Published on *The National Law Review* https://natlawreview.com

Happy NIS Year, Everyone! A New Common Cybersecurity Framework for the European Union

Article By:

Dr. Thomas Nietsch

Dr. Ulrike Elteste

The European Parliament and Council dropped an early Christmas present on all stakeholders in the digital environment and critical infrastructure that may feel to some like a bit of coal in the stocking, as it will require significant new investments and efforts.

On 14 December 2022 the EU's Official Journal published the new EU Directive 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2) - this will take effect on 17 January 2023 (and also repeals the prior NIS Directive 2016/1148). Like the previous NIS Directive, the aim of NIS2 is to ensure a high common level of cybersecurity across the European Union (EU), but it broadens the scope to additional relevant sectors and introduces new obligations, forming part of a wider EU effort to strengthen the resilience of European infrastructure, including the draft Cyber Resilience Act (CRA) and the EU Regulation 2022/2554 on digital operational resilience for the financial sector (DORA) (see our respective alert here). This trend does not only manifest in Europe but we see various cybersecurity regulation efforts around the world, for instance in the US, China and Australia.

Especially in post-COVID times, the increased reliance on digital infrastructure led to increasing numbers of large scale cyber-attacks, leaks and outages, leading to both material monetary and reputational damage as well as to significant economic damages and negative societal impacts, a trend further accelerated by fallout from the war in Ukraine. The ever-evolving digital landscape and new threats to the respective systems call for a modernized regime to improve resilience, integrity, confidentiality and availability. The review process for NIS Directive 2016/1148 also revealed a divergence in application of its requirements across the EU member states, which increased the need for a more harmonized EU-wide regulation.

- To strengthen cooperation between member states, NIS2 sets up an EU-wide coordination group to improve information exchange among the member states.

- In addition, member states are required to set up a robust administrative framework by establishing a national cybersecurity strategy and competent supervisory authorities as well as one or more Computer Security Incident Response Teams (CSIRTs) that are intended to

work together to develop coordinated vulnerability disclosures which must be bundled at the European Union Agency for Cybersecurity (ENISA).

Exchange of relevant information among member states and EU bodies is one key focus of NIS2, as most cyber threats are supranational and insufficient information flows, hindered by national vs. EU-level approaches, often lead to fragmentary threat responses. These (partly new) public structures under NIS2 emphasize that cyber security is not merely a task of (private) operators of infrastructure or service providers, but that also a harmonized public infrastructure is required to protect the European economy and society across borders. Nonetheless, this alert focuses on private entities' obligations as these will have to assess potential new obligations and may be subject to material fines.

The new NIS2 framework will form the general basis of cyber security in the EU going forward, and will, as such, provide for a minimum harmonization allowing member states to provide for a higher level of cyber security. Having said this, regulated entities should, on the basis of risk-based assessments, look at adopting stricter or modified rules in line with potentially stricter requirements in their respective country of establishment.

WHO IS AFFECTED?

NIS2 generally applies to all types of public or private entities listed in its Annex I or II and providing services or operating in the EU. Thus, NIS2 is not limited to a local establishment or other entities simply having a similar physical basis in the EU, but goes beyond that. Annex I comprises the following sectors:

- Energy;
- Transport;
- Banking and other financial market infrastructures;
- Health;
- Drinking and waste water;
- Digital infrastructure (including internet exchange points, domain name system (DNS) service providers, top level domain (TLD) name registries, cloud computing service providers, data center service providers, content delivery network providers, trust service providers, providers of public electronic communications networks and respective services);
- Information and communication technology (ICT) service management (B2B);
- Public administration; and
- Space.

Annex II comprises:

- Postal and courier services;
- Waste management;
- Manufacture;
- Production and distribution of chemicals and food;
- Manufacturing;
- Digital providers (online marketplace providers, online search engine operators, online social network operators); and
- Research.

Limited Exceptions for Micro and Small Entities

NIS2 does exempt micro and small entities from its scope, unless these have a key role for the economies or societies of member states, such as operators of public electronic communication networks or providers of respective services, trust service providers or TLD name registries, DNS service providers and critical entities according to EU Directive 2022/2557. Pursuant to EU Commission Recommendation 2003/361, micro and small entities are those employing fewer than 50 persons and having an annual turnover or annual balance sheet of not more than EUR 10 million.

NIS2 Implements a Two-Level Prioritization Approach

Within this group of regulated entities, NIS2 provides for a two-level approach for private entities, distinguishing between:

1. Essential entities being

- Of a type listed in Annex I of the NIS2 Directive and exceeding thresholds for medium sized entities (more than 50 employees and annual turnover exceeding EUR 10 million);
- Qualified trust service providers;
- TLD registries and DNS service providers;
- Public electronic communications networks operators or respective service providers;
- Public administration bodies;
- Those types of entities listed in Annex I or II and identified by a member state as essential (or having already been identified under the previous NIS Directive)
- Critical entities according to EU Commission Recommendation 2003/361.

2. Important Entities being any other types of entities listed in Annex I or II of NIS2 that do not fall in

the scope of essential entities.

This approach limits the room to maneuver that member states have to determine which sectors are critical and should be regulated, which was apparently an issue under the previous NIS Directive leading to the above mentioned divergence in application. However, it should be noted that this distinction does not affect the core obligations of the regulated entities under NIS2 but only the public oversight mechanism (see below).

NIS2 does not directly apply to manufacturers of IT hardware and software but regulated entities will have to consider existing products when implementing these in their services. Further, it is possible for the EU Commission or member states to require use of hardware and software products meeting certain standards. To some extent, IT hardware requirements are also covered in other regulatory schemes, such as the aforementioned DORA.

WHAT NEEDS TO BE DONE?

Unlike an EU regulation, NIS2, as a directive, does not apply directly to regulated entities, but rather obliges the EU member states to transpose the provisions of the directive into their respective national laws. Once a member state has implemented NIS2, entities which fall within the scope of NIS2 will need to implement adequate and proportionate technical, operational and organizational measures to manage cyber security risks posed to the security of network and information systems. These entities are also under the obligation to notify the national competent authorities or CSIRTs of any cyber security incident having a significant impact on the provisions of the services they provide. The below provides a high level summary of obligations, but regulated entities should be aware that these may be further modified and detailed in the course of each member state implementing the NIS2 into their respective national laws. National laws can be stricter but never less strict than the EU Directive. It remains to be seen how such local requirements, from different member states, may superimpose onto one another for multinational companies.

The applicable cybersecurity risk management measures are, by nature, only described in generic terms and only some examples of measures are expressly called out in NIS2, such as

- Incident handling,
- Business continuity and crisis management,
- Supply chain security,
- Policies and procedures to assess effectiveness of implemented measures,
- The use of encryption,
- Cyber security trainings or
- Access control policies.

As a general rule, and similar to cyber security obligations under other legal frameworks such as GDPR (Art. 32) and the previous NIS Directive, a regulated company must assess the potential risks related to its operations in case of an incident and implement respective safeguards considered

adequate to counter these risks, taking into account state of the art, applicable international or European standards (e.g., ISO standards), costs, risk exposure as well as likelihood and severity of potential damages. This generic regulatory approach has the advantage that it can be tailored to specific industries and allows for a broad range of entities to be regulated. On the other hand, the regulated entities will need to expend greater efforts to identify potential risks and threat scenarios and determine adequate mitigation measures. To minimize the resulting uncertainties and provide stakeholders with much needed legal foreseeability, the EU Commission has the right (and in some cases the obligation) to adopt additional implementing acts regarding technical and methodological specifications for digital service providers.

Cybersecurity incidents having a significant impact on NIS2-covered entities will now need to be reported to the local supervisory authority or CSIRT without undue delay and, where appropriate also to the affected recipients of these services, including information on how these can mitigate the risks and damages (and without prejudice to other breach reporting requirements, such as under Art. 33 et seq. GDPR). In certain cases, a public notification can also be required. An initial notification (early warning) will need to be delivered to the competent authority or CSIRT within 24 hours after becoming aware of the incident. The CSIRT in turn must respond within another 24 hours, to offer feedback and support. Within 72 hours of becoming aware of the incident a more detailed incident report needs to be delivered and, within one month after this incident report, a final report. To assist digital service providers, the EU Commission has the right (and in some cases the obligation) to, by way of an implementing act, specify which incident should be considered significant. In order to encourage such transparency, the member states will need to ensure, in their national law implementation, that the mere act of notification will not increase the liability of the notifying entity. These disclosure obligations mirror those being adopted by other jurisdictions, including in the United States for financial institutions and critical infrastructure, hence larger multi-national enterprises may be able to begin adopting enterprise-wide incident response and disclosure approaches that satisfy multiple jurisdictions.

Again, it is worth mentioning that the risk management measures and notification obligations are basically identical for essential entities and important entities. The distinction of these two categories is only relevant for the supervision and enforcement (see below).

TLD registries or operators of domain name registration services for TLDs will be obliged to maintain accurate and complete domain name registration data, publish such data excluding personal data and grant access to such data (including personal data) for legitimate access seekers without undue delay in accordance with European data protection laws.

ENISA will be required to create a database of essential and important entities and, for that purpose, the national supervisory authorities must oblige all digital service providers regulated under NIS2 to provide core company and contact details by 17 January 2025.

For the first time, NIS2 requires that management bodies of regulated entities approve the cyber security risk management measures of their respective entity, supervise their implementation, and adopt personally accountability for non-compliance with the obligations of NIS2. In order to strengthen the expertise of management body members, they will need to attend regular cyber security trainings. By this move, the regulator makes cyber security a management topic and managers are well advised to focus on cybersecurity matters themselves rather than delegating the task.

WHAT IS THE TIMELINE FOR IMPLEMENTATION?

EU member states have until 17 October 2024 to implement the local laws necessary to comply with NIS2, to meet the deadline to be in force on 18 October 2024. Before then, even though regulated entities will not yet be bound by NIS2, it is highly advisable that companies in the relevant sectors, in particular the broad field of digital service providers, closely follow the national transposition process and the expected clarifications from the EU Commission and prepare for compliance, given the complexities and ambiguities in the technical details of NIS2. This should also include a comparison for overlaps with already existing obligations, e.g. under GDPR or sector-specific regulations.

HOW WILL NIS2 BE ENFORCED?

EU member states will monitor and enforce NIS2 through a combination of new or expanded competent national (or regional) supervisory authorities.

Importantly, NIS2 divides the competences of supervisory authorities: essential entities are subject to an ex ante supervision, while important entities are, at least in some cases, only subject to an ex post supervision. This means that supervisory authorities may make use of their statutory supervision powers (e.g., audits, inspections, information requests) towards essential entities without a specific suspicion, while their statutory powers are limited towards important entities to cases where there is an indication that a breach may have occurred. However, the ex post supervisory approach to important entities is not consistently applied in NIS2, as only some of the provisions are expressly deleted or made subject to an ex post qualifier.

Importantly, enforcement powers are integral to NIS2 - if an essential or important entity does not comply with an instruction within a reasonable deadline, the competent supervisory authority may suspend any licenses or impose a ban of the involved responsive personnel from any managerial activities. This emphasizes again the relevance for managers to be directly involved in cybersecurity matters.

As stated above, member states still hold a certain margin of interpretation on how NIS2 will be implemented, and this leverage also encompasses the effective, proportionate and dissuasive administrative fines in case of breach of NIS2 undertakings. Member states are however bound by minimal fines capped at “at least” (each time, whichever is higher):

- *For Essential Entities*: EUR 10,000,000 or 2% of the total worldwide annual turnover of the undertaking; or
- *For Important Entities*: EUR 7,000,000 or 1.4% of the total worldwide annual turnover.

The term “at least” suggests that member states are free to establish higher caps.

As a general rule, regulated entities fall under the jurisdiction of the member state where they have their main establishment (if there is more than one establishment in the EU). Where a digital service provider has no establishment in the EU despite offering services in the EU, it will need to appoint a local representative established in a member state where the services are offered (following in the footsteps of the too often overlooked Art. 27 GDPR), and similar to the requirements in DORA. Where no representative is appointed, any member state in which the services are provided may take legal action.

HOW DOES NIS2 INTERACT WITH OTHER LEGAL FRAMEWORKS ON EU LEVEL?

Several other legal acts of the EU also address cyber security topics for specific sectors. These sector-specific regulations shall continue to apply as leges speciales to the extent they provide for security measures and reporting obligations having at least an equivalent effect. Such is the case for DORA for the finance sector.

In contrast to NIS2 , the CRA applies to certain products with digital elements and, despite certain overlaps, both cover a separate area of cybersecurity.

As in most other newer EU acts of legislation, all obligations apply subject to GDPR, i.e., all obligations must be complied with in a way that also complies with GDPR, provided that personal data is involved (which will be most likely). As for fines that may be issued under NIS2 , it is at least clarified in Art.35 NIS2 that if a fine is issued under GDPR for data breach, no fine under the NIS2 framework should be issued for the same infringement (however, without prejudice to injunctive measures the NIS2 supervisory authority may implement).

National Law Review, Volumess XIII, Number 13