ARTHUR COX

Group Briefing
October 2018

Can we Protect our Businesses from Cyber Threats? New EU Cyber Security Regulations Published

Ireland Client Service Law Firm of the Year 2018
Chambers Europe Awards

Ireland Law Firm of the Year 2018
International Financial Law Review (IFLR) Europe Awards

Advised on Equity Deal of the Year 2018 – Allied Irish Banks IPO
International Financial Law Review (IFLR) Europe Awards

Ireland Law Firm of the Year 2018
Who's Who Legal

Ireland Law Firm of the Year 2017
Chambers Europe Awards

Best Firm in Ireland 2018, 2017 & 2016
Europe Women in Business Law Awards

Best National Firm for Women in Business Law 2018, 2017 & 2016
Europe Women in Business Law Awards

Best National Firm Mentoring Programme 2018, 2017 & 2016
Europe Women in Business Law Awards

Best National Firm for Minority Women Lawyers 2018
Europe Women in Business Law Awards

For Irish businesses deemed to be Operators of Essential Services or Digital Service Providers new cyber security regulations impose comprehensive standards in cyber-security.

As a basic point, the regulations are not personal data focused, but rather focus on continuity of EU business operations. While a particular cyber incident could (well) overlap with corporate obligations under GDPR, criminal law and regulatory requirements, for example, the focus of the regulations is specific.

These new rules are contained in the EU Directive on the Security of Network and Information Systems, known as the NIS Directive. The Irish transposing legislation, the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 (the "2018 Regulations") and the Commission Implementing Regulation (EU) 2018/151 (referred to here as the "Implementing Regulation"), add further detail to the obligations.

WHO CAN BE DEEMED TO BE AN OES?

OESs are designated as such by either the Minister for Communications, Climate Action and the Environment or the Central Bank of Ireland, depending on their sector of business. They are operators of essential services within one of seven categories of economic and societal activity, including energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, and digital infrastructure. Interestingly, non-traditional utilities in the form of providers of digital infrastructure, consisting of IXPs, DNS service providers and TLD name registries, also fall within the definition of OESs. (It is also noteworthy that banking is within scope under the Irish transposing legislation, whereas the United Kingdom availed of an exemption in the NIS Directive to exclude banking from the remit of their implementing legislation.) One sector not included is telecoms, on the basis that they are separately regulated in the information security area.

WHO CAN BE DEEMED TO BE A DSP?

DPSs are providers of digital services which are normally provided for remuneration, at a distance and by electronic means and at the individual request of the recipient of such services.

Further, in order to be caught by the 2018 Regulations, the digital service must be provided in the European Union, by a company which has its main establishment or a designated representative in Ireland, and which is not a micro or small enterprise.

According to Schedule 2 of the 2018 Regulations, DSPs fall into the following three categories:

» online marketplaces;

» online search engines; and

» cloud computing services.

WHAT ARE THE OBLIGATIONS FOR BUSINESSES?

OESs need to take "*appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the network and information systems.*" Further, steps need to be taken to prevent and minimise the impact of any incident which affects the security of their network and information systems to ensure the continuity of the service which the OES provides.

OESs are required to notify the computer security incident response team ("**CSIRT**"), a unit of the Department of Communications, Climate Action and Environment, "*of any incident concerning it that has a significant impact on the continuity of an essential service provided by it in respect of which it is designated as an operator of essential services.*" The same notification requirement applies where the OES relies on a DSP and such DSP is affected by an incident which has a significant impact on the continuity of the essential service provided by the OES.

In similar vein, DSPs are required to take "*appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use*" in the context of offering services within the Union.

The Directive supplies a list of elements which shall be taken into account when implementing such proportionate technical and organisational measures. These include:

» the security of systems and facilities;

» incident handling;

» business continuity management;

» monitoring, auditing and testing; and

» compliance with international standards.

DSPs are required to notify the CSIRT "*of any incident that has a substantial impact on the provision by it of a digital service [...] offered by it within the Union.*" What is considered to be a '*substantial impact*' is further clarified in the 2018 Regulations but also in the Implementing Regulation which states that it is an incident where at least one of the following applies:

» The service is unavailable for at least 5 million user hours;

» More than 100,000 users across the EU are affected;

» A risk to public safety, public security or loss of life is created; or

» Damage is caused to at least one user in the EU which exceeds €1,000,000.

Notifications of an incident to the CSIRT need to be made within 72 hours after becoming aware of it. Similarly notifications of the resolution of these incidents need to be made within 72 hours of resolution.

It should be noted that in relation to both OESs and DSPs, the CSIRT may decide to inform the public about the incident where the CSIRT considers this to be necessary, in particular where there is a risk to other OESs or DSPs.

Interestingly, the 2018 Regulations also allow for voluntary notifications to be made by companies which are not OESs or DSPs, stating that the company which makes such a notification shall not be subject to any obligations to which it would not have been subject if it had not made the notification, thus encouraging the notification of incidents by ensuring that businesses will not be subjected to the 72 hour reporting requirements and the associated offences.

DSPs are also required to keep sufficient documentation to enable the competent authority, which in Ireland is the Minister for Communications, Climate Action and Environment, to verify the compliance with their security requirements.

WHAT ARE THE OFFENCES UNDER THE IRISH TRANSPOSING REGULATIONS?

Under the 2018 Regulations, it is an offence for both OESs and DSPs to fail to notify the CSIRT of an incident referred to above or of the fact that such an incident has been resolved.

It is further an offence for a person to fail to comply with a request, instruction or direction from an authorised officer in the exercise of their functions. Where a person who has been served with a compliance notice fails to comply with same, or causes or permits another person to contravene the notice, an offence is likewise committed.

The 2018 Regulations provide that where offences are committed by companies, but have been committed with the consent or connivance of one of its directors or other officers, or where such person has been acting with wilful neglect, that person as well as the company are guilty of an offence and may be prosecuted.

WHAT ARE THE CONSEQUENCES OF NON-COMPLIANCE?

Under the 2018 Regulations, all offences are punishable on summary conviction to a fine of €5,000 or on conviction on indictment to a fine not exceeding €50,000 (in the case of an individual) or not exceeding €500,000 (in the case of a company). These penalties are noticeably less than those set out in the GDPR. For corporates, possible criminal prosecution, rather than penalties, is the main fact to consider.

Furthermore, where persons are convicted under the 2018 Regulations, the Court will order the person to pay the prosecutor a sum equal to the costs and expenses reasonably incurred by the prosecutor in prosecuting the offence, unless there are "*special and substantial reasons*" for not doing so.

As provided for in the NIS Directive, the 2018 Regulations also make provision for cross-border cooperation in cyber security matters.

CONCLUSION

OESs and DSPs need to put the NIS Directive and Irish transposing regulations on their agenda and ensure they are in compliance with same. The extent to which the Directive and the 2018 Regulations will have an effect in practice will become clear over the next few months. However, these are significant pieces of legislation because for the first time businesses across the EU need to adhere to a common standard in cyber security. Given the number of high-profile date breaches and cyber-incidents which have occurred in the recent past, this is an area in which OESs and DSPs will be under intense scrutiny by the public and therefore will need to ensure they are in compliance with their legal obligations.

The question is, will this be enough?

We will discuss the position of DSPs in more detail in a subsequent article.

With thanks to Max Riegel for his help in preparing this article.

KEY CONTACT

PEARSE RYAN
PARTNER
+353 1 920 1180
pearse.ryan@arthurcox.com