NIS2 Directive

Why did the Commission propose a new NIS Directive?

The NIS Directive— the first EU cybersecurity law — is the first horizontal internal market instrument aimed at improving the resilience of network and information systems in the Union against cybersecurity risks. Despite its notable achievements, the NIS Directive has shown certain limitations. The digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape. New challenges have appeared, which require adapted and innovative responses.

To be able to analyse the impact and identify the deficiencies of the NIS Directive, the Commission carried out an extensive stakeholder consultation. The Commission identified the following main issues:

- insufficient level of cyber resilience of businesses operating in the EU
- inconsistent resilience across Member States and sectors
- insufficient common understanding of the main threats and challenges among Member States
- lack of joint crisis response.

As a result, and in order to respond to the growing threats due to digitalisation and interconnectedness, in December 2020 the Commission proposed a revised set of future-proof rules aiming to strengthen the level of cyber resilience in the Union, on which the co-legislators have reached a political agreement on 13 May 2022 and formally adopted the new Directive in late November 2022.

How has the COVID-19 crisis influenced the new Directive?

Since the COVID-19 crisis, the European economy has grown more dependent on digital solutions than ever before. Sectors and services are becoming increasingly interconnected and interdependent. This has resulted in a growing and rapidly evolving cybersecurity threat landscape: any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the whole internal market.

The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of unexpected risks. It intensified the already emerging issues in the current NIS Directive and served as a catalyst for its revision. A concrete change to the NIS Directive in view of this crisis was to expand the scope of the new Directive, covering more specific elements in the health sector, such as entities carrying out research and development activities of medicinal products.

What elements of the previous NIS Directive does the NIS2 Directive build on?

The NIS2 Directive provides legal measures to boost the overall level of cybersecurity in the EU, in order to contribute to the overall functioning of the internal market. It builds on the 3 main pillars that were the basis of the NIS1 Directive:

1. Building on the NIS1 strategy on the security of network and information systems, in order to achieve a high level of preparedness of Member States, the NIS2 Directive requires Member States to adopt a national cybersecurity strategy. Member States are also required to designate national Computer Security Incident Response Teams (CSIRTs), who are responsible for risk and incident handling, a competent national cybersecurity authority, and a single point of contact (SPOC). The SPOC has to exercise a liaison function to ensure cross-border cooperation between the Member State authorities with the relevant authorities in other Member States and, where appropriate with the Commission and ENISA as well as to ensure cross-sectorial cooperation with other competent authorities within its Member State.
2. The NIS2 Directive also continues the NIS1 framework establishing the NIS Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States, and the CSIRTs Network,

which promotes swift and effective operational cooperation between national CSIRTs.
3. The NIS1 Directive ensures that cybersecurity measures are taken across seven sectors, which are vital for our economy and society and which rely heavily on ICT, such as energy, transport, banking, financial market infrastructures, drinking water, healthcare and digital infrastructure

Public and private entities identified by the Member States as operators of essential services (OES) in these sectors are required to undertake a cybersecurity risk assessment and put in place appropriate and proportionate security measures. They are required to notify serious incidents to the relevant authorities. Furthermore, providers of key digital services (digital service providers or DSPs), such as search engines, cloud computing services and online marketplaces, have also to comply with the security and notification requirements under the Directive. At the same time, the latter are subject to a so-called 'light-touch' regulatory regime, which entails that those entities are not subjected to ex-ante supervisory measures.

NIS2 Directive significantly expands the scope of sectors and introduces a size threshold to define which entities fall in its scope and would be required to report significant cybersecurity incidents to the national competent authorities.

What are the key elements of the NIS2 Directive?

The NIS2 Directive aims to address the deficiencies of the previous rules, to adapt it to the current needs and make it future-proof.

To this end, the Directive expands the scope of the previous rules by adding new sectors based on their degree of digitalisation and interconnectedness and how crucial they are for the economy and society, by introducing a clear size threshold rule— meaning that all medium and large-sized companies in selected sectors will be included in the scope. At the same time, it leaves certain discretion to Member States to identify smaller entities with a high security risk profile that should also be covered by the obligations of the new Directive.

The new Directive also eliminates the distinction between operators of essential services and digital service providers. Entities would be classified based on their importance, and divided into two categories: essential and important entities, which will be subjected to different supervisory regime.

It strengthens and streamlines security and reporting requirements for companies by imposing a risk management approach, which provides a minimum list of basic security elements that have to be applied. The new Directive introduces more precise provisions on the process for incident reporting, content of the reports and timelines.

Furthermore, NIS2 addresses security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in the supply chains and supplier relationships. At European level, the Directive strengthens supply chain cybersecurity for key information and communication technologies. Member States in cooperation with the Commission and ENISA, may carry out Union level coordinated security risk assessments of critical supply chains, building on the successful approach taken in the context of the Commission Recommendation on Cybersecurity of 5G networks.

The Directive introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States.

It also enhances the role of the Cooperation Group in shaping strategic policy decisions and increases information sharing and cooperation between Member State authorities. It also enhances operational cooperation within the CSIRT network and establishes the European cyber crisis liaison organisation network (EU-CyCLONe) to support the coordinated management of large-scale cybersecurity incidents and crises.

NIS2 also establishes a basic framework with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creates an EU vulnerability database for publicly known vulnerabilities in ICT products and ICT services, to be operated and maintained by the EU agency for cybersecurity (ENISA).

Which sectors and types of entities will the NIS2 cover?

The NIS2 covers entities from the following sectors:

Sectors of high criticality: energy (electricity, district heating and cooling, oil, gas and hydrogen); transport (air, rail, water and road); banking; financial market infrastructures; health including manufacture of pharmaceutical products including vaccines; drinking water; waste water; digital infrastructure (internet exchange points; DNS service providers; TLD name registries; cloud computing service providers; data centre service providers; content delivery networks; trust service providers; providers of public electronic communications networks and publicly available electronic communications

services); ICT service management (managed service providers and managed security service providers), public administration and space.

Other critical sectors: postal and courier services; waste management; chemicals; food; manufacturing of medical devices, computers and electronics, machinery and equipment, motor vehicles, trailers and semi-trailers and other transport equipment; digital providers (online market places, online search engines, and social networking service platforms) and research organisations.

How will the NIS2 strengthen and streamline security requirements and incident reporting obligations of the entities?

The evaluation of the current rules on security and incident reporting requirements has shown that in some cases Member States have implemented these requirements in significantly different ways. This has created an additional burden for companies operating in more than one Member State.

Furthermore, when it comes to cybersecurity requirements we want to be sure that all companies address the necessary core set of elements in their cybersecurity risk management policies.

For this reason, NIS2 includes a list of 10 key elements that all companies have to address or implement as part of the measures they take, including incident handling , supply chain security, vulnerability handling and disclosure, the use of cryptography and where appropriate, encryption.

When it comes to incident reporting, we need to strike the right balance between the need for swift reporting in order to avoid the potential spread of incidents, and the need for in-depth reporting to draw valuable lessons learned from individual incidents. The new Directive foresees a multiple –stage approach to incident reporting. Affected companies have 24 hours from when they first become aware of an incident to submit an early warning to the CSIRT or competent national authority which would also allow them to seek assistance (guidance or operational advice on the implementation of possible mitigation measures) if they request it. The early warning should be followed by an incident notification within the 72 hours of becoming aware of the incident and a final report no later than one month later.

How will the new rules be supervised and enforced?

The new NIS Directive puts supervision and enforcement at the heart of the tasks of the competent authorities and sets a coherent framework for all supervisory and enforcement activities across Member States.

In order to strengthen the supervision that helps ensure effective compliance, the NIS2provides for a minimum list of supervisory means through which competent authorities may supervise essential and important entities. These include regular and targeted audits, on-site and off-site checks, request of information, and access to documents or evidence.

In addition, the new Directive establishes a differentiation of supervisory regimes between essential and important entities, with a view to ensuring a fair balance of obligations for both entities and competent authorities.

As regards to enforcement, so far there has been an overall reluctance across Member States to apply penalties to entities failing to put in place security measures or report incidents. This can have negative consequences for the cyber resilience of entities. In order to make enforcement effective, the new Directive sets up a consistent framework for sanctions across the Union. It therefore establishes a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations laid down in the NIS2 Directive. These sanctions include binding instructions, order to implement the recommendations of a security audit, order to bring security measures in line with NIS requirements, and administrative fines. In relation to administrative fines, the new NIS Directive distinguishes between essential and important entities. With regard to essential entities, it requires Member States to provide for a certain level of administrative fines, notably a maximum of at least €10,000,000 or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. With regard to important entities, NIS2 requires Member States to provide for a maximum fine of at least € 7,000,000 or at least 1,4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

When exercising their enforcement powers, competent authorities should give due regard to the particular circumstances of each case, such as the nature, gravity and duration of the infringement, the damage caused or losses incurred, the intentional or negligent character of the infringement.

In order to ensure real accountability for the cybersecurity measures at organisational level, NIS2 introduces provisions on the liability of natural persons holding senior management positions in the entities falling within the scope of the new NIS Directive.

How does the Commission propose to improve cyber crisis management?

The new rules improve the way the EU prevents, handles and responds to large-scale cybersecurity incidents and crises. They do so by introducing clear responsibilities, appropriate planning and more EU cooperation. NIS2 requires Member States to appoint national authorities responsible for cyber crisis management, introduces national large-scale cybersecurity incident and crisis response plans, and establishes the European cyber crisis liaison organisation network (EU-CYCLONe) to support the coordinated management of large-scale cybersecurity incidents and crisis at operational level. This Network is a key component contributing to the establishment of the EU cyber crisis management framework outlined by the Commission in 2017 with the Recommendation on coordinated response to large-scale incidents and crises.

Which Member State will have jurisdiction over the entities in the scope of NIS 2?

As a rule, essential and important entities are deemed to be under the jurisdiction of the Member State where they are established. If the entity is established in more than one Member State, it should fall under the jurisdiction of each of these Member States. The competent authorities each of these Member States should cooperate, provide mutual assistance to each other and, where appropriate, carry out joint supervisory actions. There are several exceptions to this rule:

- providers of public electronic communications networks or providers or publicly available electronic communications services would fall under the jurisdiction of the Member State where they provide their services.
- public administration entities would fall under the jurisdiction of the Member State which established them.
- certain types of entities would be under the jurisdiction of the Member State, in which they have their main establishment in the Union. These entities include domain name system service providers, top level domain 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 and of social networking platforms. This is to ensure that such entities do not face a multitude of different legal requirements, as they provide services across borders to a particularly high extent. For the purpose of effective supervision, these types of entities will be required by the Member States to notify among others where the entity's main establishment is as well as its other legal establishments in the Union or, if not established in the Union, the place where the entity's representative is designated. ENISA would be required to create and maintain a registry with the information provided on this basis by the Member States.

How will the rules improve cooperation?

EU Cooperation is taken forward by allowing Member States to act jointly and tackle emerging security risks posed by the ongoing digital transformation.

More specifically, Member States will be able to jointly supervise the implementation of EU rules and mutually assist each other in the case of cross-border malpractices, have a more structured dialogue with the private sector and coordinate the disclosure of vulnerabilities found in software and hardware sold across the internal market. They will also be able to work in a coordinated manner to assess the security risks and threats related to new technologies, as done for the first time with 5G.

Member States will draw on EU cooperation to improve national capabilities through staff exchanges between authorities and peer reviews. The existing groups, notably the Cooperation Group gathering national cybersecurity authorities and the Network of Computer Security Incident Response Teams (CSIRTs) will contribute to advance cooperation respectively at both strategic and technical levels.

How does this initiative interact with other EU policies?

NIS2 Directive is closely linked with two other initiatives, the Critical entities Resilience (CER) Directive and the Regulation for the Digital Operational resilience for the financial sector (Digital Operational Resilience Act, DORA) .

The scope of the NIS 2 and the Critical Entities Resilience Directive (CER Directive) have been aligned to a large extent to ensure that physical and cyber resilience of critical entities are addressed in a comprehensive manner. Entities identified as critical entities under the CER Directive, will become also subject to the cybersecurity obligations of NIS2 Directive. Furthermore, national competent authorities under the CER and NIS2 Directives have to cooperate and exchange on a regular basis relevant information such as on risks, cyber threats and incidents as well as on non-cyber risks, threats and incidents. The Cooperation Group under NIS2 will have to meet on a regular basis and at least once per year with the Critical Entities Resilience Group established under the CER Directive.

As regards the financial sector, while the new NIS Directive includes credit institutions, operators of trading venues and central counterparties under its scope, DORA will apply to these entities as regards cybersecurity risk management and reporting obligations. At the same time, it is important to maintain a strong relationship for the exchange of information between the financial sector and the other sectors covered by NIS 2. To that end, under the DORA , the European Supervisory Authorities (ESAs) for the financial sector and the financial sector national competent authorities would be able to participate in the discussions of the NIS Cooperation Group. Furthermore, the DORA competent authorities would be able to consult and share relevant information with the Single Point of Contacts (SPOCs) and CSIRTs established under NIS2. The competent authorities, SPOCs or the CSIRTs established under NIS2 would also receive details of major ICT-related incidents from the competent authorities under DORA. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs may cover the financial sector in their activities.

What are the next steps?

Member States will have to transpose the Directive by 17 October 2024 (21 months of entry into force of NIS2). The Commission then has to periodically review the functioning of the Directive and report on this for the first time by 17 October 2027 to the Parliament and to the Council.

Source URL:
https://digital-strategy.ec.europa.eu/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

© European Union, 2023 - Shaping Europe’s digital future (https://digital-strategy.ec.europa.eu/en) - PDF generated on 07/12/2023

Reuse of this document is allowed, provided appropriate credit is given and any changes are indicated (Creative Commons Attribution 4.0 International license).
For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.