POSITION PAPER

Brussels, 11 June 2021

Position Paper on the European Commission's proposal for a Directive on measures for a high common level of cybersecurity across the European Union (NIS2)

Executive summary

To respond to the growing threats posed by digitalisation and the rise of cyberattacks, the European Commission has put forward a proposal replacing the current Network and Information Security (NIS) Directive. With this NIS2 proposal, the Commission aims to strengthen the security requirements in the EU by expanding the scope to include a wide range of medium and large-sized entities and sectors and their supply chains, streamlining reporting obligations, introducing more stringent supervisory measures and stricter enforcement requirements, and including harmonised sanctions across the EU.

Orgalim welcomes the Commission's proposal to address the increasing level of cyber threats. As the proposal is now covering a wider range of Europe's technology industries due to the enlargement of its scope, we believe that for it to be workable, meaningful and effective, a number of issues need to be addressed:

1. To adapt the scope of the proposal needs to:
   - Increase the size-cap from 50 to 250 employees, aligned with the EU's SME definition,
   - Introduce an extra criterion for "important" entities to target truly cyber-relevant entities,
   - Work on a clearer definition of "cloud computing service",
   - Ensure availability of support measures for the "important" entities, for building their cybersecurity capacities.

2. Differentiate the obligations for the "essential" and "important" entities:
   - Narrow down the scope of incidents that need to be reported to ensure workability,
   - Increase the notification time and time for reporting to make it more impactful,
   - Narrow down the enforcement measures to make them more proportionate.

3. Ensure that certification and conformity are future-proof and meaningful:
   - Certification should remain voluntary,
   - There should be separate horizontal legislation on cybersecurity for networkable products within the NLF, instead of addressing it in the NIS2.

4. Ensure proportionality of fines.

1. Introduction

Worldwide economies and societies rely more and more on billions of connected products, the digitalisation of processes and business models and the exchange of digitised data and information. Undoubtedly, in such a digital world cybersecurity is ever more relevant to assure all our digital and tangible assets. We believe that the proposed NIS2 Directive is a relevant and necessary building block of a more cybersecure Europe.

We explicitly welcome the two declared objectives of NIS2 to "increase the level of cyber resilience of a comprehensive set of businesses" and to "reduce inconsistencies in the resilience across the Internal Market". However, Orgalim notes that by introducing "important entities" the NIS2 Directive is extending its scope with respect to its predecessor (Directive (EU)1016/1148) which would also include thousands of small and medium-sized enterprises.

Europe's companies have already invested billions of euros in cybersecurity for their own protection as well as that of their customers. According to the Digital Economy and Society Index Report 2020 (DESI 2020 Cybersecurity), 93% of EU enterprises have adopted at least one ICT security measure. The adoption of ICT security measures is widespread among both large enterprises and SMEs: 99% of large enterprises and 92% of SMEs deploy some ICT security measures[1].

We believe it is the task of the NIS2 Directive to ensure existing measures can still be applied in a harmonised manner across all Member States. New measures need to remain proportionate and clear for organisations to implement, as well as actually contribute to an increased level of protection in practice.

2. The need to adapt the scope of the proposal

2.1. Increase the size-cap from 50 to 250 employees, aligned with the EU's SME definition

The proposal now includes in its scope all companies with a workforce of 50 employees or more. This places a considerable compliance burden on a large number of small and medium-sized companies. It is questionable whether new companies of 50 employees or more can comply with the NIS2 directive requirements without any additional support.

Looking at the NACE codes[2] shows that 19,531 companies larger than 49 employees would be added to the scope compared to the original NIS.[3]

For the sake of coherence and legal certainty, we recommend defining **the "size-cap" for "important" entities based on the usual EU SME definition of 250 employees or more.**

[1] Digital Economy and Society Index Report 2020 (DESI 2020 Cybersecurity), Integration of Digital Technology by Enterprises | Shaping Europe's digital future (europa.eu)

[2] Div. 26 to div. 30 of section c "manufacturing" of the NACE Rev. 2 classification

[3] Statistics | Eurostat (europa.eu), numbers are from 2017 or 2018.

This extension of the exemption rule would hardly decrease the targeted security level, as companies with a critical function can be included in the scope by the Member States through the criteria listed in Article 2 (2) of the NIS2 Directive, regardless of the number of employees.

In accordance with the above-mentioned, we would propose to change the scope and the wording in Article 2 (1) as follows:

"This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to important entities that qualify as micro, small ***and medium-sized*** *enterprises within the meaning of Commission Recommendation 2003/361/EC."*

2.2. Introduce an extra criterion for "important" entities to target cyber-relevant entities

In addition to the new size-cap, we would like to propose the introduction of the additional criterion for "important" entities to better define the scope of NIS2. The use of NACE codes in the NIS2 Directive is a very rough classification that does not reflect in a granular way the "importance" of entities in terms of cybersecurity risks. This makes the directive less targeted and inefficient to define in a detailed way which entities truly need to be within the scope because of cybersecurity risks.

In the new category of "important entities", we therefore recommend focusing on entities which are truly "crucial" or "relevant", clearly linking it to their actual impact on cybersecurity. Having clearer criteria regarding the impact would also be important to ensure harmonisation and similar implementation across the 27 Member States.

In accordance with the above-mentioned, we would propose to change the definition of "important entity" in Article 4 (26) as follows:

"'important entity" means any entity of a type referred to in Annex II and ***whose product, application or service might have an impact on the cybersecurity of an "essential" entity****."*

2.3. Work on a clearer definition of "cloud computing service"

The current definition of "cloud computing service" in Article 4 paragraph 1 (19) is too broad and imprecise. The current wording includes the providers of only distributed storage and computing capacities, but also software providers who offer storage space in a cloud in connection with their virtually usable software products. Almost every service uses hosting as a partial service connected to its products.

Due to further virtualisation of information technology, this very broad definition could therefore lead to a high number of such services being caught by this provision. We propose to make a **distinction between "digital service providers" on the one hand and users, such as "enterprises" or "operators of essential services", on the other hand, who in turn require "digital services" as a basis for providing their services.**

The same applies to the term "Providers of online marketplaces" in Annex II No. 6 which are identified in the proposal as "important entities". The problem regarding the classification is comparable: there is no explicit distinction between those providers whose service is primarily an online marketplace and providers who merely "offer" such a service as a secondary objective of their product.

In accordance with the above-mentioned, we propose the following:

Proposal for Article 4 (19): *'cloud computing service' means a digital service that in its core function enables on-demand administration and broad remote access to a scaleable and flexible pool of shareable and distributed*

computing resources. Excluded from this definition are services that only use the cloud computing services of a third party as a partial performance to be able to provide their own service with a different focus.

Proposal for Article 4 (17): *'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC. Excluded from this definition are services that only enable online contracting on a website as a minor service subordinated to the main service with a different focus.*

2.4. Ensure availability of support measures in place for "important" entities, for building their cybersecurity capacities

We believe that to effectively defend Member States, and eventually Europe, against cyber threats it will be very important to actively support the enterprises in building their cybersecurity capacities to ***prevent*** the incidents in the first place.

SMEs already have difficulties in finding cybersecurity experts on the labour market. The 2019 (ISC)² cybersecurity workforce study ((ISC)², 2019) asserted that there is a shortage of approximately 291,000 cybersecurity professionals in Europe – up from the previous estimate of 142,000 professionals that had been given in the 2018 report. This result is complemented by what participants in a Symantec CISO Forum said in February 2019 (Symantec, 2019), when they concluded that hiring cybersecurity personnel takes at least 6 months, with between 9 and 12 months not being unusual. On a similar note, another survey discovered that 33% of 1,125 chief information security officers in the United States and the EU have difficulty hiring new talent and 49% believe this might expose their organisations to greater risks[4].

To build up the necessary cyber resilience a two-way approach should be taken:

- Firstly, the CSIRTs should also have the obligation to **serve as a consultancy for companies seeking support**. This could be addressed by amending Article 10 with concrete support measures such as offering a specific helpdesk or a contact point for important entities or to explicitly spell out the obligation to offer consultancy free of charge to these entities.
- Secondly, the NIS2 Directive should oblige Member States **to introduce funding measures to promote improvement in cyber resilience, open not only to entities in Annex II, but also to smaller companies which are not (yet) within the scope of NIS2**. This could take the form of tax advantages for relevant investment into cybersecurity or direct financial participation in such investments, or support for organisational measures and consultancy related to the measures in Article 18 and Article 20 in addition to those offered by the CSIRTs.

Examples of helpful tools for SMEs could be templates for IRPs (cybersecurity incident response plans), organisation of table-top exercises (cybersecurity simulations), catalogues of best cybersecurity practices (ideally harmonised, available in official EU languages and accepted by all EU Member States), guides to implement security frameworks, and training material for employees.

[4] Cybersecurity skills development in the EU (2020): https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

3. Differentiate the obligations for the "essential" and "important" entities

In general, the obligations for essential and important entities are similar. The exceptions relate to the supervision and enforcement provisions which are ex-ante for essential entities and ex-post for important ones.

We believe that a differentiated approach should apply according to the type of entities and their exposure to risks when it comes to their related obligations. In the NIS Directive, this approach was applied and proved to be efficient, with risk-based and differing obligations between Operators of Essential Services and Digital Service Providers.
We believe that obligations for important entities should be more proportionate and differentiated in the current proposal, and we therefore recommend the following modifications:

In Article 18 on cybersecurity risk measures

- paragraph 2(d) on supply chain and thus paragraph 3 accordingly should not apply to "important" entities. While this may be appropriate for "essential" entities it would not be proportional for "important" entities, as they would already be covered by this obligation when part of the supply chain of "essential" entities. In addition, it is not clear for the company to understand where the risk management measures stop and on what kind of standards they should be based.

In Article 20 on reporting obligations

- The scope of incidents that needs to be notified for "important" entities needs to be narrowed, to ensure that only significant or major incidents will be reported. The reference to threats, so called "near-misses" in paragraph 2. should be not applicable to "important" entities to make it manageable for important entities to report only significant or major incidents.
- For "important" entities, the proposed 24 hours for an initial notification is too short and should be at least aligned with the 72 hours under the GDPR (paragraph 4.a.).
- For "important" entities, the final report after the submission of the intermediate report should be submitted not later than 90 days rather that the proposed 30 days, which is too short for many incidents.

In Article 30 on the supervision and enforcement for important entities:

- Provisions on supervisory measures, information that could be required and especially the enforcement powers of paragraph 4 may have a significant business impact and should not only be clarified and justified but must be exercised under the explicit provision of proportionality. Any supervisory powers and measures, such as onsite inspections, should especially avoid disruption to business operations which could be an effect of onsite inspections. Paragraph 4(c) (order to cease conduct) should also not lead to disruption of business operations.
- Some of the proposed measures for enforcement go too far (such as name and shame) while the possibility of administrative fines should be considered as sufficiently coercive to ensure compliance with the obligations of the Directive. We suggest deleting paragraph 4 g) and h)[5].

[5] (g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;

(h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;

4. Ensure that certification and conformity are future-proof and meaningful

4.1. Certification should remain voluntary

Certification plays a crucial role in increasing trust and security in essential products and services for the digital world. Currently, a number of different security certification schemes for ICT products exist and are still being developed in the EU. However, making certification mandatory for products, services, and processes, as stipulated in Article 21, is one of the central points of industries' concerns regarding the current draft of the proposal. Certification should be made mandatory only for certain types of entities.

In Article 21. Member States are allowed to impose essential and important entities to use only those types of certain products and services which were certified under a specific European cybersecurity certification scheme of the Cybersecurity Act (CSA). The intention seems to be to allow Member States to require certified products for particularly critical infrastructures, like 5G. This is understandable, but the wording goes too far because it allows a national authority to require certification not only for the context of the essential entities, but also for the important ones. This means that a Member State could, for example, demand that some manufacturers and their suppliers only use certified products and components for certain products pursuant to the CSA. This would create mandatory requirements that conflict with the voluntary nature of certification under the CSA. Moreover, there is no possibility for important entities to use products that are certified according to the requirements of the New Legislative framework (NLF).

4.2. A separate horizontal legislation on cybersecurity for networkable products within the NLF instead of addressing it in the NIS2

When it comes to product certification, and security overall, we call for a separate horizontal legislation on cybersecurity for networkable products within the NLF, instead of this being addressed in the NIS2. Orgalim is convinced that, specifically for ICT products, a coherent regulatory framework is of the utmost importance, especially in the context of the Single Market. Therefore, Orgalim proposes, complementary to the CSA, the introduction of a horizontal legislation on cybersecurity for networkable products within the New Legislative Framework (NLF).

While certification can play a pivotal role in ensuring compliance and trust, there are also important cost considerations that companies, especially SMEs, must consider before deciding whether to certify.

We would recommend the following modifications:

In Article 21 (1) we would propose to **remove** the words **"ICT products"** and **"The products"**. Article 21 should only apply to "essential entities".

5. Ensure proportionality of fines

Another key development in the proposal is the inclusion of potential administrative fines to essential and important entities of a maximum of at least €10 million or up to 2% of the total worldwide annual turnover (See Article 31(4)), reflective of the approach taken under the GDPR (See Art. 83(4) GDPR).

In the case of cybersecurity, the objective is not to protect a fundamental right, unlike in the GDPR for data protection, but to protect critical elements of our society and economy. Nor do the considerations regarding data protection law – that have led to fines being calculated on the basis of group sales – fit here.

It is therefore important to ensure that fines remain proportionate and to take into consideration the specifics of each individual case.

The maximum level of administrative fines should be no higher than €2 million without any reference to annual turnover. Such a level would strike a balance between the deterrent effect for companies violating the requirements stipulated in Articles 18 and 20, and the risk of being too excessive or non-proportional. This is particularly important since the incident itself is already in reality a punishment to the concerned company.

6. Conclusion

Orgalim understands that NIS2 is an attempt to catch up with the reality around us and to decrease the amount of cyber incidents in the EU. However, it is very important that we are on the right track and tackle not only the risks, but also reflect on the existing situation by defining the right scope,the existing level of skills and support for the SMEs and the necessary level of investments in cybersecurity. Orgalim is convinced that there is a need to produce not simply the rules, but rather the enabling environment for our industries to ensure the cybersecure future of the EU.

Orgalim aisbl
BluePoint Brussels
Boulevard A Reyers 80
B1030 | Brussels | Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438