

Track Changes

Track Changes

December 2020

Romania: Minimum network and information systems security requirements to be complied with by the operators of essential services in the next 6 months

BACKGROUND

Operators of essential services in energy, transport, banking, financial market infrastructure, health services, drinking water supply and distribution and digital infrastructure sectors are bound to implement minimum network and information systems security requirements by 26 May 2021. The 6 month implementation period started on 26 November 2020, by the publication of Order no.1323/2020 for the approval of technical rules on minimum requirements to ensure the security of networks and information systems applicable to operators of essential services (hereinafter the "**technical norms on minimum security requirements**").

The technical norms on the minimum requirements have been adopted based on Law No. 362/2018 on ensuring a high common level of security of information networks and systems ("**Law no. 362/2018**"), which also represents the legal instrument which transposed Directive (EU) 2016/1148 ("**NIS Directive**") into the national legal system. The NIS Directive entered into force in 2016, being the first EU-wide legal act on cybersecurity, aiming to ensure a common high level of security of network and information systems across the EU, while setting out measures to improve cybersecurity and the functioning of the internal market.

The technical norms on minimum security requirements are applicable to operators of essential services and are intended to ensure a common level of security for networks and information systems. These technical rules have been developed by the Romanian NIS authority – The National Computer Security Incident Response Team ("**CERT-RO**"), established within the Ministry of Communications ("**MCSI**").

OPERATORS OF ESSENTIAL SERVICES AND THEIR OBLIGATION TO IMPLEMENT

The concept of "operators of essential services"

The operators of essential services ("**OSEs**") are private or public natural or legal persons who offer services:

- that are essential for the maintenance of critical societal and/or economic activities;
- the provision of which depends on network and information systems; and
- which can be severely disrupted in the event of incidents.

OSEs provide services in the energy, transport, banking, financial market infrastructure, health services, drinking water supply and distribution and digital infrastructure sectors. If any of the above-mentioned conditions is not fulfilled, then such operator is not an OSE, and no further action need be taken.

Obligations on the implementation of minimum security requirements

According to the Law no. 362/2018, in order to ensure a common level of security of networks and information systems, operators of essential services shall be required to comply with the technical rules drawn up by CERT-RO within 6 months from the date of entry into force of such technical rules (i.e. 26 May 2021), or from the registration date in the Registry for operators of essential services.

As per the technical rules on minimum requirements, OSEs set objectives, develop strategies, plans and schemes while implementing the minimum security measures. The OSEs shall identify the risks of non-implementation, shall plan the activities underlying the implementation and determine who is responsible for their implementation.

Once the minimum requirements have been implemented, the OSEs shall notify the National Authority for network and information systems security (ANSRSI).

MINIMUM TECHNICAL REQUIREMENTS WITHIN 4 SECURITY AREAS

There are 4 security areas which shall be used in setting minimum requirements for the security of networks and information systems. These security areas are also divided into categories of security activities. Each security activity has several security measures allocated to one or more minimum security requirements, which in turn contain control indicators.

Security areas established by the technical rules:

- **governance**, with the objective of definition and implementation of security policies at the organizational level; commitment of the organization's high-level management to the provision of information security management systems; risk management regarding identified threats, vulnerabilities and risks;
- **protection**, with the purpose of ensuring the security of networks and information systems, physical and personal security; managing and maintaining the resources of information networks and systems; controlling access to elements/components of information networks and systems;
- **cyber defense**, having the objective of ensuring the management of security incidents; detecting and dealing with security incidents affecting the security of networks and information systems;
- **resilience**, aiming to ensure management of the continuity of the essential services provided; management of crisis situations, in particular security incidents that have a major impact on essential services.

SANCTIONS

The failure to implement the minimum security requirements within the 6 months' time-period may trigger substantial fines to be applied by CERT-RO. In cases of companies with a turnover higher than 2 million RON, the fines amount to up to 2% of their annual turnover and up to 5% for repeated violations.

About WOLF THEISS

Wolf Theiss is one of the leading European law firms in Central, Eastern and South-Eastern Europe with a focus on international business law. With 340 lawyers in 13 countries, over 80% of the firm's work involves cross-border representation of international clients. Combining expertise in law and business, Wolf Theiss develops innovative solutions that integrate legal, financial and business know-how.

For more information about our services, please contact:



Anca Ioana Jurcovan
Partner
anca.jurcovan@wolftheiss.com
T: +40 21 3088 100



Maria Ionescu
Associate
maria.ionescu@wolftheiss.com
T: + 40 21 3088 100

This memorandum has been prepared solely for the purpose of general information and is not a substitute for legal advice.

Therefore, WOLF THEISS accepts no responsibility if – in reliance on the information contained in this memorandum – you act, or fail to act, in any particular way.

If you would like to know more about the topics covered in this memorandum or our services in general, please get in touch with your usual WOLF THEISS contact or with:

Wolf Theiss
Schubertring 6
AT – 1010 Vienna

www.wolftheiss.com