JONES DAY

AUGUST 2016

COMMENTARY

The New EU Cybersecurity Directive: What Impact on Digital Service Providers?

On August 8, 2016, the Directive on Security of Network and Information Systems ("NIS Directive") entered into force after it had been approved by the European Parliament on July 6, 2016, and published in the Official Journal of the EU on July 19, 2016. Andus Ansip, the European Commission Vice-President for the Digital Single Market, stated that "this Directive is the first comprehensive piece of EU legislation on Cybersecurity and a fundamental building block for our work in the area." Indeed, the NIS Directive will provide measures to boost the overall level of cybersecurity in the European Union ("EU") by imposing minimum harmonization rules for EU Member States.

The NIS Directive provides guidelines for two types of entities: (i) "essential service operators" within the energy, transport, banking, financial market infrastructure, health, drinking water, and digital infrastructure sectors, and (ii) "digital service providers," including entities such as online marketplaces, online search engines, and cloud computing service providers.

Considerable disagreement surrounded the inclusion of digital service providers within the draft NIS Directive, bringing opposition from the European Parliament, various Member States, and entities falling under the definition of "digital service provider." These opponents viewed cyberattacks on digital service providers as insufficiently significant and therefore argued against additional regulation, which would potentially negatively affect innovation. While the final NIS Directive does extend to digital service providers, it subjects them to a lighter regulatory touch than essential service operators.[1]

For the purposes of this *Commentary*, we will focus on such digital service providers.

Relevant Terms

A "**digital service provider**" ("DSP") is defined as a legal person that provides "service normally provided for remuneration, at a distance, by electronic means[2] and at the individual request of a recipient of services."

Notably, as stated in the NIS Directive's recitals, DSPs do not include "hardware manufacturers and software developers." In this respect, technical and organizational measures imposed on digital service providers have to adhere to the "state of the art" but will "not require a particular commercial information and communications technology product to be designed, developed

or manufactured in a particular manner." Thus, while the NIS Directive includes recitals highlighting the key role of hardware and software developers in enabling operators of essential services and digital service providers to secure their network and information systems, it does not impose additional regulation with respect to these. Indeed, hardware and software products are already subject to existing rules on product liability.

DSP services cover the three following categories (NIS Directive (Annex III)): "online marketplace," "online search engine," and "cloud computing services":

- "**Online marketplace**" covers "a digital service that allows consumers and/or traders to conclude online sales or services contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace." Such definition should not cover online services serving only as an intermediary to third-party services through which a contract can ultimately be concluded, as indicated in the recitals to the NIS Directive.
- "**Online search engine**" covers "a digital service that allows users to perform searches of all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found." The scope of the NIS Directive does not extend to either the provision of search functions that are limited to the content of a specific website, or services that compare the price of particular products or services from various traders.
- "**Cloud computing service**" means "a digital service that enables access to a scalable and elastic pool of shareable computing resources." According to the NIS Directive's recitals, such computing services include resources such as networks, servers, or other infrastructure, storage, applications, and services.

Notably, while the regulation of providers of other categories of services such as streaming, major online computer games, digital distribution platforms for application software, and social network providers was debated during the legislative process, they were ultimately left out of the scope of the Directive.

DSP Obligations

Security Requirements. The NIS Directive aims at implementation of "state of the art" measures. It requires the following from DSPs:

- Identify and take appropriate technical and organizational measures to manage the risks facing the security of the network and information systems used in offering services within the EU. Such measures must adhere to the "state of the art" and take into account the following elements: (i) security of systems and facilities; (ii) incident management; (iii) business continuity management; (iv) monitoring, auditing, and testing; and (v) compliance with international standards.
- Take measures to prevent and minimize the impact of incidents affecting the security of their network and information systems on services offered within the EU, with a view toward ensuring service continuity.

Incident Notification Requirements. DSPs must promptly notify the competent authority or "Computer Security Incident Response Team" ("CSIRT") designated by the EU Member State of any incident having a substantial impact on the provision of a service offered within the EU. Notifications must include information to enable the competent authority or CSIRT to determine the significance of any cross-border impact. However, the notification should not expose the notifying party to increased liability.

The following parameters under the NIS Directive should be considered when determining the significance of the impact of an incident:

- The number of users affected by the incident, in particular users relying on the service for the provision of their own services;
- Duration of the incident;
- Geographical spread with regard to the area affected by the incident;
- Extent of the disruption of the functioning of the service; and
- Extent of the impact on economic and societal activities.

The obligation to notify applies only if the DSP has access to the information required to assess an incident's impact in relation to the aforementioned parameters.

Implementation, Post-Notification Procedure, and Enforcement of the Directive

Regarding implementation of the NIS Directive, EU Member States are required to adopt the Directive's strategy for regulatory measures for cybersecurity within the EU, to create a computer security incident response team for EU nations to address cross-border security incidents, and to establish a unified strategic cooperation group to encourage Member States to exchange information.

National Strategy for the Security of Network and Information Systems. EU Member States must adopt a national strategy defining the objectives, as well as appropriate policy and regulatory measures, in order to achieve a high level of security. In this respect, EU Member States must designate:

- A national single point of contact responsible for coordinating issues to facilitate cross-border cooperation; and
- One or more CSIRTs responsible for risk and incident handling on a national level by providing early warnings and alerts, sharing information about incidents and risks with relevant stakeholders, building public awareness regarding online activities and associated risks, and working toward the development of standardized practices for cybersecurity.

Post-Notification Procedure. After consulting the DSP concerned, the notified competent authority or CSIRT (and, where appropriate, the authorities or CSIRTs of other EU Member States concerned) may inform the public about individual incidents or require the DSP to do so, if it determines that public awareness is necessary to prevent an incident or respond to an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

Enforcement. EU Member States should ensure that the competent authorities take action, if necessary, through *ex post* supervisory activities, when provided with evidence that a DSP does not meet the requirements regarding security or incident notification. Such evidence may be submitted by a competent authority of another Member State where the service is provided.

In relation to such *ex post* supervision, the competent authorities have the power to:

- Require DSPs to provide information needed to assess the security of their networks and information systems, including documented security policies; and
- Require that DSPs remedy any failure to fulfill the requirements regarding security and incident notification.

The NIS Directive requires EU Member States to set out rules on penalties applicable to infringements of the national provisions adopted pursuant to the Directive and to take all measures necessary to ensure their enforcement. Penalties must simply be "effective, proportionate and dissuasive," thereby leaving the establishment of specific rules on sanctions for noncompliance to each Member State.

Jurisdiction and Territoriality/Extraterritorial Reach of the Directive

A DSP is deemed to be under the jurisdiction of the EU Member State where its main establishment (i.e., head office) is located.

If a DSP's main establishment is in a given EU Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment and the competent authorities of the other Member States must cooperate and assist each other.

Standardization is encouraged under the NIS Directive to promote harmonious implementation of the security requirements and incident notification procedures.

DSPs having their main establishment outside of the EU could nevertheless be considered to fall within the scope of the Directive if they offer services within the EU. They must then designate a representative based within the EU. Pursuant to the NIS Directive, however, mere accessibility to a DSP's website in the EU or to an email address and other contact details is insufficient. However, factors such as the use of a language

or a currency generally used in one or more Member States, with the possibility of ordering services in such other language, and/or the mentioning of customers or users who are in the EU, may make it apparent that the DSP in fact envisages offering services within the EU.

Relationship with General Data Protection Regulation

Data controllers and processors, as DSPs, may be simultaneously subject to both the NIS Directive and the General Data Protection Regulation ("GDPR") (Regulation (EU) 2016/679 of April 27, 2016), which contains various new protective measures for EU data subjects, as well as significant fines and penalties for noncompliance. A data security incident could therefore trigger notification obligations under both regulations.

A significant distinction, however, can be made with regard to the type of data protected under the NIS Directive and the GDPR. While the NIS Directive covers any type of data breach, the data protected under the GDPR is limited to "personal data," which it defines as "any information relating to an identified or identifiable natural person ("data subject")."

Furthermore, the NIS Directive encompasses not only data breaches but also any "incidents" that could affect the security of DSP networks and impact the provision of service.

Outlook

The Member States will have until May 9, 2018, to implement the NIS Directive into their national laws.

The NIS Directive will require DSPs and other concerned entities to carefully review existing network security and to establish proper incident notification measures in view of meeting the terms of the Directive.

Entities within the scope of the NIS Directive must implement "state-of-the-art" security measures that "shall ensure a level of security appropriate to the risk." To implement this level of security, businesses will need to have a comprehensive and auditable security program. To be prepared, businesses should:

- Designate an individual or group within senior management to evaluate the applicability of the NIS Directive to the business and develop a preparedness plan.
- Conduct a security impact assessment.
- Review all internal security processes and prepare self-audit capabilities required by national authorities.
- Adopt an internal security and response strategy that is coordinated with the board of directors, chief legal officer, and other senior executives.
- Implement an incident response program that will comply with breach reporting requirements in a timely manner.
- Consider the adoption of a security strategy that can be integrated with the new NIS threat intelligence sharing program.

The NIS Directive's potential reach over entities established outside of the EU also calls for companies to evaluate whether their activities may bring them within the scope of the Directive. As penalties for noncompliance are yet to be determined by each Member State, this is even greater reason for companies to ensure that they do not fall foul of the NIS Directive.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Elizabeth Robertson
London
+44.20.7039.5204
erobertson@jonesday.com

Jörg Hladjk
Brussels
+32.2.645.15.30
jhladjk@jonesday.com

Rhys E. Thomas
London
+44.20.7039.5101
rethomas@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Paloma Bru
Madrid
+34.91.520.3985
pbru@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Laurent De Muyter
Brussels
+32.2.645.15.13
ldemuyter@jonesday.com

Gregory P. Silberman
Silicon Valley
+1. 650.739.3954
gpsilberman@jonesday.com

Olivier Haas
Paris
+33.1.56.59.38.84
ohaas@jonesday.com

Jonathon Little
London
+44.20.7039.5224
jrlittle@jonesday.com

Giuseppe Mezzapesa
Milan
+39.02.7645.4001
gmezzapesa@jonesday.com

Rémy Fekete
Paris
+33.1.56.59.39.90
rfekete@jonesday.com

Endnotes

1 Example: Digital service providers must notify incidents having a "substantial impact," whereas operators of essential services are subject to the broader-ranging requirement of notifying any incident having a "significant impact," and the parameters for determining such incidents are more narrowly defined.

2 "Electronic means" cover those services "sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means." (Article 1(1)(b), Directive (EU) 2015/1535 of the European Parliament and of the Council of September 9, 2015, laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services).