knowledge 16 July 2024 | 6 min read

Impending cybersecurity obligations: Are you subject to NIS 2?

The NIS 2 Directive (Directive (EU) 2022/2555) aims to ensure a common high-level security of network and information systems across EU Member States and to update cybersecurity obligations.

As the 17 October 2024 deadline for implementation of the NIS 2 Directive is fast approaching, the Heads of Bill for the National Cyber Security Bill (the **"Bill"**) are expected to be published imminently. The NIS 2 Directive will impose enhanced cybersecurity obligations on those who are already subject to the current regime and expands the scope of the previous regime to capture a wider number of bodies.

Organisations should consider the NIS 2 Directive to determine (1) whether they are subject to it, and (2) what their obligations are, so that they are prepared when the Government publishes the applicable national legislation. Notably, the NIS 2 Directive provides for an enhanced enforcement regime, which includes the possibility of substantial administrative fines and potential personal liability for senior management.

1. The current and prospective regime

Many organisations will be familiar with the Network and Information Security Directive (Directive (EU) 2016/1148) (**"NIS Directive"**), which was adopted in 2016 and implemented in Ireland by the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 (S.I No. 360 /2018) (the **"NIS Regulations"**).

While the NIS Directive was the first EU-wide legislation on cybersecurity, a number of shortcomings were identified during a review by the European Commission in the context of an era of increased digitization, highlighted in particular by the increased reliance on technology during the COVID-19 pandemic. These shortcomings included the limited number of sectors covered, differences in implementation by Member States and ineffective enforcement. As a result, the European Commission introduced the NIS 2 Directive in an effort to address those shortcomings.

The NIS 2 Directive was adopted on 16 January 2023 and Member States have until 17 October 2024 to transpose its measures into national law. The Government Legislation Programme for Summer 2024 notes that the Heads of Bill are in preparation for the Bill which is intended to implement the NIS 2 Directive in Ireland. In light of this and the upcoming October deadline, we expect that the Heads of Bill should be published in the coming weeks. When this happens, it would be useful for organisations to have identified whether or not they are subject to the NIS 2 Directive (noting its increased scope) and the obligations it sets out, so that they are in a position to comply with the national legislation when it enters into force. While some organisations will have been subject to the previous regime, many organisations will be considering its requirements for the first time.

2. Are you captured by NIS 2?

The NIS 2 Directive imposes cybersecurity obligations on both public sector bodies and private sector entities who are considered to be either 'essential entities' or 'important entities'. The NIS 2 Directive sets out detailed factors which determine whether entities fall within its scope, and applicable 'essential' or 'important' entities are primarily defined by reference to specified sectors, the size of the applicable entity and the critical nature of the service provided by the relevant entity.

The NIS 2 Directive covers 'sectors of high criticality' which might be expected to be covered by the regime including: energy; transport; banking/financial market infrastructures; health; water; digital infrastructure; public administration, and space. However, it also captures 'other critical sectors', including: postal/courier services; waste management; the manufacture, production and distribution of chemicals; the production, processing and distribution of food; manufacturing; digital providers (e.g. providers of online marketplaces, online search engines or providers of social networking services platforms), and research organisations.

By 17 April 2025, Member States are required to establish a list of 'important' and 'essential' entities (which will be reviewed at least every two years) and notify certain information regarding those entities to the competent authorities.

In addition, given the supply chain management requirements of the NIS 2 Directive, service providers to organisations which are subject to the NIS 2 Directive may be expected to sign up to contractual obligations relevant to security obligations and the notification of incidents to such organisations.

3. How does NIS 2 interact with other European legislation?

The obligations set out in the NIS 2 Directive are intended to co-exist with existing obligations which are already imposed on applicable organisations by other European legislation such as the General Data Protection Regulation (**"GDPR"**).

In addition, certain financial entities may also be captured by the upcoming Digital Operational Resilience Act (**"DORA"**), which will apply from 17 January 2025. Where equivalent obligations are set out in other European legislation such as DORA, the corresponding provisions of the NIS 2 Directive will not apply to entities subject to those equivalent obligations. The European Commission has issued guidelines (https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive)on the interaction between such other European legislation, in particular DORA, and the NIS 2 Directive. See our briefing here (https://www.mccannfitzgerald.com/knowledge/finance/briefing-dora-digital-operational-resilience-act)for further information regarding DORA.

4. What are the key obligations?

a. **Cybersecurity risk-management measures**

Essential entities and important entities must take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the 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.

The NIS 2 Directive specifies minimum measures which organisations must put in place. This includes, but is not limited to, policies on risk analysis and information system security;

incident handling; business continuity and crisis management measures; and supply chain security (which includes carrying out due diligence on suppliers and ensuring certain obligations are imposed on suppliers).

Management bodies of essential and important entities are required to approve the cybersecurity risk-management measures taken by those entities, oversee its implementation and can be held liable for infringements by the entities. A "management body" might comprise, for example, the board of an essential or important entity.

b. **Incident notification**

Essential entities and important entities are required to notify, without undue delay, the Computer Security Incident Response Team (**"CSIRT"**) or the relevant competent authority (where applicable), of an incident that has a 'significant impact' on the provision of services (with further guidance provided in the NIS 2 Directive on what is considered to be 'significant').

The NIS 2 Directive provides for a phased reporting model. An early warning must be provided within 24 hours, followed by a full incident notification within 72 hours, and a final report within 1 month of the incident notification. Essential and important entities are also required to communicate, to recipients of their services, details of significant cyber threats or any measures or remedies which may be relevant in responding to those threats. In certain circumstances, there may also be a requirement to inform the general public of a significant incident.

Depending on the nature of the breach, a significant incident which requires reporting under the NIS 2 Directive may also trigger reporting requirements under other legislation (such as personal data breach notifications under the GDPR). Essential and important entities will be required to ensure their internal policies for handling incident notifications cover all potential reporting obligations.

5. What does NIS 2 say about supervision and enforcement?

a. **Supervision**

Supervision under the NIS 2 Directive differs depending on whether an entity is an essential entity or an important entity. Essential entities are subject to more extensive proactive supervision by the competent authority, where the competent authority will have the power to exercise various supervisory tasks including random onsite inspections, regular and ad hoc audits, targeted security audits and security scans to check for vulnerabilities. With regard to important entities, the competent authority will take reactive action when there is evidence, an indication or information alleging non-compliance with the NIS 2 Directive.

b. **Enforcement**

Competent authorities have a wide range of enforcement powers under the NIS 2 Directive that can be exercised against essential entities and important entities, including the power to issue warnings, instructions and orders, and to impose administrative fines. Additional enforcement powers can be exercised over essential entities, such as the appointment of a monitoring officer to oversee compliance. The maximum fines are:
for essential entities, the greater of €10 million or 2% of worldwide annual turnover in the preceding financial year, and;

for important entities, the greater of €7 million or 1.4% of total worldwide annual turnover in the preceding financial year.

6. What are the next steps?

In order to be prepared for the introduction of the applicable Irish legislation, organisations should consider whether they may fall under the scope of the NIS 2 Directive. If they are likely to constitute an important or essential entity, they will need to begin a review of the relevant obligations which the NIS 2 Directive imposes and take steps to ensure compliance with such obligations.

If you need assistance with your assessment of the scope and obligations of the NIS 2 Directive, please do not hesitate to contact the Technology & Innovation Group or your usual McCann FitzGerald contact.

Also contributed to by Lisa Leonard

This document has been prepared by McCann FitzGerald LLP for general guidance only and should not be regarded as a substitute for professional advice. Such advice should always be taken before acting on any of the matters discussed.

Key contacts

Paul Lavery
Partner