STEVENS&BOLTON

CYBERSECURITY - NETWORK AND INFORMATION SYSTEMS REGULATIONS 2018 (NIS)

EU Directive 2016/1148 (the "Directive") was introduced with a view to establishing a secure and consistent cyber security framework within Europe. The Network and Information Systems Regulations 2018 (the "Regulations") subsequently transposed the Directive into UK law.

The Regulations apply to digital service providers, classified by the Regulations as being either:

Relevant Digital Service Providers (RDSPs) – organisations providing the following digital services:

- an online marketplace;
- an online search engine; or
- a cloud computing service,

and, which:

- have a head office, or a nominated representative in the UK; and
- have more than 50 staff and a turnover or balance sheet of more than €10 million

Operators of Essential Services (OESs) – organisations providing services which are essential "for the maintenance of critical societal or economic activities". This means that a service provider will be an OES if it provides a service which relies on a network and information system in the sector of:

- energy;
- transport;
- health;
- drinking water supply and distribution; or
- digital infrastructure

and meets certain sector specific operating thresholds specified in the Regulations.

RELEVANT DIGITAL SERVICE PROVIDERS

If an organisation satisfies the criteria above then it will be an RDSP for the purposes of the Regulations. This may bring various compliance and notification requirements.

There are multiple limbs to the definition of an RDSP and this potentially has a wide application.

Who is an RDSP – a broad definition?

As set out at the head of this note, there are multiple limbs to the definition of RDSP, and this potentially has a wide application. It is worth looking at each component part of the definition in further detail.

What is an 'online marketplace'?

For the purposes of the Regulations, online marketplaces are online platforms that allow buyers and sellers to: (a) conclude sales of goods or services on that online platform; or (b) conclude sales of goods or services on the trader's website, provided that website uses computing services provided by the online marketplace.

Not all platforms that allow individuals to buy or sell services are caught by the definition. In particular, the following are expressly excluded:

- classified adverts;
- online retailers that only sell directly to customers on behalf of themselves; and
- websites that redirect users to other services to make the final contract e.g. price comparison websites.

What is an 'online search engine'?

An online search engine is a digital service that allows users to perform searches of all websites/websites in a particular language, on any subject, using a keyword, phrase or other input, and which returns information in the form of a 'link'. Additionally, the online search engine must be provided to the public in order for this definition to apply. So an online search function operating on an internal intranet page would not be an 'online search engine' within the meaning of the Regulations.

Most obviously, this definition would cover any web search engine operators based in the UK. Conversely, websites that embed a search function would not be caught by this definition; although the provider of the underlying search function may themselves be caught.

What is a cloud computing service?

A cloud computing service, is a digital service that enables access to a scalable and elastic pool of shareable computing resources.

- *What are 'computing resources'?*

Computing resources include resources such as networks, servers or other infrastructure, storage, applications and services.

- *What is a 'scalable and elastic pool'?*

Computer resources will be 'Scalable', if they can be flexibly allocated by the service provider, regardless of the geographical location of those resources, in order to handle fluctuation in demand.

Computer resources that are provisioned and released according to demand, so that the availability of such resources can rapidly increase or decrease depending on workload, will be considered an 'elastic pool'.

- *What does 'shareable' mean?*

Computer resources will be 'shareable', if they are provided to multiple users who share a common access, but where processing is carried out separately for each user, even though the service is provided from the same electronic equipment.

- *Who might 'enable access'?*

Both cloud service providers and cloud service brokers may, depending on the circumstances, be considered to 'enable access' to a scalable and elastic pool of shareable computer resources.

Obligations imposed on RDSPs by the Regulations

Security Obligations

RDSPs are required to identify and take appropriate and proportionate measures to manage the risks posed to the security of their network and information systems. This means that RDSPs must:

- ensure a level of security appropriate to the risks posed;
- prevent and minimise the impact of incidents affecting digital services; and
- take account of the following:
    - the security of systems and facilities – being the security of network and information systems, and the physical environment of those systems;
    - incident handling – being the procedures for supporting the detection, analysis and containment of any incident and any follow up response;
    - business continuity management – being the ability to maintain or restore services to acceptable predefined levels following a disruptive incident;
    - monitoring auditing and testing – being the requirement to establish and maintain policies and processes relating to systems assessment, inspection and verification; and
    - compliance with international standards – being the requirement to comply with international standards such as ISO/IEC 27001 or ISO/IEC 22301.

The regulations impose various security and reporting obligations on RDSPs.

Reporting Obligations

RDSPs are under an obligation to report incidents which have a substantial impact on the provision of any of the relevant services that they provide. Any report must be made to the ICO within 72 hours of any such incident taking place.

In determining whether an incident is substantial enough to warrant reporting, RDSPs should take into account:

- the number of users affected by the incident, and in particular, the number of users relying on the affected digital service for the provision of their own services;
- the duration of the incident;
- the geographical areas affected by the incident;
- the extent of the disruption to the functioning of the service;
- the extent of the impact on economic and societal activities; and
- whether the impact is substantial according to the ICO's guidance

OPERATORS OF ESSENTIAL SERVICES

The regulatory approach to OES is largely sector-specific.

As with RDSPs, if an organisation satisfies the sector-specific criteria listed at the head of this note, they will be an OES for the purposes of the Regulations. Again, this may bring various compliance and notification requirements.

However, unlike RDSPs, in certain circumstances competent authorities can designate organisations as OESs, even if they do not meet the relevant statutory threshold. In such circumstances, the relevant competent authority will inform the organisation in writing of its classification as an OES.

As with RDSPs, OESs will be under various security and reporting obligations, the requirements of which are set out in the Regulations, and any specific guidance published by the OES's relevant competent authority.

REGULATORY FRAMEWORK

In the UK, the ICO is the competent authority for all RDSPs, whereas the relevant competent authority for OESs will vary depending on the sector. RDSPs and OESs are required to notify their competent authority of their status under the Regulations.

Which competent authority applies to which sector is set out in the Regulations e.g. the Secretary of State for Health is the competent authority for English OESs operating in the health sector.

Competent authorities have a range of regulatory functions, including undertaking enforcement action. For example, the ICO can issue RDSPs with a monetary penalty of up to £17 million for non-compliance with the Regulations.

PROPOSED REFORMS

A new EU NIS 2 Directive came into force on 16 January 2023, which will replace the Directive from 18 October 2024 and broaden the scope of regulation to cover more sectors and services as well as introducing new reporting obligations and stricter enforcement requirements.

Post-Brexit, the EU NIS 2 Directive will not apply directly in the UK, but the government has separately reviewed the Regulations and proposed a number of reforms in order to improve the UK's cyber resilience, including expanding the meaning of 'digital services' under the Regulations to include managed services.

KEY CONTACTS

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

Beverley Flynn
Partner
T: +44 (0)1483 734264
M: +44 (0)7769 708486
E: beverley.flynn@stevens-bolton.com

Gary Parnell
Partner
T: +44 (0)1483 734269
M: +44 (0)7738 695666
E: gary.parnell@stevens-bolton.com

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

PERSONAL\19177903v2