EU: new obligations for digital services providers and operators of essential services

Intellectual Property and Technology News

28 JUN 2016

By: Carol A. F. Umhoefer | Mathilde Hallé

First proposed by the European Commission in 2013, the long-awaited draft Directive on Network Information Security (the NIS Directive) was agreed upon by the European Parliament and the Council in December 2015.[1] In line with the EU's broader Cyber Security Strategy, [2] the NIS Directive is a significant achievement towards a more secure cross-border cyberspace with a high shared level of network and information system security. It is expected that the European Parliament and Council will soon vote to implement the Directive. Member states will then be required to implement it within 21 months.

The NIS Directive's scope The NIS Directive's principles will apply to "digital services providers" (DSPs) and "operators of essential services" (OESs).

DSP refers to "any legal person that provides a digital service" and expressly encompasses online search engines, cloud computing services and online marketplaces. DSPs are required to take appropriate technical and organizational measures to manage risks related to the security of networks and information systems.

For classification as an OES, a service is deemed "essential" when it is (i) essential for maintenance of critical societal and/or economic activities; (ii) its provision depends on networks and information systems; and (iii) an incident involving network information systems would have a "significant" disruptive effect on the provision of such service. "Essential services" include energy, transport, banking, financial market infrastructures, the health sector, water supply and distribution, and digital infrastructures. The actual identification of OESs is left to the member states. Internet exchange points, domain name systems service providers and top-level domain name registries are considered OESs (not DSPs).

Member state laws shall ensure that OESs and DSPs are required to take appropriate technical and organizational steps to manage risks related to network and information system security, and to prevent and minimize the impact of incidents affecting network and system security. For incidents having a "significant impact on the continuity of essential services," OESs and DSPs are required to notify the national authority in charge of cybersecurity matters or the national Computer Security Incident Response Team (CSIRT).

Member state cooperation

The Directive creates an operational network among EU member states on cybersecurity focusing on risks and incidents affecting networks and information systems in the EU and including representatives from all member states, the European Commission, and the European Network and Information Security Agency. Another network of representatives from member states' CSIRTs will exchange information on services, operations and cooperation capabilities, coordinate incident responses and support member states in addressing cross-border incidents. Member states are required to

develop a national NIS strategy with clear objectives and appropriate policies and regulatory measures to achieve a higher level of network and information system security.

What now?

At this stage, the scope and obligations of the NIS Directive are vague, leaving few avenues for businesses that wish to prepare for it.

Because the NIS Directive leaves identification of OESs to the member states, potential OESs − i.e., operators meeting the criteria set forth by the NIS Directive − should closely monitor the implementation of the Directive in the EU countries where they are established. Engaging with member states in establishing OES lists may also be beneficial. Given that no formal identification procedure currently exists regarding DSPs, businesses must carefully self-assess whether they fall within the broad definition. Importantly, the NIS Directive also applies to DSPs that merely offer digital services within the EU, even if they are not established in a member state.

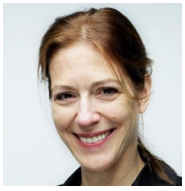
Operators likely to fall within the Directive's scope should, as a first step, review their security measures and notification procedures and perform a gap analysis. Although many businesses already face similar local obligations, for others the new regime may be a significant operational challenge, requiring preparation and important investments.

Find out more by contacting nay of the authors.

[1] See this page.

[2] See this page.

AUTHORS



Carol A. F. Umhoefer
Partner
Miami | T: +1 305 423 8500
carol.umhoefer@dlapiper.com

Mathilde Hallé
Associate
Paris | T: +33 1 40 15 24 00
mathilde.halle@dlapiper.com