STEVENS&BOLTON

CYBERSECURITY – NIS 2

BACKGROUND AND TIMELINES

In 2016 the EU introduced EU Directive 2016/1148, which was brought into UK law by the Network and Information Systems Regulations 2018 (NIS). You can read our briefing note on NIS here, but in summary its aim was to establish a secure and consistent cybersecurity framework across Europe. However, due to a combination of factors including the increasing digitisation of society and regularity of cybersecurity incidents, it quickly became necessary for NIS to be broadened and strengthened.

Accordingly, the EU introduced a replacement in the form of Directive 2022/2555, or NIS2, which comes into force across the EU from **18 October 2024**. Entities falling within the scope of NIS 2 will need to provide competent authorities with certain information to be included in the relevant Member State's register. Generally this step will need to be undertaken by entities falling in scope by **17 April 2025**, but some entities will need to register by an earlier date of **17 January 2025**.

IMPLEMENTATION

Like its predecessor, the NIS 2 directive will need to be given effect by Member States through national legislation, which may create slight variations in the way that NIS 2 is implemented between Member States.

SCOPE

NIS2 applies to both public and private entities operating in particular sectors which are defined as either "highly critical" or "critical". Highly critical sectors are:

- Energy
- Transport
- Health
- Drinking water
- Space
- Financial Market Infrastructure
- Banking
- Digital infrastructure
- Waste water
- ICT-service management

"CRITICAL" SECTORS ARE:

- Postal/courier services
- Food services
- Waste management services
- Digital providers
- Manufacturing services
- Chemical manufacturing services

Entities that fall within the scope of the critical or highly critical categories can be designated as either "essential" or "important". There are certain criteria which determine whether an entity is "essential" or "important", which largely relate to the extent to which a disruption to the services they offer would have significant consequences for society within the Member State in question. Only "large" and "medium" entities (defined by reference to revenue size and number of employees) are mentioned in those criteria. However, Member States can also designate entities as either essential or important based on their risk profile with the effect that some entities may find that they are caught by NIS 2 regardless of their size.

"Essential" entities are subject to on-going supervision, whilst "important" entities will only be supervised after they report a failure to comply with the requirements of NIS2.

DUTIES AND RESPONSIBILITIES

Cybersecurity and risk management

Entities falling into the scope of NIS 2 are required to take suitable and proportionate technical, operational and organisational steps to manage cybersecurity risks. Proportionality is determined with reference to the size of the entity, the extent it is exposed, the likelihood and potential seriousness of cyber incidents and the extent of the potential impact of such an incident. The overall approach should be approved by the entity's management board, and notwithstanding proportionality, entities are expected to be prepared for the gamut of possible incidents and incorporate at least the following policies/procedures:

(a) Supply chain security

(b) Risk analysis and information security

(c) Business continuity

(d) Incident handling

(e) Vulnerability handling and disclosure

(f) Cryptography and encryption

(g) HR security access control and asset management

Additionally, entities must have in place:

(i) Procedures to assess the effectiveness of cyber risk management

(ii) Computing hygiene practices and cybersecurity training

(iii) Multi-factor authentication and secure communication systems

Reporting

Entities falling in scope must notify the recipient of services of significant impacts to the provision of their service and, where there is a cyber threat, inform service recipients that are potentially affected on remedial measures they can apply in response to a significant cyber threat. Where appropriate, they should also inform the individuals affected on the specific threat itself.

For the purposes of NIS 2, a cyber threat is "significant" where:

- It either has caused or could cause serious operational disruption to services or losses to the entity itself, and/or

- It either has affected or could affect other natural or legal persons by causing significant damage.

Where “significant incidents” actually take place, entities are obliged to notify the computer security incident response team or competent authority within 24 hours of becoming aware (or give an “early warning”) and provide a series of more detailed reports starting with an “incident notification” 72 hours after becoming aware of the significant incident culminating in a final report not later than one month after the incident notification.

SUPERVISION AND FINES

NIS 2 requires competent authorities to have new powers of supervision. These are wide-ranging and include the right to carry out in-person inspections, scheduled and reactive security audits and requests for data relating cybersecurity policies and evidence that such policies have been implemented.

Where entities fail in certain of their obligations under NIS2, competent authorities can impose fines of:

- The higher of: (i) a maximum of at least €10,000,000; or (ii) a maximum of at least 2% of the total worldwide annual turnover in the previous financial year of the undertaking to which the entity belongs (“Essential” entities), and
- The higher of: (i) a maximum of at least €7,000,000; or (ii) a maximum of at least 1.4% of the total worldwide annual turnover in the previous financial year of the undertaking to which the entity belongs (“Important” entities).

PERSONAL RESPONSIBILITY

In addition to their fining and supervisory powers, NIS2 will give competent authorities rights to temporarily prohibit individuals at essential entities who are responsible for failing to comply with cybersecurity risk management requirements from carrying out managerial responsibilities at CEO/legal representative level.

THE POSITION IN THE UNITED KINGDOM

There are at present no plans for the UK to introduce similar legislation to NIS2, so NIS will continue to apply to companies based in the UK only, though those with operations throughout the EU will need to take steps to comply with whatever local legislation implements NIS 2 on a Member State by Member State basis. So, in common with a number of other pieces of EU legislation, it may be the case that NIS2 applies to UK businesses with cross-border operations, even though there is no direct UK equivalent.

KEY CONTACTS

For further information about any of the issues raised in this guide, please contact:

Charles Maurice
Partner
T: +44 (0)1483 406971
M: +44 (0)7557 677192
E: charles.maurice@stevens-bolton.com

Alasdair McDowell
Associate
T: +44 (0)1483 406977
M: +44 (0)7583 130133
E: alasdair.mcdowell@stevens-bolton.com

STEVENS&BOLTON

Wey House, Farnham Road
Guildford, Surrey, GU1 4YD
Tel: +44 (0)1483 302264
Fax: +44 (0)1483 302254
DX 2423 Guildford 1
www.stevens-bolton.com

BS_DEPARTMENTAL_BD\60886950v1