TECHNOLOGY

Digital Infrastructure Providers and Requirements under the NIS Directive – What They Need to Know

2 July 2020

This briefing discusses the status of a particular category of providers of technology, known as Digital Infrastructure providers, which are vital for the continued operation of the internet and thus e-commerce, with reference to their obligations under specific EU legislation focusing on the security of networks and information systems.

Pearse Ryan
Consultant
+353 1 920 1180
pearse.ryan@arthurcox.com

Maximillian Riegal
Associate
+353 1 920 1475
Max.Riegel@arthurcox.com

On 9 May 2018, the Directive on security of network and information systems[1] ("**NIS Directive**") entered into full force and effect across the European Union. The NIS Directive is the first EU substantive initiative in the area of information security, not specific to personal data (which is dealt with under data protection legislation). The NIS Directive applies to industry participants in specific regulated and unregulated market sectors, such as financial services, healthcare providers and transport. It is, by global standards, an innovative approach to securing the information security of operators of essential services ("**OESs**") and digital service providers ("**DSPs**"). As a Directive, Member States were required to implement the NIS Directive in national law. Ireland opted to implement the NIS Directive by way of the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018[2] (the "**2018 Regulations**"), which were signed by then-Minister for Communications, Climate Action and Environment, Denis Naughten, TD, on 18 September 2018.

Legislating for information security is inherently difficult, especially in the area of assessment of compliance with standards and requirements written in broad terms, with, for example, terminology used that includes an obligation to take "*appropriate and proportionate*" measures to manage information security risk. Information security is, at its base, a sub-set of corporate risk management. Applying an '*appropriate and proportionate*' standard across the various threat vectors, some of which have the benefit of international standards applying while others do not, is difficult. This difficulty in interpreting and applying requirements is reflected in the Irish NIS Compliance Guidelines for Operators of Essential Services, which state that "*It is recognised that it is not possible to fully protect information system from all potential security incidents. As such, the security requirements in the NIS Regulations are aimed at reducing risk throughout the incident response lifecycle, and should not be considered to render systems or entities invulnerable*".

This difficulty in interpretation holds true for both the national designated competent authorities, who are tasked with enforcing the NIS Directive within their respective jurisdictions, as well as OESs and DSPs, who are subject to the requirements of the NIS Directive. The NIS Directive was seen as ground-breaking when originally conceived and legislated for, but increasingly has come to be viewed simply as a necessary measure. This is due to the almost complete dependence of economic operators on networks and information systems for the conduct of their business, as well as the ever-increasing consumption of digital services by both businesses and consumers. Arguably, the

1 (EU) 2016/1148.

2 S.I. No. 360 of 2018.

current COVID-19 pandemic has pushed businesses and consumers towards near total consumption of digital services for work and leisure. It remains to be seen how lasting those changes will be when (and if) current restrictions are lifted completely.

As mentioned above, the NIS Directive and the 2018 Regulations identify OESs, which are listed in Annex II and Schedule 1, respectively. They consists of various categories of businesses which provide services that are considered crucial to the functioning of society (such as energy, healthcare and transport). Businesses falling under the definition of an OES had to be identified and contacted by the competent Irish authority, the Minister for Communications, Climate Action and Environment, prior to 9 November 2018, notifying them of their status as an OES. Member States may identify OES which meet a number of criteria, two of which, as per the 2018 Regulations, are geographical in nature, namely that the services are provided in the State and the "*person has an establishment in the State*". As with data protection legislation, determining what this means and, in particular, which competent authority applies to a provider of services from outside the EU into the EU, or from one Member State to other(s) can be difficult. The NIS Directive and 2018 Regulations contain provisions, including those giving effect to the NIS Directive requirement that "*where an entity provides a service .... in two or more Member States, those Member States shall [before identification as an OES] engage in consultation with each other*". We have seen clients preferring to fall under one competent authority rather than another, but forum shopping is not something the NIS Directive encourages, given its top down OES identification model.

Included in the categories of OESs are the following providers of '*Digital Infrastructure*':

- Internet Exchange Point (IXPs) Operators[3];
- Domain Name Service (DNS) providers[4]; and
- Top-level Domain (TLD) name registries[5]

These categories of Digital Infrastructure providers are not to be confused with DSPs (i.e. online marketplaces, online search engines and cloud computing services) to which a different set of rules apply and which are listed in Annex III and Schedule 2, respectively. We have dealt with DSPs in a different publication, which can be found here.

Under the provisions of the NIS Directive and the 2018 Regulations, OESs need to take "*appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems.*" Furthermore, OESs are required to notify the national Computer Security and Incident Response Team ("**CSIRT**") within 72 hours of becoming aware that an incident has taken place which has a "*significant impact*" on the continuity of the essential service which they provide. In Ireland the CSIRT is a unit of the Department of Communications, Climate Action and Environment and acts as the competent authority for Digital Infrastructure providers (as a sub-set of OES's) at national level, tasked with monitoring the application of the NIS Directive in Ireland.

The factors which must be taken into account when determining whether an incident is having a significant impact on the continuity of the service provided include (in summary):

- The number of users affected by the disruption of the essential service;
- The dependency of the other sectors referred to in Annex II on the service provided by that entity;
- The duration of the incident;
- The geographical spread with regard to the area affected by the incident; and
- The importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

Each of the above criteria includes further sub-criteria. As stated above, OESs must notify the CSIRT of incidents within 72 hours and must also notify the resolution of such incidents within the same timeframe. Maximum fines for failure to do so, as well as for other offences under the 2018 Regulations, range from €50,000 (in the case of an individual) to €500,000 (in the case of a body corporate)[6]. Where it can be proved that offences have been committed with the consent or connivance of a director or other officer of the company, or where they have been acting with wilful neglect, that person as well as the company are guilty of an offence and may be prosecuted. By the standards of other legislation, including, in particular, GDPR, these fines are not large. They are, however, dissuasive, can be accompanied by criminal proceedings and are part of a series of audit and administrative powers held by the regulator, which if exercised would be a serious matter for the Digital Infrastructure provider. Effectively, it was administrative powers which were of most concern to Irish business and public sector controllers and processors of personal data under the Irish data protection legislation which applied prior to the GDPR.

It should also be noted that, in addition to the threat of criminal penalties, the CSIRT may inform the public about incidents where they consider that public awareness is necessary to deal with the incident, or to prevent the same or a similar incident occurring in respect of other OESs.[7] Undoubtedly, it represents a significant risk to the reputation of companies, and their directors and other officers, where such information enters the public domain.

The above emphasises the point that Digital Infrastructure providers in Ireland need to be aware of their obligations under the new cyber security legislation. Non-compliance, in terms of adherence to the required level of information security and failure to report any incidents, may not only result in criminal liability for the company and/or its directors or officers[8], but also lead to negative publicity where such incidents are made public. In order to mitigate such risks, being NIS Directive-compliant needs to be on the agenda of each Digital Infrastructure provider in Ireland. If there was ever any doubt as to whether Digital Infrastructure providers met the test for designation as an OES, being businesses which provide services that are considered crucial to the functioning of society, the current COVID-19 related restrictions demonstrate the importance of the internet to the functioning of public life.

3 These are facilities that allow for the exchange of internet traffic between networks.

4 The naming systems which turn queries for domain names such as www.arthurcox.com into numerical IP addresses, similar to a phone book.

5 TLD name registries administer and operate the registration of internet domain names under a specific top-level domain, for example ".com".

6 Regulation 22(14).

7 Regulation 18(8).

8 Regulation 33(1).