BCLP. Client Intelligent

Insights

WHAT IS THE IMPACT OF THE EU'S NEW NETWORK AND INFORMATION SYSTEMS DIRECTIVE FOR BUSINESSES?

DIGITAL SPEAKS SERIES

Dec 06, 2024

SUMMARY

Forming part of the EU's broader digital and cyber security strategy, the new Network and Information Systems Directive 2022/2555 **(NIS2)** came into effect on 18 October 2024 (this being the deadline by which the directive is required to be implemented into national law, although this process is not yet complete). It replaces NIS Directive 2016/1148 and complements the EU's Cyber Resilience Act (discussed in a recent BCLP insight). The revised directive is intended to cast a wider net and bring more industries and sectors directly within its regulatory remit. In-scope businesses will therefore need to ensure appropriate risk-management procedures are embedded across their organisations. Senior management also need to understand the oversight which they are required to exercise, given the personal liability for cybersecurity failings which NIS2 now mandates.

WHICH BUSINESSES ARE NOW WITHIN SCOPE OF NIS2?

NIS2 covers entities in a wider variety of industries, focusing on entities in 'sectors of high criticality' and those operating in 'other critical sectors', such as:

- healthcare;
- manufacturing of pharmaceutical products or preparations, medicinal products or medical devices;
- energy and utilities;
- transport;
- financial institutions (save for those complying with the Information and Communication Technology (ICT) risk management aspects of the Digital Operational Resilience Act (DORA);

- digital infrastructure (including providers of cloud computing services);
- digital providers such as online marketplaces, online search engines and social networking services platforms
- business to business ICT service management;
- production of chemicals;
- production, processing and distribution of food;
- manufacture of motor vehicles, machinery and transport equipment;
- manufacture of computer, electronic and optical products;
- manufacture of electrical equipment; and
- research organisations.

New sectors have been added to the NIS1 list, based on their degree of digitalisation and interconnectedness and how crucial they are for the economy and society (with the complete list of high criticality sectors and other critical sectors set out in the Annex 1 and 2 of NIS2). NIS2 also introduces a clear size threshold rule, such that all medium and large-sized companies in selected sectors will be included in the scope. EU Member States also have a discretion to identify smaller entities with a high security risk profile which must comply with NIS2. The distinction between operators of essential services and digital service providers has also been removed. Entities are now classified based on their importance, and divided into two categories: essential and important entities, which are then subject to different supervisory regimes.

HOW DOES NIS2 WORK?

If a company operates in one of the sectors listed above, it must then establish if it is an 'essential entity' or an 'important entity'.

Essential entities are those companies which:

- have more than 250 employees or 50 million euro of revenue and that are in one of the following sectors: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT service management (business-to-business), public administration, or space; or
- are
  - Trust service providers
  - Public electronic communication network providers

- Public administration entities

- have been designated as critical entities under the Critical Entities Resilience Directive 2022/2557; or
- have been designated by a Member State as essential entities or operators of essential services.

Important entities are all other organizations that are not essential entities, and operate

- postal and courier services;
- waste management;
- manufacture, production and distribution of chemicals;
- production, processing and distribution of food;
- manufacturing;
- digital providers; and
- research.

Member States can also identify an entity as an 'important entity' if the entity:

- is the sole provider of a service which is essential for the maintenance of critical societal or economic activities;
- provides a service, which, if disrupted could have a significant impact on public safety, public security or public health or could induce a significant systemic risk; or
- is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State.

KEY OBLIGATIONS FOR ENTITIES IN SCOPE

- **Cybersecurity risk-management measures – Article 21:** Appropriate and proportionate technical, operational and organisational measures must be taken 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. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, these measures must ensure a level of security of network and

information systems appropriate to the risks posed. When assessing proportionality of those measures, account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

- **Governance and management responsibilities – Article 20:** Management bodies of essential and important entities must oversee and approve the cybersecurity risk-management measures taken by those entities and senior personnel can be held personally liable for infringements of Article 20.

- **Incident reporting – Article 23:** Essential and important entities must notify, without undue delay, their competent computer security incident response teams (CSIRT) or, where applicable, the relevant regulator of any incident that has a significant impact on the provision of their services. Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Information reported must include any information enabling the CSIRT or, where applicable, regulator to determine any cross-border impact of the incident. Where there is a cross-border or cross-sectoral significant incident, Member State regulators shall ensure that their single points of contact in other member states are provided in due time with the relevant information.

- **Use of European cybersecurity certification schemes – Article 24:** Essential and important entities may be required to use particular ICT products, ICT services and ICT processes, (developed in-house or procured from third parties) that are certified under European cybersecurity certification schemes.

NEW EU GOVERNANCE LAYER

The NIS2 Directive also sets out obligations for national EU member states, as well as an EU governance framework to monitor the application and enforcement of the NIS2 rules. This requires EU Member states to designate a competent regulatory authority, the single point of contact for incident reporting, designate or establish a Computer Security Incident Response Team and liaise with ENISA (the EU's cybersecurity agency) and the Commission, as well as ENISA's cyber crisis liaison organisation network (CyCLONe). The EU's NIS2 Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT product supply chains, taking into account technical and, where relevant, non-technical risk factors. National regulators can encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.

SANCTIONS FOR NON-COMPLIANCE

Companies that do not comply with the new NIS2 rules face specific penalties for non-compliance, including:

- **Non-monetary remedies:** compliance orders, binding instructions, security audit implementation orders and threat notification orders issued to customers.
- **Administrative fines:** 'Essential entities' can be fined up to a maximum of at least €10,000,000 or 2% of the global annual revenue, whichever is higher. 'Important entities' can be fined up to a maximum of at least €7,000,000 or 1,4% of the global annual revenue, whichever is higher.
- **Criminal sanctions:** new measures mean top management can be held personally liable if gross negligence causes a security incident.

INTER-RELATIONSHIP BETWEEN NIS2 AND ISO 27001

Note that voluntary compliance with the ISO 27001 standard will be seen separately from the NIS2 compliance picture as NIS2 is mandatory for entities operating within specific industry sectors. ISO 27001 should therefore be seen as a useful mechanism offering detailed approaches and procedures to fulfil NIS2's requirements.

HOW NIS 2 HAS BEEN IMPLEMENTED IN EU MEMBER STATES ?

On 28 November 2024, the European Commission opened an infringement procedure and has issued formal notice to 23 Member States (Bulgaria, Czechia, Denmark, Germany, Estonia, Ireland, Greece, Spain, France, Cyprus, Latvia, Luxembourg, Hungary, Malta, Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland and Sweden) for failure to fully transpose the NIS2 Directive into national law. These states now have two months to respond and to complete transposition (and notify the Commission).

HOW IS THE UK APPROACHING CYBER SECURITY REGULATION?

NIS2 does not apply in the UK as it was formulated after the end of the Brexit transition period. However, the UK is separately making changes to its cybersecurity laws to update the UK's Network and Information Systems Regulations (which implemented NIS1), with the issue of the long anticipated Cybersecurity and Resilience Bill (CS&R Bill). Although the wording of the Bill has not yet been released, initial indications as to what it will cover are available. One of the critical changes will be the expansion of sectors subject to cybersecurity regulation (mirroring the changes we are seeing at the EU level). The incident reporting framework is another key area where the UK's CS&R Bill is expected to align with NIS2 reporting thresholds. Under NIS1, entities have 72 hours to report a cybersecurity incident. However, it appears that, in line with NIS2, the UK government plans to shorten this window, particularly for critical entities. There will also be a push for mandatory cybersecurity standards and measures. It is anticipated the new legislative provisions will set the

baseline for cybersecurity risk management measures, operational resilience, and reporting obligations, across all relevant sectors.

RELATED CAPABILITIES

- Data Privacy & Security
- Technology Transactions

MEET THE TEAM

Pierre-Emmanuel Froge

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21
