MPR PARTNERS
MARAVELA, POPESCU & ROMAN

WE TRANSLATE LEGAL
TO BUSINESS

EMERGENCY LEGAL KIT FOR BUSINESS SERIES

Year 6, Issue 22, July 2019

Romanian legislation on network and information systems security: a work in progress

1. Introduction

The European Union's concern with safeguarding data is not limited to the protection of personal data by means of legislation such as the GDPR. Network and information systems infrastructure security is equally important.

The new regime for cybersecurity in the European Union was adopted in 2016 in the form of the NIS Directive, which should have been implemented by May 9, 2018. In Romania, transposition measures are still ongoing.

Although the main piece of legislation has been issued, secondary legislation is needed for actual implementation.

However, the importance the Romanian legislator gives cybersecurity cannot be understated. EU countries must apply effective, proportionate and dissuasive penalties to ensure that the terms of the new cyber-security regime are applied.

Romania has chosen to impose fines of up to 5% of the turnover for the previous year to providers of services deemed critical to society and the economy if they fail to comply with the legal cyber-security measures.

Such providers must take immediate actions to ensure prompt and proper compliance. Entities active in the sectors of energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure are directly concerned.

2. Overview

The Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "**NIS Directive**") has been implemented in Romania through Law no. 362/2018 for ensuring a high common level of security of networks and information systems ("**Law no. 362/2018**").

The NIS Directive aims at ensuring a harmonized legal framework for cybersecurity in the European Union. In a nutshell, the NIS Directive requires that Member States to be adequately prepared to respond to cyber-security incidents, imposing the creation of a Computer Security Incident Response Team (CSIRT) and of a competent national NIS authority. Member States also need to set up a CSIRT Network that provides rapid cooperation in the field of cybersecurity.

In Romania, the national NIS authority is CERT-RO, established within the Ministry of Communications and the Information Society ("**MCSI**").

The NIS Directive also identifies seven strategic sectors which are vital for the economy and which should be able to respond swiftly in case of cyber threats. Entities active in the sectors of energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure, and which are identified by the Member State as operators of essential services, are obliged to have in place adequate security measures and also to report serious incidents to the national authority.

Provisions of the NIS Directive are also applicable to key digital service providers (search engines, cloud computing services and online marketplaces).

Although the implementation term for the NIS Directive was May 9, 2018, Law no. 362/2018 was published in the Official Gazette on January 9, 2019. In order for the legislation to be actually enforced, however, the Romanian Government still needs to adopt secondary legislation regulating issues such as threshold values for determining the significant disruptive effect of incidents, specific sectoral criteria and threshold values for each sector and sub-sector of activity, technical norms for impact assessment of incidents, threshold values corresponding to cross-sectoral criteria.

Some of this secondary legislation is already being rolled out by the MCSI.

3. Publication of secondary legislation

On July 17, 2019, MCSI published Order no. 599/2019 approving the Methodological Norms on identification of operators of essential services and providers of digital services (the "**Methodological Norms**"). The following day, the MCSI published Order no. 601/2019 approving the Methodology for establishing the significant perturbing effect at the level of network and information systems of the operators of essential services (the „**Methodology**").

The Methodological Norms regulate how operators of essential services ("**OSEs**") and providers of digital services ("**FSD**s") are identified for the purpose of registration in registries specifically created for this purpose.

OSEs are private or public natural or legal persons who offer services:

(i) that are essential for the maintenance of critical societal and/or economic activities;

(ii) the provision of which depends on network and information systems; and

(iii) which can be severely disrupted in the event of incidents.

OSEs provide services in the sectors of energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution and digital infrastructure (i.e. IXPs, DNS service providers and TLD name registries).

FSDs are entities that provide digital services of online marketplaces, online search engines or cloud computing.

According to Law no. 362/2018, all OSEs need to be registered in the Registry for operators of essential services ("**ROSE**") and FSDs need to be registered in the Registry for providers of digital services.

In order to determine whether a service provider is an OSE or, respectively, an FSD, each entity acting in the relevant fields must carry out a self-evaluation: service providers in the sectors of energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution and digital infrastructure must assess whether they are OSEs, and service providers of online markets, online search engines or cloud computing must assess whether they are FSDs.

4. Registration of an OSE

In order for a service provider to be an OSE, three cumulative conditions must be met:

(i) the service it provides 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 that service.

If any of these conditions is not fulfilled, then the firm is not an OSE, and no further action must be taken.

4.1. Self-evaluation of the service provider

The registration process starts with a self-evaluation made by the service provider.

The self-evaluation process comprises three steps: assessing the importance of the provided service, identifying how the service is provided and evaluating the disruption effect on the service in case of an incident.

During the self-evaluation process, service providers may request specialist assistance from CERT-RO, the Romanian NIS authority.

4.1.1. Assessment of the importance of the provided service

The service provider will first check whether its service is included in the List of essential services.

The List of essential services should have already been drafted by the MCSI, but it has not yet been published.

If the service is included in the List of essential services, the self-evaluation process continues. If the service is not included in the list, the service provider will conduct an internal economic and societal analysis on the importance of the service. If the conclusion reached by the analysis is that the service is of critical importance, the service provider will continue the self-evaluation process, otherwise the process stops and the service provider is not an OSE.

4.1.2. Identifying how the service is provided

At this stage, the evaluation consists in determining whether the service is dependent of networks and information systems; in the affirmative, the self-evaluation process continues.

4.1.3. Evaluating the disruption effect on the service in case of an incident

This stage consists in the service provider making an assessment of the degree of disruption of the essential service when an incident occurs. The Methodology in the MCSI Order no. 601/2019 describes in detail how the third step must be implemented.

The process of evaluation consists of two phases:

(i) phase 1 – evaluating the degree of disruption in providing the service by taking into consideration the (non-cumulative) factors described below;

(ii) phase 2 – evaluating the disturbance degree according to sector-specific criteria and thresholds; this phase starts to the extent phase 1 was concluded with a negative or low impact result, or if the disturbance degree of the service was not identified.

Phase 1 – Evaluation of the disruption degree according to inter-sector criteria

In phase 1 of the evaluation, the service provider will analyse all the relevant inter-sector criteria established by the Methodology based on Law no. 362/2018, in the order of their appearance.

The service provider will determine specific threshold values ("**VI**") (which differ from service provider to service provider) and compare them to threshold values to be established by Government Decision ("**P**") (however, the Methodology already provides threshold values). The disruption degree ("**GP**") will depend on the relationship between VI and P.

As a general rule, if the specific threshold value identified by the service provider is lower than the threshold value established by Government Decision (VI < P), then the disruption degree is deemed low (GP = low). If both threshold values are equal (VI = P), the disruption degree is deemed medium (GP = medium), and if the specific threshold value identified by the service provider is higher than the threshold value established by Government Decision (VI > P), the disruption degree is deemed high (GP = high).

The comparison of VI and P is made by the service provider for each of the relevant inter-sector criteria, in order: if for the first factor GP = low (i.e. the disruption degree is low), then the self-evaluation continues with the next inter-sector criterion, and so on, until all six inter-sector criteria are analysed. If for all the criteria GP = low, then the service provider proceeds to phase 2 of the evaluation of the disruption effect.

To the extent GP = medium or GP = high (i.e. the disruption degree is medium or high), then the service provider is deemed to be an OSE. The self-evaluation process ends, and the service provider proceeds with the next step in registering as OSE.

The inter-sector criteria are the following.

i. The number of users relying on the service provided by the service provider

The service provider will calculate the number of beneficiaries and the number of contracts it had ongoing in the year previous to the evaluation.

If the number of beneficiaries is below 50,000 (i.e. if VI is a number below P, which is 50,000), the disruption degree is deemed low. If the number is equal to 50,000, it is deemed medium, and if it is above 50,000, the disruption degree is deemed high.

The P for the number of concluded contracts is 22,600.

ii. The dependency of other essential services sectors on the service provided by the service provider

For this step the service provider must identify the beneficiaries of its services that are also active in the sectors listed as essential in the Law no. 362/2019 (i.e. Energy, Transport, Banking, Financial market infrastructures, Health, Drinking water supply and distribution and Digital Infrastructure). If two or more sectors are affected, or if three or more of the affected entities are OSE, then the disruption degree is deemed medium or high.

iii. The impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety

For this step, the service provider will consult analytical and statistical data related to information technology. If the disruption lasts 1 hour or more, or if it has an intensity of 1 Gbps or more, then the disruption degree is deemed medium or high.

iv. The service provider's market share

To the extent the service provider's market share in the relevant sector(s) (i.e. according to the relevant NACE code) is equal to or above 5%, then the disruption degree is deemed medium or high. The market share shall be calculated based on financial data from the previous year.

v. The geographic spread with regard to the area that could be affected by an incident

The threshold values for this inter-sector criterion, P, is one affected county/district (for Bucharest), three affected administrative-territorial units (out of which at least one must be a city/town) or two affected countries. If the affected geographic regions are equal to or more than the threshold values, then the disruption degree is deemed medium or high.

vi. 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

To the extent there is more than one alternative means of providing the service, even in the event of cyber-attacks, then the disruption degree is deemed low.

Phase 2

In the phase 2 evaluation the service provider will compare specific threshold values for its sector of activity (VI) with the threshold values established by Government Decision (P). Order no. 601/2019 provides threshold values for each of the sectors deemed essential by the NIS Directive and Law no. 362/2018.

Similar to the reasoning in phase 1, if the service provider's specific threshold values are equal to or higher than the established threshold values (VI = P or VI > P), then the

disruption degree is medium (GP = medium) or high (GP = high), resulting in the service provider having to register as OSE.

4.2. Notification to CERT-RO

If the conclusion of the self-evaluation is that the service provider is an OSE, the service provider must notify CERT-RO for registration in ROSE.

The service provider will fill in a standard notification form which will be sent to CERT-RO. The notification will be accompanied by an audit report attesting to the fulfilment of minimum security measures (by 2021, the audit report will be replaced by an affidavit attesting to the implementation of minimum security measures).

After being notified, CERT-RO will proceed with evaluating the OSE. During the evaluation process, CERT-RO may request additional documentation, such as audit reports and supporting documents for (i) establishing the status of OSE, for (ii) establishing the necessary measures to be implemented by the service provider in order to be compliant with the Law no. 362/2018 and for (iii) establishing the interdependence and interconnection of the service provider. CERT-RO may also request a list of public authorities who are clients of the service provider.

If the evaluation procedure is successful, the OSE is registered in the ROSE. The data within ROSE may be modified and also deleted, when the conditions that made the registration possible no longer apply.

According to Law no. 362/2018, ROSE is a classified document. However, the documentation on which the registration in ROSE is made is not classified.

According to Law no. 362/2018, the OSEs have the obligation to notify CERT-RO within 30 days from the date the conditions for being an OSE are met. For the first two years after the law enters into force, registration in ROSE is made by submitting an affidavit, accompanied by a self-evaluation documentation regarding the fulfilment of minimum notification and security requirements.

Failure to notify CERT-RO may be deemed as an administrative offence which is sanctioned with a fine ranging from RON 3,000 (approximately EUR 635) to RON 50,000 (approximately EUR 10,500). If the service provider has a turnover of over RON 2,000,000 in the previous year, the fine will range between 0.5% and 2% of that turnover. For repeated offences, the fine may go up to 5% of the turnover.

5. Steps in the registration of an FSD

Similar to OSEs, registering as FSD requires a process of self-evaluation from the provider of digital services.

In the event the results of the self-evaluation are positive, the process continues with a submission of documents to CERT-RO, followed by an evaluation by CERT-RO.

5.1. Self-evaluation of the service provider

This self-evaluation process also has three stages:

(i) establishing the type of business – if the service provider is a small or medium-sized business (within the meaning of Law no. 346/2004 on stimulating the setting-up and development of small and medium enterprises), it is exempt from the obligation of notification as FSD;

(ii) identifying the rendered digital services – if the service provider's services are in the field of online markets, online search engines or cloud computing, then the legislation on network security is applicable;

(iii) establishing the category of the service – it must be accurately established whether the service is an online market, a search engine or cloud computing.

5.2. Notification to CERT-RO

After the self-evaluation, the service provider will designate persons responsible with network security within its organisation, who will also be the contact persons with CERT-RO. The list of designated persons and the standard form with the data of the service provider are communicated to CERT-RO.

5.3. Evaluation by CERT-RO

CERT-RO proceeds with evaluating the service provider. The authority may ask for additional documentation, such as (i) the analysis that concluded whether the service provider was FSD, (ii) the analysis of the interconnection with other operators and (iii) the list of public authorities who are clients of the service provider. Not providing this information and documentation may result in fines ranging from RON 3,000 (approximately EUR 635) to RON 50,000 (approximately EUR 10,500). If the service provider has a turnover of over RON 2,000,000 in the previous year, the fine will range between 0.5% and 2% of that turnover. For repeated offences, the fine may go up to 5% of the turnover.

At the end of the (successful) evaluation procedure, the FSD is registered in the Registry for evidence of FSDs. The data within the Registry may be modified and also deleted, when the conditions that made the registration possible no longer apply.

6. Conclusions and recommendations

The Romanian State seems to be making progress in ensuring that the network security legal framework is ready to be applied in practice.

However, currently there are still gaps in the legislation that need to be filled. By way of example, there is still no list of essential services which the Romanian Government should issue. Also, MCSI has not issued the technical norms that establish the impact of incidents. According to the CERT-RO website (https://cert.ro/pagini/nis-acte-subsecvente), the relevant Government Decisions are in various stages of approval.

Presently the timeframe for fulfilling the service provider's obligations of self-evaluation and submission of the affidavit is still unclear. However, taking account of the generally balanced approach of the authorities with respect to applying sanctions when there are legislative gaps, it is probable that no sanctions will be applied at least until all the secondary legislation is in place.

Nevertheless, given the magnitude of the applicable sanctions, service providers in the relevant sectors (i.e. service providers in the energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure, as well as providers of online search engines, cloud computing services and online marketplaces) should

(i) monitor the implementation of the secondary legislation;

(ii) undertake the relevant assessments, to the largest extent possible given the current status of the legislation; and

(iii) ask for guidance from the relevant authority where they find difficulties in the self-assessment process.

*****

Alina Popescu

Founding Partner

alina.popescu@mprpartners.com

Flavia Ștefura

Senior Associate

flavia.stefura@mprpartners.com