CLIFFORD
CHANCE

Briefing note September 2016

NIS Directive adopted: cyber-security taken to the next level

As of 2014, 88% of the world malicious web resources were located in Europe and North America; it was time to act. On 6 July 2016 the European Parliament adopted the final version of Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"). This new instrument is set to establish a cyber-security framework with new onerous requirements.

Transport, energy, financial services, health, e-commerce, cloud computing services, search engine businesses in the loop

The Directive introduces cyber-security-related obligations for operators of essential services, i.e., entities that depend on networks to provide services essential for the maintenance of critical activities, in sectors such as transport (e.g. air carriers, airport managing bodies); energy (electricity, oil, gas operators), finance (e.g. credit institutions), health (e.g. hospitals and private clinics), digital service providers (e-commerce, cloud computing and search engine operators). It will be up to the Member States to identify operators of essential services with an establishment on their territory.

Contractors indirectly caught by the NIS Directive?

Operators of essential services may try to pass on their cyber-security obligations to their suppliers or subcontractors in order to ensure a full compliance with the NIS Directive over the whole business chain. For instance, aircraft manufacturers and pharmaceutical companies may face cyber-security contractual obligations similar to those set out in the NIS Directive.

Onerous cyber-security obligations

Networks and information systems cyber-security requirements for providers of essential services will include:

- Risk management;
- Mandatory notification to the competent national authority in case of incidents;
- Mitigation of the impact of incidents.

Compliance with these requirements will notably involve implementation of (i) highly-secured technical infrastructures and (ii) upgraded internal policies to ensure threats are monitored and notified if necessary. Actual requirements will differ within the EU as the NIS Directive allows Member States to maintain or enact stricter domestic provisions.

Cyber-security requirements also apply to digital service providers, however lightened as Member States will not be able to enact stricter provisions.

Operators that fail to comply with the cyber-security requirements will face pecuniary sanctions determined by Member States.

Some precedents in France and Germany

Some Member States have already implemented cyber-security provisions, especially concerning operators of essential services.

In France, under the 18 December 2013 military programming law[1], operators of critical importance are subject to specific cyber-security requirements (e.g. internal controls, breach detection and reporting). However, such law does not cover digital service providers.

---

[1] *Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire*

Similarly, in Germany, the “Act to Increase the Security of Information Technology Systems” of 2015 provides for minimum levels of cyber-security in critical infrastructures of companies essential to national interests.

Get prepared

Companies need to start preparing for a set of strict and complex regulatory regime that encompasses the NIS Directive and the EU General Data Protection Regulation[2].

From a legal standpoint, this notably includes:

- Due diligence: Review of contracting documentation to identify any risk areas (e.g. with suppliers and subcontractors).
- Contractual enhancement: Where possible adjust contracts (e.g. as regards liability, indemnification and warranty provisions) to anticipate the upcoming EU digital framework.
- Policies: Create or adapt cyber-security policies to have robust processes in case of incidents.

[2] *See our client briefing "Political agreement on the EU General Data Protection Regulation – the data protection "big bang" – December 2015*

Contacts

Dessislava Savova
Partner, Paris

Paris Cyber Risk and TMT Team leader

T: +33 1 44 05 54 83
E: Dessislava.Savova
@cliffordchance.com

Alvin Khodabaks
Partner, Amsterdam

Global Cyber Risk Team leader

T: +31 20711 9374
E: Alvin.Khodabaks
@cliffordchance.com

Luke Tolaini
Partner, London

Risk and Crisis Management expert

T: +44 207006 4666
E: Luke.Tolaini
@cliffordchance.com

Grégory Sroussi
Senior Associate, Paris

Cyber Risk and TMT expert

T: +33 1 44 05 52 48
E: Gregory.Sroussi
@cliffordchance.com

Jaap Tempelman
Senior Associate, Amsterdam

Cyber Risk and TMT expert

T: +31 20711 9192
E: Jaap.Tempelman
@cliffordchance.com

Richard Jones
Director, London

Cyber Risk and Data Privacy

T: +44 207006 8238
E: Richard.Jones
@cliffordchance.com

Jonathan Kewley
Senior Associate, London

Cyber Risk and TMT expert

T: +44 783489 0170
E: Jonathan.Kewley
@cliffordchance.com