bpv GRIGORESCU ȘTEFĂNICĂ

THE LAW REGARDING THE TRANSPOSITION OF NIS DIRECTIVE

LEGAL AND TAX ALERT, 15 January 2019

The law regarding the transposition of the NIS Directive[1] was published in the Official Gazette of Romania no. 21 dated January 9th, 2019 (the "Transposition Law")[2]. The Transposition Law establishes minimum security measures, certain obligations for operators of essential services and digital service providers, including the obligation to notify security incidents occurring at their level.

Also, the Transposition Law provides fines that can reach up to 5% of the turnover of companies that do not fulfill their obligations.

The objectives of Transposition Law are: *(i)* to establish a framework for national cooperation and participation at European and international level in the field of network and information security assurance; *(ii)* to designate the competent national authority and the public and private law entities that have the competencies and responsibilities to enforce the provisions of the law, the single point of contact at national level and the national intervention team in case of computer security incidents; *(iii)* to establish security and notification requirements for operators of essential services and digital service providers and to set up mechanisms to update them in line with developments in network and information security threats.

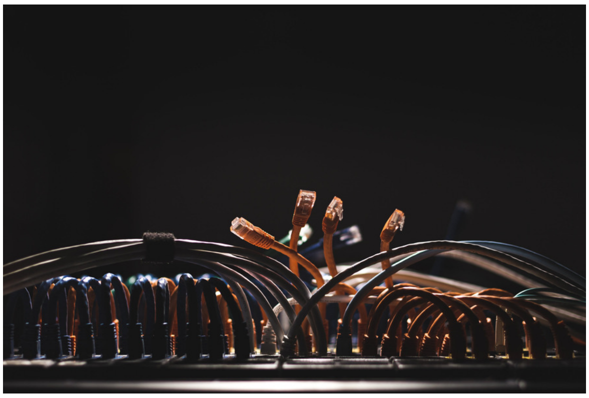
The competent authority in the field

Following the requirements of NIS Directive, the Transposition Law sets the Romanian National Computer Security Incident Response Team - CERT-RO as the competent authority at the national level for network and information security to provide essential services or provide digital services. The single point of contact at the national level and the IT security incident response team at the national level - national CSIRT are organised within CERT-RO.

[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 – NIS Directive;
[2] Law on ensuring a high common level of security of networks and information systems.

To whom the Transposition Law applies

The Transposition Law provisions apply to both operators of essential services and digital service providers. Thus, the Transposition Law is applicable to large companies that rely heavily on information and communication technology and are active in the following areas: energy (electricity, oil, gas), transport (air, rail, water, road transport), banking sector, financial market infrastructures, health sector (hospitals and private clinics), drinking water supply and distribution, digital infrastructure (IXP, DNS, TLD), digital service provision (online markets, online search engines, cloud computing).



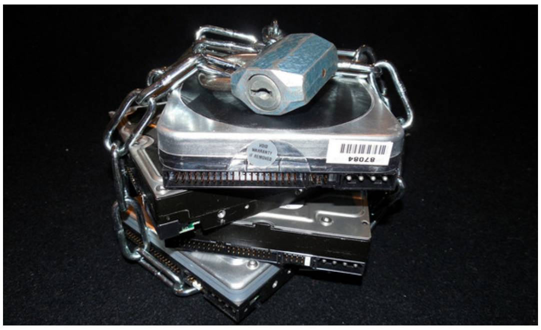
As per the Transposition Law, CERT-RO identifies operators of essential services with their registered office, subsidiary, branch, working unit or other forms of legal representation established on the territory of Romania. In this regard, an operator of essential service is a natural or legal person of public or private law who provides a service that fulfils the following cumulatively:

- the service is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems;
- an incident would have significant disruptive effects on the provision of that service.

The assessment of the degree of disruptive in the provision of the essential service is based on certain criteria (*without being cumulative*), criteria such as:

- the number of users relying on the service provided by the entity concerned;
- the dependency of other sectors of the above mentioned on the service provided by that entity;
- the impact that incidents could have, in terms of intensity and duration, on economic and societal activities or public safety;
- the market share of that entity;
- the geographic spread on the area that could be affected by an incident;
- the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

Digital service providers are those who typically provide a service at a charge, at a distance, by electronic means and at the request of the recipient of the service, a service that falls into one of the following categories: *(i)* online marketplace; *(ii)* online search engine; *(iii)* cloud computing service.



The key obligations in this field

In order to ensure network and information security, the key obligations of operators of essential services and digital service providers are:

- implementing adequate and proportionate technical and organisational measures to meet the minimum security requirements;
- implementing appropriate measures to prevent and minimise the impact of incidents affecting the security of networks and computer systems used to provide essential and digital services;
- prompt notification of CERT-RO as a national CSIRT of incidents that have a significant impact on the continuity of essential services or digital services provision;
- establishment of the permanent means of contact, designation of the network and information security officers responsible for monitoring the means of contact and communication to CERT-RO of the list, as well as any subsequent changes as soon as they have occurred;
- interconnecting with the CERT-RO alert and cooperation service, ensuring the permanent monitoring of alerts and requests received through this service or other means of contact and taking the appropriate response measures at the level of their networks and information systems.

Certified security auditors

Operators of essential services and digital services providers are also required to conduct a security audit of their networks and IT systems. The security audit has to be performed by computer security auditors who have valid certificates issued by CERT-RO to audit computer networks and systems that serve essential services or digital services.

According to the Transposition Law, several exclusions are provided, according to which the security audit cannot be carried out by:

- certified auditors who regularly provide IT security services or CSRIT services to an operator of essential services or digital service provider, or are their employees;
- the auditor who has concluded a service provision agreement for the network and the system under audit at the time of the audit or within a period of less than one year;
- the auditor who has performed 3 consecutive audits with the same operator of essential service or digital service provider.

Notification to CERT-RO

Both operators of essential service and digital service providers are required to immediately notify CERT-RO the incidents that have a significant impact on the continuity of essential services or the provision of digital services. They have to provide at least the following information:

- the identification of the infrastructure and the operator or supplier concerned;
- description of the incident;
- the period of the incident;
- the estimated impact of the incident;
- preliminary measures adopted;
- list of authorities of the state affected by the incident;
- the potential geographical extent of the incident;
- data on potential cross-border effects of the incident.

Penalties

As regards the sanctions for non-fulfilment of the obligations imposed by the Transposing Law, the fines that could be applied are between:

- RON 3,000 and RON 50,000, and in the case of a repeated violation, the limit of the fine is up to RON 100,000;
- 0.5% and 2% of the company's annual turnover for non-compliance with the Transposition Law, and in the case of a repeated violation, the fine limit is up to 5% of the turnover for companies with a turnover of over RON 2,000,000.

Cătălin Grigorescu, LL.M. Eur
Managing Partner
catalin.grigorescu@bpv-grigorescu.com

Roxana Mitroi
Associate
roxana.mitroi@bpv-grigorescu.com

bpv GRIGORESCU ȘTEFĂNICĂ
33 Dionisie Lupu Street
RO-020021 Bucharest
Phone: +40 21 264 16 50
Fax: +40 21 264 16 60
office@bpv-grigorescu.com
www.bpv-grigorescu.com

bpv LEGAL Alliance

bpv BRAUN PARTNERS
Europeum Business Center
Suché mýto 1 SK-811 03 Bratislava
Phone: +421 233 888 880
Fax: +421 257 200 170
Email: bratislava@bpv-bp.com
Web: ww.bpv-bp.com

bpv HÜGEL RECHTSANWÄLTE
Rond Point Schuman 9, Postbox 14,
B - 1040 Brussels
Phone: +32 2 286 81 10
Fax: +32 2 286 81 18
Email: brussels@bpv-huegel.com
Web: www.bpv-huegel.com

bpv JÁDI NÉMETH
Vörösmarty tér 4.
H-1051 Budapest
Phone: +36 1 429 4000
Fax: +36 1 429 4001
Email: budapest@bpv-jadi.com
Web: www.bpv-jadi.com

bpv BRAUN PARTNERS
Ovocný trh 8
CZ-110 00 Prague 1
Phone: +420 224 490 000
Fax: +420 224 490 033
Email: prague@bpv-bp.com
Web: www.bpv-bp.com

bpv HÜGEL RECHTSANWÄLTE
Donau-City-Str. 11, ARES-Tower
A 1220 Vienna
Phone: +43 1 260 50 0
Fax: +43 1 260 50 133
Email: vienna@bpv-huegel.com
Web: www.bpv-huegel.com