting obligations, the generalized obligation in Article 14 para. 3 NIS1 is replaced with a detailed and tiered plan in Article 20 para. 4 NIS2. Incidents having a significant impact on an entity's services have to be notified to the EU Member State's authorities (i) within 24h at the latest (initial notification), (ii) upon request of the authorities (intermediate report) and (iii) no later than one month after the initial notification (final report).

2.2.2 Supervision and sanction

The only differentiation between important and essential entities provided by NIS2 is in the manner of supervision. For this purpose, NIS2 differentiates between *ex ante* supervision, i.e. the taking of supervisory measures in advance and *ex post* supervision, i.e. taking supervisory action when provided with evidence or an indication that an entity does not meet the cybersecurity and incident notification requirements. Essential entities are subject to a “fully-fledged”²⁵ supervisory regime (*ex ante* and *ex post*), while important entities are subject to a “light”²⁶ supervisory regime (*ex post* only). Necessarily, supervision of essential entities includes for example “regular audits” in Article 29 para. 2 (b) NIS2, while Article 30 (b) NIS2 with regard to important entities includes “targeted security audits based on risk assessments or risk-related available information” only.

A new measure is introduced in NIS2 with regard to the members of management bodies of entities. Under certain circumstances NCAs may levy a professional ban on management personnel of essential entities (see Article 29 para. 5 (b) NIS2), and management personnel may be “held liable for breach of their duties to ensure compliance with the obligations laid down” in NIS2 (see Article 29 para. 6 NIS2). However, the wording of both provisions could be construed in different ways, i.e. which natural persons should be covered and what legal nature the liability for breach of duty is supposed to have. The latter provision could be read to mean a civil law liability to third parties, which would mean a piercing of the corporate veil, something quite rare in many legal systems in the EU. However, it could also be construed to mean a liability of the natural person *vis-à-vis* the essential entity in the context of the employee/employer relationship.

The general clause on administrative fines resembles in principle Article 83 GDPR. Article 31 para. 4 NIS2 includes a severe maximum fine of EUR 10 million as well as a fine calculated by up to 2% of total worldwide (group) annual turnover.

²⁵ Cf. Recital 70 sentence 3 NIS2.

²⁶ Cf. Recital 70 sentence 3 NIS2.

3 Key challenges for NIS2 and current status

3.1 Challenges for entities and supervision

There appear to be two central challenges in connection with NIS2 that were identified in this contribution: the material switch from an identification process to the singular size criterion across the EU to determine the scope of application and the consequences arising therefrom for (i) entities and (ii) supervision.

The EC has provided an estimate of the average increases in ICT spending for entities in the first three to four years following the implementation of NIS2. For entities newly in scope of NIS2 the EC estimates cost increases of about 0.63% of the entity's total turnover.²⁷ For entities currently in scope of NIS1, the EC estimates cost increases of 0.58% of the entity's total turnover.²⁸ The main cost driver in NIS2 for ICT spending would evidently be the cybersecurity requirements.²⁹ Still, some entities will have invested in ICT of their own volition and in such cases cost increases would of course be lower than the estimates given above. Since NIS2 does not differentiate cybersecurity requirements between its two categories, the cost estimates are identical for essential and important entities. It could prove beneficial to also differentiate the cybersecurity requirements between the two categories.

The approach to supervision will necessarily change from NIS1 to NIS2, given the estimated seven-fold increase in the number of entities to be supervised. If NCAs are to continue their supervision activities at the same level of intensity with essential entities under NIS2 as with OES under NIS1, NCAs will require corresponding financial and human resources even if the identification process were to be omitted.³⁰ In order to know the identities of entities to be supervised, NCAs would necessarily need to make an assessment in this regard. Whether the removal of the identification process will prove less burdensome and lead to freeing up capacities at NCAs remains to be seen. The need for NCAs to know the identity of the entities they are to supervise may still require considerable resources.

3.2 Current status of NIS2

The proposal is subject to the ordinary legislative procedure. After the presentation of the proposal by the EC on 16 December 2020, the Council and the European Parliament (EP) are called upon as co-legislators. Pursuant to Article 294 TFEU, both co-legislators may adopt the proposal at first or second reading. If both the Council and the EP have not achieved a consensus, a conciliation committee would be created. However, it is standard practice nowadays that for the adoption of EU legislation, interinstitutional negotiations between the Council, EP and EC (so-called

²⁷ Cf. EC, Impact Assessment Report, EU-doc. SWD (2020) 345 final, Part 1/3, p. 72.

²⁸ Cf. EC, Impact Assessment Report, EU-doc. SWD (2020) 345 final, Part 1/3, p. 73.

²⁹ Cf. EC, Impact Assessment Report, EU-doc. SWD (2020) 345 final, Part 1/3, p. 74.

³⁰ The EC estimates cost increases of 20–30% with NCAs, cf. EC, Impact Assessment Report, EU-doc. SWD (2020) 345 final, Part 1/3, p. 83.

“trilogues”) are conducted usually before the first reading.³¹ For this purpose, each co-legislator adopts a mandate for negotiations in the trilogue. In the case of the EP, the mandate is usually based on a report adopted in committee and in the case of the Council the mandate is typically in the form of a general approach, including the main positions of the Council.

The first draft of the report by the rapporteur in the Committee on Industry, Research and Energy (ITRE) is publicly available and includes 91 proposed amendments on a host of issues.³² On the side of the Council, in the discussions within the Council Horizontal Working Group on Cyber Issues (HWPCI) EU Member States broadly welcomed the revised directive, while raising a number of concerns, according to a press release.³³ The press release mentions concerns of EU Member States regarding the interaction of NIS2 with sectoral legislation like CER³⁴ and DORA³⁵, as well as the “significant expansion of the scope” and the size-cap criterion as the “sole element to be considered when identifying essential and important entities to be covered”.

4 Conclusion

In summary, the work on NIS2 by the co-legislators is currently progressing. Each co-legislator appears to have a number of amendments that will have to be agreed upon during trilogue. If enacted as originally proposed, NIS2 will bring a significant extension of the scope of application and with it, it will have considerable impacts on the entities themselves and their supervision. That said, the original NIS1 proposal took more than three years before adoption; as such, it remains to be seen how much time negotiations will require for NIS2 to be finally adopted.³⁶

³¹ Roughly 85% of EU legislation during the parliamentary term 2009–2014 was passed on first reading after a preceding trilogue, cf. *European Ombudsman*, Decision on case OI/8/2015/JAS (12.07.2016), no. 18.

³² *Bart Groothuis*, Draft report on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (03.05.2021), available at https://www.europarl.europa.eu/doceo/document/ITRE-PR-692602_EN.pdf.

³³ *General Secretariat of the Council, Press office*, Background on TTE Council 4 June (31 May 2021), p. 3, available at: https://www.consilium.europa.eu/media/50000/background-brief-telecoms_en-june-2021.pdf.

³⁴ Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, EU-doc. COM (2020) 829 final (16.12.2020)—so-called “critical entities resilience directive” or “CER” for short.

³⁵ Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, EU-doc. COM (2020) 595 final (24.09.2020)—so-called “DORA” for short.

³⁶ NIS1 was adopted on 6 July 2016; it had been originally proposed by the EC on 7 February 2013, cf. *EC*, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, EU-doc. COM/2013/048 final (07.02.2013).