knowledge 9 September 2024 | 8 min read

NIS 2 implementation by October 2024: Government publishes General Scheme of National Cyber Security Bill

In advance of the 17 October 2024 deadline for implementation of the NIS 2 Directive, on 30 August 2024 the Irish government published the eagerly awaited General Scheme for the National Cyber Security Bill (the "**Cyber Security Bill**"), which is ultimately intended to transpose the NIS 2 Directive in Ireland.

This is the first draft of the Cyber Security Bill that has been published. It is expected to progress through the Irish legislative process quickly and organisations who are likely to be subject to the NIS 2 Directive will be reviewing it carefully to consider its implications for their business and how the NIS 2 Directive will be implemented in Ireland. There are explanatory notes which provide helpful colour and context for some key provisions. See our previous briefing here (https://www.mccannfitzgerald.com/knowledge/data-privacy-and-cyber-risk/impending-cybersecurity-obligations-are-you-subject-to-nis-2) for an overview of the NIS 2 Directive, and who is subject to it.

The Cyber Security Bill contains detailed provisions setting out how the NIS 2 Directive will be applied in Ireland. These address, among other things, the organisations to whom the Irish NIS 2 regime will apply, who the designated 'competent authorities' for various sectors ("**Competent Authorities**") in Ireland will be; and how the Irish supervision and enforcement regime will operate. Some key aspects of the Cyber Security Bill are summarised below.

1. Territorial Applicability

The Cyber Security Bill will generally apply to organisations within its scope who are 'established' in Ireland, or who have their 'main establishment' in the EU in Ireland or, in limited circumstances, who are not established in Ireland but provide services in Ireland. For the purpose of determining whether an organisation with operations in more than one EU member state has its 'main establishment' in Ireland and will be subject to the Cyber Security Bill, the test will be as set out in Article 26 of the NIS 2 Directive (i.e. (i) in which EU member state are decisions related to cybersecurity risk management predominantly taken; or (ii) if such a member state cannot be determined or if such decisions are not taken in EU, in which member state are cybersecurity operations carried out or (iii) if such a member state cannot be determined, the main establishment will be in the member state where that organisation has the highest number of employees in the EU.

2. NCSC

(a) *Establishment* - The National Cyber Security Centre ("**NCSC**") was established in July 2011 and is already actively involved in the regulation of cyber security in Ireland. However, following a review of the NCSC, the explanatory notes to the Cyber Security Bill indicate that the government agreed that the NCSC should be established on a legislative basis as an Executive Office of the Minister and the Department for the Environment, Climate and Communications (the "**Minister**" and the "**Department**"), and the Cyber Security Bill provides for this.

(b) *Roles under NIS 2* – The Cyber Security Bill confirms that, among other functions, the NCSC will be designated as the Computer Security Incident Response Team ("**CSIRT**") and the Competent Authority for certain entities and for the management of large-scale cyber security incidents and crises in Ireland.

In addition to being designated as Competent Authority for certain entities, although not required by the NIS 2 Directive, as a policy decision the Cyber Security Bill provides that the NSCS will act as 'lead' Competent Authority for the purposes of the NIS 2 Directive. This will involve the NCSC acting as a central co-ordinator providing advice, guidance and support including the development of a regulatory framework and tools, acting as the central authority for engagement with EU bodies and other member states, and supporting other Irish Competent Authorities.

(c) *Powers* - In connection with its appointment in various roles under the NIS 2 Directive, the Cyber Security Bill sets out the powers and obligations of the NCSC, which include the proactive non-intrusive scanning of publicly accessible network and information systems and sensor deployment on networks of essential and important entities (with consent).

3. Competent Authorities

While the NCSC has been designated as 'lead' Competent Authority for the purposes of the NIS 2 Directive, the Cyber Security Bill has also designated a number of other regulators as Competent Authorities in the respective sectors which generally fall under the existing remit of that regulator.

Specifically, these include: (1) the Commission for the Regulation of Utilities ("**CRU**") for the energy, drinking water and waste water sectors; (2) the Commission for Communications Regulation ("**ComReg**") for digital infrastructure, ICT service management, space and digital providers; (3) the Central Bank of Ireland ("**CBI**") for banking and financial markets; (4) the Irish Aviation Authority ("**IAA**") for the aviation sector; (5) the Commission for Rail Regulation ("**CRR**") for the rail sector; (6) the Minister for Transport for the maritime sector; (7) the National Transport Authority ("**NTA**") for the road sector; (8) and, an Agency or Agencies under the remit of the Minister for Health for the health sector. The NCSC has been designated as the Competent Authority for all other sectors which are captured by the NIS 2 Directive.

4. Essential and important entities

The Cyber Security Bill generally mirrors the definitions for essential and important entities which are set out in the NIS 2 Directive. However, due to the broad nature of the scope set out in the NIS 2 Directive, the Cyber Security Bill also proposes that the Minister may make regulations designating an entity as an essential or important entity (in consultation with relevant stakeholders). The explanatory note envisages that this will apply where the criteria set out in the NIS 2 Directive is particularly broad, such as where "*the person is the sole provider in the State of a service which is essential for the maintenance of critical societal or economic activities*". As such, it is possible that entities which are uncertain as to whether they fall within scope of the Cyber Security Bill will ultimately find themselves subject to it by way of a specific regulation.

In addition, while the Cyber Security Bill lists certain entities as falling within the definition of essential public administration entity (such as the Office of the Revenue Commissioners), the Minister is provided with the power to designate additional entities as a public administration entity even where they do not technically fall within the definition, where certain criteria are met and an appropriate risk assessment has been carried out.

5. Application to public bodies

The Cyber Security Bill replicates the notification obligations which are set out in the NIS 2 Directive, but also envisages that the reporting obligations with regard to significant cyber security incidents will apply to public bodies falling within the definition set out in the Cyber Security Bill (in addition to those who are subject to the Cyber Security Bill generally by falling within the definition of public administration entity). However, the Cyber Security Bill specifically states that certain of the penalty provisions and enforcement procedures set out in the Cyber Security Bill will not apply to such public bodies.

6. Cyber security risk management measures and governance

The Cyber Security Bill reflects the requirements set out in the NIS 2 Directive with regard to the obligation to put in place specified cyber security risk management measures, and notably with regard to the requirement that the management board of applicable entities approve those measures and be held liable for any infringement of the Cyber Security Bill by the relevant entity.

In addition to the European Commission's implementing regulation which will provide further details on the technical and methodological requirements for the relevant cyber security risk management measures (see our briefing on the draft implementing regulation here (https://www.mccannfitzgerald.com/knowledge/cyber-security/have-your-say-on-upcoming-nis-2-cybersecurity-obligations)), the Cyber Security Bill provides that the Minister may make regulations in relation to the types of cyber security risk management measures to be taken by essential and important entities.

While the Cyber Security Bill envisages that essential or important entities may be required to use particular ICT products, services and processes that are certified under a European cyber security certification scheme as is provided for in the NIS 2 Directive, the explanatory note in the Cyber Security Bill notes that there is no plan to mandate this in the short to medium term in Ireland. The Cyber Security Bill also provides that such entities may be advised to use such products, services and processes certified under a national cyber security certification scheme, and the explanatory note further explains that the NCSC intends to seek sanction from the Irish National Accreditation Board ("**INAB**") for a voluntary national cyber security certification scheme, which is currently under development.

7. Supervision and enforcement

A large proportion of the Cyber Security Bill contains the transposition of the supervision and enforcement provisions set out in the NIS 2 Directive as will be applicable in Ireland.

(a) *Compliance notices* - These provisions in the first instance envisage the use of authorised officers acting on behalf of a designated Competent Authority (who are provided with extensive powers of investigation and inspection), and the application of compliance notices.

If an essential or important entity does not comply with a compliance notice, the designated Competent Authority has the power to (a) apply to the High Court to declare that a chief executive officer or director of that entity shall not act as the chief executive officer or as a director or secretary, or exercise any managerial functions in respect of that entity, until the court is satisfied that the compliance notice has been complied with or, (b) where the essential or important entity operates under a licence or permit issued by the applicable Competent Authority, the Competent Authority may temporarily suspend the licence or authorisation.

(b) *Personal liability* – The Cyber Security Bill provides that where a corporate body has committed an infringement, offence or non-compliance of the Cyber Security Bill, an individual (such as a director, manager, secretary or other officer of that corporate body, or a member if the affairs of the corporate body are manged by its members) can be held personally liable for that infringement, offence or non-compliance if it can be proven that they had knowledge of such act, or that such act can be attributed to the wilful neglect of that individual.

(c) *Penalties and procedures* – The Cyber Security Bill contains detailed provisions regarding the imposition of penalties and administrative sanctions on essential and important entities and enforcement procedures, with the explanatory notes stating that the Department was cognisant of the need to ensure due process, fair procedures and rights of appeal (having regard to other legislation which has implemented administrative sanctions from EU directives).

The enforcement procedures set out in the Cyber Security Bill involve the use of a notice of suspected non-compliance, followed by a referral for adjudication if required. The Cyber Security Bill provides that an adjudication will take effect once confirmed by the High Court, and sets out the circumstances under which an adjudication can be appealed or a decision made or act done by a designated Competent Authority can be challenged.

The maximum amount of a financial penalty which may be imposed by an adjudicator is: (i) for essential entities, the greater of €10 million or 2% of worldwide annual turnover in the preceding financial year, and; (ii) for important entities, the greater of €7 million or 1.4% of total worldwide annual turnover in the preceding financial year.

Next steps

The Cyber Security Bill will be put before the Oireachtas and subject to legislative scrutiny. It is likely that there will be, at a minimum, some tidy up changes. There will be limited time, however, for any substantive changes to be made. In light of the deadline of 17 October 2024 for EU member states to transpose the NIS 2 Directive, organisations who are likely to be subject to the Irish NIS 2 regime should familiarise themselves with the Cyber Security Bill with the expectation that the Act which is ultimately implemented is likely to be substantively similar to the Bill.

Also contributed to by Lisa Leonard

Key contacts

Paul Lavery
Partner

Amy Brick
Partner