September 2016

MANDATORY EU CYBERSECURITY STANDARDS IN CRITICAL BUSINESS SECTORS AND IN DIGITAL SERVICES

The EU Cybersecurity Directive[1], known as the "**NIS Directive**" was published on 19 July 2016 in the Official Journal of the European Union. The NIS Directive entered into force on 8 August 2016 and the Member States will have to transpose the Directive into their national laws by **9 May 2018**.

The NIS Directive pursues a high common level of security of network and information systems within the EU and therefore uniform protection against incidents. It is considered "*the first comprehensive piece of EU legislation on cybersecurity*[2]".

WHO IS DIRECTLY IMPACTED BY THE NIS DIRECTIVE?

(1) **Operators of an essential service** (presumed to be vital for our economy and society and, moreover, relying heavily on ICTs): energy, transport, banking, financial market infrastructures (e.g. stock exchanges, central counterparties), health services, drinking water supply and distribution and digital infrastructure - as listed in Annex II to the NIS Directive. The competent authorities to be appointed by each Member State will prepare the list of the entities in these sectors with an establishment on their territory by **9 November 2018** (six months after the transposing deadline), which will be periodically updated thereafter.

For the purposes of this assessment to be carried-out by the competent national authorities pursuant to the NIS Directive, a service is deemed to be essential if the following cumulative criteria are met: (i) the service is essential for the maintenance of critical societal and/or economic activities; (ii) the provision of that service depends on network and information systems; and (iii) an incident would have significant disruptive effects on the provision of the service (which generally translates into number of users affected, the duration of the incident, the geographical spread, etc.).

(2) **Digital service providers**: online marketplaces, online search engines, cloud computing providers.

The NIS Directive does not apply to undertakings providing public communication networks or publicly available electronic communication services and to trust service providers, which are subject to separate specific security requirements. Moreover, at least equivalent special rules in specific and/or regulated sectors, such as financial markets and banking will continue to apply.

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union;

[2] Statement of the European Commission Vice-President Andrus Ansip, responsible for the Digital Single Market, welcoming the adoption of the first EU-wide rules on cybersecurity, European Commission – Statement, Brussels, 6 July 2016.

WHAT NEW OBLIGATIONS FOR THOSE ENTITIES ACTING IN THESE INDUSTRIES?

(1) Implementation of Preventive Security Measures

The operators of essential services and the digital service providers shall take **appropriate** and **proportionate technical** but also **organizational** measures (e.g. introduce appropriate compliance processes and standards) to **prevent** and **minimise** the impact of incidents affecting the security of the network and information systems used for the provision of the relevant services, **with a view to ensuring the continuity of those services**.

(2) Reporting Obligations

The operators of essential services and the digital service providers shall notify, without undue delay, the competent authority or the established CSIRT (computer security incident response teams network) of incidents having a **significant / substantial** impact on the continuity of the essential service / digital service provided. The notification must include information allowing an assessment of the cross-border impact of the incident, with a view to further allow prompt and relevant exchange of information across the EU regulatory network.

Member States have discretion to impose stricter security or notification requirements solely on operators of essential services but not on digital service providers.

NATIONAL FRAMEWORKS AT STATE LEVEL AND ACROSS-EU COLLABORATION

A significant part of the NIS Directive deals with the rules and frameworks to be established at the national level and with cooperation across the EU Member States, with a view to minimize the impact of potential cyber attacks.

The NIS Directive requires each Member State to have in place a national strategy on the security of network and information systems defining the strategic objectives, appropriate policy and regulatory measures to be implemented.

Moreover, each Member State must:

- designate one or more competent national authorities on the security of network and information systems, which shall monitor the application of the NIS Directive at the national level ("competent authority");
- designate a single point of contact on the security of network and information systems, which shall exercise a liaison function to ensure cross-border cooperation of Member State authorities ("single point of contact");
- designate a computer security incident response teams network ("CSIRT"), which shall monitor incidents at a national level, provide early warning,

alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents, respond to incidents, provide dynamic risk and incident analysis and situational awareness.

By the NIS Directive, a Cooperation Group, composed of representatives of Member States, the Commission and the European Union Agency for Network and Information Security ("ENISA"), shall be established in order to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems. The Cooperation Group will have, amongst others, the following tasks: (i) providing strategic guidance to CSIRTs network; (ii) exchanging best practice between Member States and, in collaboration with ENISA, assisting Member States in building capacity to ensure the security of network and information systems; and (iii) exchanging information and best practice on research and development relating to the security of network and information systems.

Furthermore, a network of the national CSIRTs is to be established in order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation. The CSIRTs network must submit a report to the Cooperation Group, assessing the experience gained through the operational cooperation, including conclusions and recommendations.

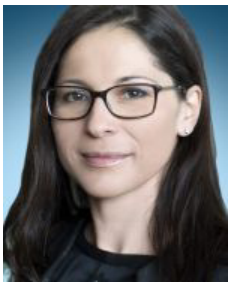
* * *

Romania has a draft cybersecurity law in public debate, which has been preliminarily approved by the Ministry of Communications (http://www.mcsi.ro/Transparenta-decizionala/Proiecte-2016). It remains to be seen how this project will progress considering the partial overlapping with the NIS Directive.

About WOLF THEISS

Wolf Theiss is one of the leading law firms in Central, Eastern and Southeastern Europe (CEE/SEE). We have built our reputation on a combination of unrivalled local knowledge and strong international capability. We opened our first office in Vienna almost 60 years ago. Our team now brings together over 340 lawyers from a diverse range of backgrounds, working in offices in 13 countries throughout the CEE/SEE region.

For more information about our services, please contact:



Ileana Glodeanu
Partner
ileana.glodeanu@wolftheiss.com
T: +40 21 308 81 00

Adelina Iftime-Blăgean
Senior Associate
adelina.iftime-blagean@wolftheiss.com
T: +40 21 308 81 00

Wolf Theiss Rechtsanwälte GmbH & Co KG
Gheorghe Polizu 58-60
13th floor, sector 1, 011062
Bucharest

Tel.: +40 21 308 81 00
Fax: +40 21 308 81 25
bucuresti@wolftheiss.com

www.wolftheiss.com