MPR PARTNERS
MARAVELA, POPESCU & ASOCIAȚII

WE TRANSLATE LEGAL
TO BUSINESS

THE REVIEW OF THE NIS DIRECTIVE - WHAT TO EXPECT

1. Introduction

Though not more than two years have passed since the Directive on security of network and information systems[1] ("**NIS Directive**") had to be transposed by the Member States into their national legislation, the European Commission (the "**Commission**") has announced, early this year, its intention to review the NIS Directive. The initiative comes earlier than planned, due to the fact that there is a dire need to "*further strengthen overall cybersecurity in the Union*".

In order to prepare the review, the Commission already took several steps in this direction, namely:

(i) drafted and published a report that assessed the consistency of Member States' approaches in the identification of operators of essential services;

(ii) published a combined evaluation roadmap/inception impact assessment

(iii) organized a public consultation that was opened for 12 weeks in order to gather views on the implementation and the impact of the envisioned changes to the NIS Directive;

(iv) organized several workshops to discuss the impact of the envisioned changes.

Following the steps mentioned above, the Commission will adopt in the last quarter of 2020 the review of the NIS Directive.

2. Targeted changes

The consultation period offered the opportunity to more than one hundred stakeholders to provide feedback on the implementation and functioning of the NIS Directive. Based

[1] Directive (EU) 1164/2018 concerning measures for a high common level of security of network and information systems across the Union.

on the collected feedback, the Commission was able to identity several issues related to the implementation of the same and to pursue some potential changes, such as:

(i) transforming the NIS Directive into a regulation, due to fact that the wide margin of discretion granted to Member States in implementing the NIS Directive might undermine the level playing field for some operators and lead to further fragmentation of the single market. However, according to the public information on the review of the NIS Directive[2], the review will take the form of a Directive;

(ii) enlarging the scope of the NIS Directive, as several additional sectors and sub-sectors have been identified as essential by the Member States when implementing the same;

(iii) clarifying the definitions of both operators of essential services ("**OESs**") and digital services providers ("**DSPs**"), since this will provide for the correct identification of the same by the Member States;

(iv) placing on equal foot the OESs and DSPs[3];

(v) defining security objectives and planning for each sector with the involvement of the private sector, in order to bring under a common denominator the security requirements set by the Member States, that at this moment vary greatly from one Member State to another;

(vi) addressing the cost burden generated by the unequal regulation faced by operators that are present in several Member States.

3. New rules for the identification of the OESs

Based on the envisaged changes mentioned above, we consider that by far, the most important one entails the revision of the rules for the identification of the OESs. As outlined in the Report of the Commission on assessing the consistency of the approaches taken by Member States in the identification of OESs[4], the failure to consistently identify such operators providing services cross-border "*may result in an uneven level of cyber-resilience between different Member States, increasing the risk that a cross-border incident would damage critical infrastructures or cause the loss of the life of citizens*". The different approaches taken by the Member States in the identification of OESs made possible for the number of OESs in the energy sector to span *"from 0.3 operators to 29 operators per 1.000.000*

[2] Available here https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive.

[3] In the current form, both OESs and DSPs are subject to security requirements, but DSPs have a lighter regime. By placing OESs and DSPs on equal footing, the European legislator envisioned the situation when an OES rely in essential way from the service provider. In this context, when Cloud Services providers offer services to OES, they could comply with security requirements (risk assessment, security measures) and notification requirements equivalent to the ones of the OES.

[4] Available here https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546.

inhabitants". The same is the case in the banking sector where the number of OESs ranges *"from 0.07 operators to 51 operators per 1.000.000 inhabitants (not taking into account Member States that have not identified a single OES in that sector)"*.

4. Incident reporting mechanism

Another aspect that in practice generated divergent approaches between Member States is related to the incident reporting mechanism and to the types of incidents that require notification to the relevant supervisory authority. In this respect, it is in the interest of the OESs that are present in a number of Member States to have in place a uniform framework for incident reporting and proper clarification with respect to the types of incidents that require notification to the relevant supervisory authority. Thus, the burden of cost that the OESs is facing now to meet the regulatory requirements of each Member State will be properly addressed.

5. New sectors, new actors

With respect to the potential enlargement of the scope of the NIS Directive, one aspect worth mentioning is that in the public consultation some voices requested for the telecom sector to be included in the scope of the NIS Directive. However, choosing such option will entail not only a full overhaul of the NIS Directive, but also 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. Moreover, for regulatory stability sake, both the overhaul of the NIS Directive and the amendment of the telecom framework should be done in parallel. Otherwise there will be two coexisting legal frameworks regulating such obligations of the electronic communication providers. This would be burdensome as it may lead to increased compliance costs and potential conflicts between the two frameworks, as well as increased legal uncertainty due to the lack of consistency and coherence across the legislation.

At the same time, in the current form, NIS Directive does not address any aspects related to the equipment suppliers or other types of vendors, but only states that the general product liability regime is applicable in relation with the same. Nevertheless, in the public consultation process, some voices raised the possibility for the software and hardware manufacturers to be covered in the future NIS Directive as a new category of actors, subject to the same regulatory requirements. Although it can be agreed that the suppliers and vendors are considered to play an important role in enabling the OESs and the DSPs to secure their network and information systems, the obligations imposed through the NIS Directive should be incumbent solely on the latter.

Such option is preferable since imposing obligations both on the operators and the suppliers would not help ensure a more robust and resilient protection of network and information systems, but it would only diffuse the coercive effect of the provisions. Each

of the OESs, DSPs and the suppliers already comply with relevant obligations that help to ensure a secure and resilient digital system.

Enforcing another layer of obligations would not enhance the security of the digital value chain, but it would only place more burden on the relevant stakeholders, with additional costs that would only deter the current efforts to ensure a more robust and resilient networks and information systems.

At the same time, extending the stakeholders that fall under the scope of the NIS Directive would also place more burden on the competent authorities, which would need to have in place additional resources in order to be able to monitor and control the compliance with the rules not only by the OESs, DSPs, but also by the suppliers.

From this perspective, it would be more logical and constructive to keep the obligations related to the security of the systems and networks to the providers of such systems and networks and for the suppliers to continue to comply with the product related regulations in force.

6. Conclusions

It will be interesting to see which of the potential changes mentioned above will find a place in the new NIS Directive. Most probably we will have more clarity in the course of this month when a final study report will be published by the Commission pursuant to the workshops organised and the feedback collected from the stakeholders by the contractor of the study commissioned by the Directorate General or Communications Networks, Content and Technology[5].

It is envisioned that the revision of NIS Directive will create a greater level of cybersecurity preparedness at Member State level and a reduction of the costs at the level of companies and other organisations with the cybersecurity incidents.

However, it is important to see what policy options will be chosen by the European Commission for the purpose of reaching these objectives.

*****

[5] Details about the study and one of the workshops held available at: https://ec.europa.eu/newsroom/dae/item-detail.cfm?item_id=680095&newsletter_id=364&utm_source=dae_newsletter&utm_medium=email&utm_campaign=Cybersecurity&utm_content=Workshop%20Study%20to%20support%20the%20review%20of%20Directive%20on%20security%20of%20network%20a&utm_term=Cybersecurity&lang=en.

Cristina Crețu

Senior Privacy & Technology Consultant

cristina.cretu@mprpartners.com

Laura Dinu

Associate

laura.dinu@mprpartners.com