MPR PARTNERS
MARAVELA, POPESCU & ASOCIAȚII

LOADING NIS DIRECTIVE 2.0 FOR HIGHER CYBERSECURITY PROTECTION

1. Introduction

In the last years, cybersecurity has become one of the European Commission's critical priorities. Given that the landscape of threats has significantly expanded, it comes as no surprise that the Commission has proposed a revised version (the "**Proposal**") of the Directive concerning measures for a high common level of security of network and information systems across the Union[1] ("**NIS Directive**").

In one of our previous articles[2], we have touched upon the issue of the potential amendments to NIS Directive. The most important novelties are summarised below.

The Proposal has been published by the Commission on December 16, 2020 and has now reached the preparatory phase in the European Parliament. A final version might be adopted in the earlier months of 2021.

2. What are the changes?

We think that the aspects listed below are of the utmost importance.

2.1. Changes in scope: new entities and sectors covered by the Proposal

The NIS Directive contains distinct rules for operators of essential services ("**OESs")** and for digital services providers ("**DSPs**"). Although guidance on how to identify the entities that qualify as OESs has been published, the Member States took different approaches when identifying such entities. In practice, this has resulted in many inconsistencies within the process of designating entities as OESs under the NIS Directive.

[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] Available here: https://www.lexology.com/library/detail.aspx?g=8316ddf8-2fc5-4dfa-bebf-2a79fe024dae.

In this context, one of the aims of this Proposal is to address these inconsistencies, by, firstly, eliminating the distinction between the OESs and DSPs and secondly, providing for a classification based on the importance of the entities resulting in two categories of entities: the essential ones and the important ones[3].

It is also noteworthy that the Proposal introduces a clear size cap – meaning that all medium and large companies in selected sectors would be included in the revised scope of the directive. In order to ease the burden of small and micro companies, these are to be covered by the Proposal only under certain specific conditions.

Aside from the new distinction between essential and important entities, the Proposal introduces new sectors and new actors as essential/important entities that would fall within the revised scope of the NIS Directive, namely[4]:

(i) new sectors:

- public administration;
- wastewater and water management;
- space;
- food production, processing and distribution;
- manufacturing of certain critical products (such as pharmaceuticals, medical devices, chemicals, computer, electronic and optical devices);
- postal and courier services.

(ii) new actors in the existing sectors:

- providers of public electronic communications networks or services;
- content delivery network providers;
- data centre providers;
- trust service providers;
- providers of social networking platforms[5].

[3] See Annexes 1 and 2 to the Proposal.

[4] Idem note 3.

[5] In the current form, NIS Directive regulates the digital services providers, formed of providers of online marketplace, of online search engine and of cloud computing services. The Proposal plans to introduce the providers of social network platforms under the digital providers and to move the cloud computing service providers under the digital infrastructure.

Considering that, during the public consultation process, certain voices[6] requested for the telecom sector to be included in the scope of the NIS Directive, it should come as no surprise that the providers of public electronic communications networks or services are now included in the scope of the Proposals. This will entail the amendment of the European telecom framework, whereunder the electronic communication networks and services providers are already bound to ensure the security and integrity of their networks and services. In order to make things easier, the Proposal provides for the respective provisions of Articles 40 and 41 of Directive (EU) 2018/1972 establishing the European Electronic Communications Code to be deleted.

At the same time, the European Union Agency for Cybersecurity ("ENISA") will create and maintain a registry of those entities providing cross-border services, such as digital providers, domain name system ("DNS") service providers, top–level domain ("TLD") name registries, cloud computing service providers, data centre service providers and content delivery network. Since the named entities are deemed to be under the jurisdiction of the Member State where they have their main establishment within the European Union, the registry would be meant to ensure that such entities would not face a multitude of different legal requirements.

2.2. There is a need to manage risks to the security of network and information systems used in the provision of services

Under the Proposal, in case a company is deemed to be an important or essential entity, the same will need to implement at least the following key risk management measures in order to manage risks to the security of network and information systems used in the provision of its services:

- risk analysis and information system security policies;
- incident handling (prevention, detection, and response to incidents);
- business continuity and crisis management;
- supply chain security;
- security in network and information systems acquisition, development and maintenance;
- policies and procedures to assess the effectiveness of cybersecurity risk management measures;
- using cryptography and encryption.

[6] Including from the telecom sector.

This approach is expected to pave the way for an increased overall level of cyber resilience across the Member States and is aimed at ensuring that all entities covered by the Proposal are subject to the same regulatory regime, no matter under which jurisdiction they fall within the EU.

2.3. Supervision and enforcement

The Proposal aims to strengthen the role of the relevant national authorities. In that respect, a distinction is made between an ex-ante supervisory regime, applicable to essential entities, and an ex-post supervisory regime, applicable to important entities.

In the latter case, the relevant authorities would act only when provided with evidence or indication that an important entity does not meet the security and incident notification requirements.

The ex-ante supervisory regime of the essential entities would entail, amongst others:

- on-site and off-site inspections, including random checks;
- regular audits, as well as targeted security audits;
- requests to access data, documents or any information necessary for the performance of the supervisory tasks of the competent national authorities. Since this wording is rather broad, it remains to be seen whether it will be amended so as to put a limit to the powers of competent authorities to access data and request documents and information.

The ex-post supervisory regime of the important entities would entail, amongst others:

- on-site and off-site ex-post supervision;
- targeted security audits;
- the power to request any information necessary to assess ex-post the cybersecurity measures taken by the important entities.

In terms of sanctions, the relevant authorities could:

- issue warnings;
- issue binding instructions;
- in certain cases, impose administrative fines with a maximum of at least EUR 10 million or up to 2 percent of the total worldwide annual turnover, whichever is higher.

Cooperation and mutual assistance between national authorities would be required as necessary when entities provide services in more than one Member State or when an entity's main establishment or its representative is located in a certain Member State, but its network and information systems are located in one or more other Member States.

When the infringements of the cybersecurity risk management measures and reporting obligations would entail a personal data breach and the relevant data protection authorities would move to exercise their powers, the relevant authorities under the Proposal could not impose a fine for the same infringement.

3. Remaining steps

Although many stakeholders anticipated a NIS Regulation, the Commission decided, for the sake of flexibility granted to the Member States, to keep the Proposal as a directive.

As future steps, the Proposal will follow the ordinary legislative procedure and will be subject to the negotiations between the European Parliament and Council. After its adoption, Member States will have to transpose the Proposal into their national legislations.

*****

This article contains general information and should not be considered as legal advice.

Alina Popescu

Founding Partner

alina.popescu@mprpartners.com

Cristina Crețu

Senior Privacy & Technology Consultant

cristina.cretu@mprpartners.com

Laura Dinu

Associate

laura.dinu@mprpartners.com