Bloomberg BNA

Privacy and Security Law Report®

NIS Directive

The European Union is arming itself with a first-time ever cybersecurity framework to promote a harmonized set of rules on cooperation, data security and breach notification across EU countries. Covered companies may generally expect all EU countries to have rules onsecurity requirements and breach notice requirements, but there is risk that the rules will undercut harmony and create a patchwork of compliance obligations, the authors write.

EU Adopts Cybersecurity Directive: Harmonized Rules for Security and Breach Notification for Selected Actors



BY ALEX VAN DER WOLK, SOTIRIOS PETROVAS AND RONAN TIGNER

The European Union is arming itself with a first-time ever cybersecurity framework to promote a harmonized set of rules on cooperation, data security and breach notification across member states. The Network and Information Security Directive (NIS Directive) was adopted by the Council in May and by Parliament on July 6 (15 PVLR 1447, 7/11/16). It is expected to enter into force in August.

Alex van der Wolk is a partner at Morrison & Foerster LLP in Berlin and is a member of the firm's Privacy & Data Security practice.

Sotirios Petrovas is an associate at Morrison & Foerster LLP in Brussels and is a member of the firm's Privacy & Data Security practice.

Ronan Tigner is an associate at Morrison & Foerster LLP in Brussels and is a member of the firm's Privacy & Data Security practice.

The NIS Directive is in line with the Digital Single Market strategy and is one of the first steps in achieving a comprehensive regulatory framework for online platforms. It can be summarized in three main components:

(i) promoting cooperation on cybersecurity issues among member states generally;

(ii) promoting a harmonized approach to security; and

(iii) enabling a uniform format for breach notification procedures.

Note that points (ii) and (iii) apply to a narrow scope of actors: Operators of Essential Services (i.e., 'critical

 ISSN 1538-3423

infrastructure' operators) and Digital Service Providers (e.g. providers of ecommerce services, cloud computing services, and search engines).

I. Context

The EU has thus far not implemented any compulsory set of rules specific to cybersecurity. Rules on cybersecurity and breach notification are defined at national level, despite the existence of the EU Network and Information Security Agency (ENISA)—an advisory body that issues recommendations and assists member states with the implementation of cybersecurity solutions. Companies have thus been facing a patchwork of sometimes inconsistent rules from one jurisdiction to another.

For example, in regard of data security requirements around personal information, some member states provide for security obligations as open norms without further specifying up front the type of security that is required, whereas countries such as Italy or Spain have very specific and detailed security measures that need to be applied. By the same token, obligations to notify data security breaches involving personal information differs greatly amongst EU countries. Breach notification obligations currently exist in countries such as Germany, the Netherlands, and Austria. In France, Poland, and Finland, mandatory notification exists for specific actors and entities (e.g., telecommunications operators). In Italy, breach notification is mandatory only if biometric and certain health data are affected. In other countries such as the U.K., Ireland, and Belgium, breach notification is recommended by regulators even though it is not mandatory by law. On top of these differences, even where there may be an obligation to notify, the exact conditions and the format of notification may differ significantly across countries.

Companies have thus been facing a patchwork of sometimes inconsistent rules from one jurisdiction to another.

II. Security and Breach Notification Obligations

The NIS Directive is designed to reduce the differences between member states by creating a common baseline across the EU (unless otherwise indicated, references are to provisions of the NIS Directive). Article 3. However, the scope of the Directive is narrow and targets only two types of actors: Operators of Essential Services (OESs) and Digital Service Providers (DSPs).

1. Operators of Essential Services

Definition. OESs are broadly defined in the Directive. These are operators in critical industries such as energy, transport, health and finance, and member states are tasked with identifying which organizations will qualify as OESs within six months after the deadline for transposing the Directive, i.e., by November 2018 (note that member states may already have legislation in preparation or in place to define what categories of organizations may be considered ''critical infrastructure'' entities which will be subject to the NIS Directive, such as the German Information Security Law of July 17, 2015).

Annex II of the NIS Directive includes a table with categories of entities that may qualify as OESs, and the Directive provides three criteria for the identification of OESs at Article 5(2):

(i) whether the service is ''essential for the maintenance of critical societal and/or economic activities;''

(ii) whether the provision of the service ''depends on network and information systems;'' and

(iii) whether an ''incident would have significant disruptive effects on the provision of that service.'' ''Disruptive effect'' is further qualified according to a number of factors to be considered, including the number of users relying on the service, the dependency of other sectors, and the impact on economy and public safety of incidents. Article 6.

Obligations. OESs will be subject to strict security requirements and regulatory oversight. Articles 14-15. The Directive imposes an obligation on member states to ensure that OESs take appropriate and proportional technical and organizational measures to manage risks, and prevent and minimize the impact of security incidents. OESs will have to report any incident having a significant impact on the continuity of services that are deemed essential, and will have to comply with information requests and instructions from competent national regulators.

2. Digital Service Providers

Definition. The NIS Directive applies to three types of digital services:

(i) Providers of **online marketplace** services, which means an online service allowing consumers and/or traders to conclude online sales and service contracts.

(ii) **online search engines**, and

(iii) **cloud computing services**.

Obligations. DSPs that meet a size threshold—micro- and small enterprises are excluded from the Art. 16(11) security and notification obligations—will have to take measures to manage cybersecurity risk (which includes reporting major incidents) for which they are subject to regulatory oversight. More specifically, pursuant to Article 16, DSPs are required to do two things:

(i) ''identify and take appropriate and proportionate technical and organizational measures'' to manage risks to network and information systems security; and

(ii) notify security incidents to competent authorities.

Regarding security measures (point 1), the Directive echoes the standard of ''reasonableness'' for which the U.S. industry has been advocating for several years, and the Directive explicitly indicates that the level of se-

  PVLR ISSN 1538-3423

curity must be appropriate to the risk posed, taking into account several factors such as: security of systems and facilities, incident handling, business continuity, monitoring/auditing/testing and compliance with international standards. These provisions in the Directive provide for high level obligations only, and specifically in regard of DPSs the NIS Directive attributes power to the European Commission to provide more detailed provisions by means of implementing acts. Although responsibility for implementing the Directive lies primarily with the member states, under EU law there is the possibility to empower the commission to adopt ''implementing acts'' where uniform conditions throughout the EU are required. Such implementing acts are then binding on the member states.

3. Discussion

In regard of DSPs, there are a number of aspects in the NIS Directive that stand out.

First, the definition of 'online marketplace' under the NIS Directive is drafted so that it applies to websites where online contracting is facilitated between consumers and traders (or between traders), rather than websites where a company sells its own products and services. Webshops and ecommerce websites are therefore not covered under the NIS Directive. If a service provider offering the online market links to a company's own website, then this is also not covered under the NIS Directive, unless the company's own website uses the service provider's computing services to facilitate online contracts (in which case the service provider is subject to the NIS Directive.

The Directive does not prescribe what concrete security measures need to be in place to manage cyber risks. The NIS Directive also does not restrict the criteria used to assess whether an incident has a significant or substantial impact on the relevant services (which triggers the reporting obligations) or the conditions under which a local regulator may/must inform the general public of an incident.

At the same time, where the NIS Directive provides for minimum harmonization as regards OESs (i.e. allowing member states to impose stricter requirements than those laid down in the NIS Directive, it provides for maximum harmonization in regard of DSPs. In respect of DSPs, the Directive provides that member states may not impose further security or notification requirements and attributes this specific power to the European Commission by way of implementing acts (Article 16(10)). This should enable DSPs to be treated in a uniform way across the Union, in a manner proportionate to their nature and the degree of risk they might face.

The Network and Information Security Directive requires each member state to adopt a national strategy on the security of network and information systems, and provides extensive details on the elements of such strategies.

The topic of enforcement is fully left to member states, both in regard of competent authority as well as fining powers. The Directive provides that national implementing legislation must confer upon competent authorities ''necessary powers and means'' to (i) assess compliance by OESs and DSPs, (ii) obtain information and evidence of compliance by OESs and DSPs, and (iii) instruct OESs or DSPs to take specific actions to remedy any deficiencies. But here too, the Directive does not further detail what powers and means it deems necessary for authorities to have, nor does it provide any guidance around penalties, other than that these should be ''clear, proportionate and dissuasive.'' This seems to allow for a great deal of variation amongst member states.

Finally, in regard of geographical scope of application, the NIS Directive provides for an extraterritorial reach in regard of DSPs. While the scope of application in regard of OESs is limited to those that have an establishment on the territory of a member state (provided that they have been designated as such by the member state pursuant to criteria provided by the Directive), the Directive is more broader in scope in regard of DSPs.

DSPs that have an establishment within the territory of a member state, *or* that offer services within the EU (even if there is no establishment within the EU) are subject to the Directive's requirements. This potentially opens up the scope of the Directive to a multitude of digital service providers that offer their services remotely from outside the EU.

The NIS Directive will create harmonized cooperation, data security and breach notification, but still leave a lot of room for variations amongst member states.

In regard of enforcement of such non-EU established DSPs, the Directive provides for a ''one-stop-shop''

principle, by allowing to submit to the authority of a single member state (provided services are offered in that member state). DSPs without establishment in the EU but who offer services within the EU are required to designate a representative in one of the member states, through which the DSP comes under the jurisdiction of that member state for all of its EU operations.

III. National Frameworks for Cybersecurity and Cooperation Between Member States

The NIS Directive requires each member state to adopt a national strategy on the security of network and information systems. Article 7 provides extensive details on the elements of such strategies and includes such measures as governance framework, measures to raise awareness on cybersecurity, research and development plans, etc.

With regard to cooperation, an EU cooperation group will be created to support strategic cooperation, draw up guidelines, and exchange best practices, and a network of computer security incident response teams will be put in place to ensure coordination and cooperation between member states at the operational level. Finally, each member state will have to designate a national authority responsible for implementation and cooperation with other EU countries.

IV. Conclusion and Next Steps

While the object of the NIS Directive is to create harmonization on cooperation, data security and breach notification across member states, it still leaves a lot of room for variations amongst member states. After implementation of the NIS Directive, covered companies may generally expect all EU member states to have rules in regard of security requirements and breach notification requirements, but there remains a risk of a patchwork of different requirements they may end up having to comply with.

Companies should begin to consider and assess:

- whether they fall under the scope of the NIS Directive (i.e., are they offering critical infrastructure services, or covered digital services) and if so;
- how this could impact their business (e.g., need to adapt security policies), also considering the reforms required by the General Data Protection Regulation (e.g., ensure synergies and consistency between personal data breach and cybersecurity breach procedures); and
- in which member states would they be most affected, and for what implementations at member state level they may want to advocate.

The NIS Directive was published in the Official Journal of the European Union July 19. Member states will subsequently have twenty-one months to transpose the Directive into national law, i.e., by May 2018, and six additional months to identify OESs that will be covered.

  PVLR ISSN 1538-3423