LK SHIELDS
YOUR LEGAL COUNSEL

TECHNOLOGY

Get Ready for Ireland's New Cyber Security Regime

by **Jane O'Grady, Ian Lavelle, Laura Keane**

Get Ready for Ireland’s New Cyber Security Regime

25th September 2024 | by Jane O’Grady, Ian Lavelle, Laura Keane

Do Your Part – Be Cyber Smart: Get Ready for Ireland’s New Cyber Security Regime

From October, Irish cyber security law will undergo a significant change with new requirements to boost the overall level of national cyber security.

This is part of EU wide enhanced measures set out in a directive requiring a high common level of cyber security in all EU states. The EU Network and Information Security Directive, (EU) 2022/2555, commonly referred to as “NIS 2”, will increase cyber security obligations for businesses operating in sectors of high criticality for EU security and the EU’s economy. Businesses caught by the new rules will include providers of essential services in energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

In preparing for the implementation of NIS 2, the Irish Government recently published proposals for legal changes in the General Scheme for the National Cyber Security Bill 2024. The proposal for a National Cyber Security Bill will incorporate NIS 2 into Irish law. The proposal also includes a general framework for Ireland’s national cyber security strategy including new measures beyond the requirements of NIS 2. The proposals also include giving Ireland’s primary cyber security authority, the National Cyber Security Centre, a statutory function with a clarified mandate and role.

What does NIS 2 entail?

NIS 2 requires EU Member States (including Ireland) to ensure that operators in certain sectors implement appropriate and proportionate technical, operational and organisational measures to manage risks posed to the security of network and information systems and to prevent or minimise the impact of incidents on recipients of such services. NIS 2 places these requirements on organisations that are deemed “essential” or “important” and are established in a Member State or are not based in the EU but provide services into a Member State.

Entities with 250 employees or more and an annual turnover of €50 million operating in the following sectors will be deemed “*essential*”:

- Energy
- Transport
- Finance
- Health
- Waste and/or Drinking Water
- Public administration
- Digital Infrastructure
- B2B ICT Management
- Space

“Important” entities are organisations with approximately 50 employees or more having an annual turnover of €10 million that operate in the following sectors:

- Postal and courier services
- Waste management
- Chemicals
- Food
- Manufacturing in the areas of medical devices, computers, electronics, machinery, vehicles or transport equipment.

Key provisions of the proposed Cyber Security Bill

1. National authorities

National authorities will be designated to oversee the implementation of NIS 2 in different crucial sectors. Regulatory bodies that will have new powers in relation to essential entities will include the CRU, ComReg, the Central Bank of Ireland and the Irish Aviation Authority.

2. The National Cyber Security Centre

The National Cyber Security Centre (NCSC) will be designated as the lead national authority responsible for the implementation and enforcement of cybersecurity measures in Ireland. It will also act as Ireland’s Computer Security Incident Response Team (CSIRT), which is a required function under NIS 2.

The NCSC will have several capabilities including network and information system scanning to detect vulnerabilities. All essential and important entities will have obligations to report cyber security threats to the NCSC within 24 hours of becoming aware of a significant incident or an early warning and thereafter submit a report to the NSCS one month after reporting the cyber incident.

3. Internal framework for risk management

Essential entities will be obliged to have an internal framework for risk management measures, including:

- carrying out risk assessments on a regular basis
- ensuring that security measures are in place
- devising an appropriate incident response plan
- carrying out cybersecurity risk management training

4. Incident notification

Both essential and important entities will be obliged to report incidents which have a “significant impact” on services to CSIRT. The timelines for notification are as follows.

- Within 24 hours: early warning
- Within 72 hours: full incident notification
- Within 1 month: final report

5. Non-compliance

The management bodies of essential and important entities will be required to approve the cybersecurity risk-management measures for those bodies and oversee their implementation.

A competent authority will be able to issue compliance notices to entities directing them to comply with their legal obligations where there is a finding of a breach.

A number of national measures for non-compliance with NIS 2 have been proposed, where the breach has not been remedied in line with a compliance notice.

- Possible restriction of company CEO, director or other senior managers from their positions based on an application to the High Court by the NCSC.
- Where NSCS has issued a licence to an entity to operate their business in the state, they have the power to suspend that licence until there is compliance with the legislation.
- Essential entities can be fined up to €10m or 2% of total global annual revenue for essential entities.
- Important entities can be fined €7m or 1.4% of total global annual revenue, whichever figure is higher. Where a national competent authority (NCA) issues a licence to an essential entity or important entity to operate its business in Ireland, the relevant NCA may suspend that licence until the entity in question is in compliance with its obligations.

What should you do now?

When it comes to penalties for breaches, the stakes are high. Businesses falling within the scope NIS 2 and the proposed Irish bill should be doing everything they can to prepare for compliance.

1. Determine if your organisation is an essential entity or an important entity.

2. If NIS 2 applies to your entity, here are some practical steps you can take to comply with your upcoming obligations.

- Review your cybersecurity procedures to ensure that you have appropriate and proportionate technical, operational and organisational measures to manage security risks.
- Review the corporate governance procedures in your organisations to identify who is responsible within the organisation for approving cybersecurity measures.
- Ensure that management has oversight of cyber security risk management systems and oversees their implementation because infringement actions and restrictive measures may be brought against individual directors and managers.
- Establish a framework to respond to and comply with any notification requirements of the NCA overseeing your sector in line with required time limits. Introduce cybersecurity training for management and staff to ensure awareness with the requirements and penalties set out in NIS 2.
- Carry out security audits and review arrangements with third party IT suppliers to ensure they are obligated to assist you in reporting and compliance measures.

What’s next?

NIS 2 will take effect across the EU on 17 October 2024. The Irish parliament recently returned after summer recess. It is expected that this legislation will be a priority so that the proposed national cyber security legislation is enacted in tandem with NIS 2 coming into place.

We will be issuing a further update once the legislation is in force.

For more information contact Jane O'Grady at jogrady@lkshields.ie, Ian Lavelle at ilavelle@lkshields.ie and Laura Keane at lkeane@lkshields.ie.

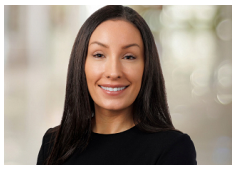
About the Authors

Jane O'Grady
Partner

Jane is dual qualified as a solicitor and a trade mark and design attorney, with many years' experience advising on commercial contracts, intellectual property, commercial agency and all aspects of technology law.
T: +353 1 637 1554 **E:** jogrady@lkshields.ie

Ian Lavelle
Partner

Ian is a partner in our Litigation and Dispute Resolution department.
T: +353 1 6385823 **E:** ilavelle@lkshields.ie



Laura Keane
Senior Associate

Laura advises on a wide range of commercial disputes, with a particular focus on insurance litigation.
T: +353 1 638 5801 **E:** lkeane@lkshields.ie