EuroCommerce for retail & wholesale

Position Paper
June 2021

Revised Network and Information Security (NIS 2) Directive

Introduction

EuroCommerce welcomes the revision of the NIS 2.0 Directive and the efforts of the European Commission to increase cyber resilience. Due to the ongoing digitization of the economy and society and the subsequent rise of cyber security risks there is an urgent need to ensure that the digital infrastructure of all sectors of the economy are secure and resilient. However, we note that this should be done in a risk based and proportionate manner, that would provide legal certainty and avoid further regulatory fragmentation and overregulation. For that purpose, we take this opportunity to express our specific concerns on the proposal.

Key points

Scope	The extension of the scope should include companies of systemic relevance.
European Vulnerability Registry	The creation of a central publicly accessible registry is very risky and will have great appeal to cybercriminals.
Legislative duplication	The European Commission to ensure consistency between national requirements already in place and the cooperation between member states.
Risk management measures and reporting obligations	The burden of proof for the whole supply chain is not realistic and can be extremely burdensome and that reporting should be done on a confidential basis and to one specific competent authority.
Certification schemes	The cost of certification for both suppliers and the purchasing entity would be very high. It should also be possible to use internationally recognized certification schemes and alternative certification solutions.
Overlapping with. GDPR	The interaction of the Directive with GDPR rules needs further clarity to avoid confusion about different reporting obligations and timelines.
Sanctioning regime	A cooperative approach is more preferable than a sanctioning regime with more incentives for important and essential entities to train and build the necessary infrastructure rather than sanctions and fines.

Scope (Article 2 / Annex II)

The proposed revision of the NIS 2.0 Directive will broadly widen the scope to cover new categories of important entities (Annex II) active in a variety of sectors, among them food distribution. This will include all entities with >50 employees and >10 million euro annual turnover, whereas in the current NIS directive it was up to the member states to identify and appoint the operators of essential services. We observe that **these changes will bring many more companies under the scope of the Directive and would lead to high compliance costs**.

Although we support the inclusion of new sectors as we recognize the importance of the resilience of the entire supply chain, we strongly believe that new sectors should only be included if the risk for society so requires. In any case, **the obligations imposed should always be proportionate to the risk presented by each entity**. Any inclusion of additional services and providers should take place as a result of a thorough risk analysis that outlines the necessity of imposing these obligations. The inclusion of additional business sectors to the annexes of the Directive and applying all provisions to them would lead to measures disproportionate to the potential risk posed. In addition, it would lead to high compliance costs for businesses, also at a time where they are still struggling to overcome the COVID-19 crisis. According to the impact assessment, the Commission estimated that new businesses covered under NIS 2.0 would need to **increase their IT spending by 22%** with a 12% increase for businesses currently under its scope. From our practical perspective these estimates are clearly too low. The effort of complying with the measures could cost at least **100,000 € per company in the first two years**. Also, the scope of application would lead to thousands of new companies being affected. In the food sector alone, the number of affected businesses would increase a hundredfold.

Therefore, **we believe that the extension of the scope should in principle include only companies of systemic relevance**. The European Commission should follow clear and scientifically based definitions of what should be considered as critical infrastructure. Unfortunately, the public discourse is characterised by a different, sometimes misleading understanding of critical infrastructure. The term has been seen less in terms of what is *worth protecting* and more in terms of what needs to function and be maintained. Therefore, we recommend focusing on cyber threats in the framework of the NIS Directive and **not confusing the maintenance of local food supply with the criticality of IT of critical infrastructure sectors**.

This is also supported by the impact assessment where we observe that while in most sectors respondents tended to welcome the extension of the scope of the NIS Directive, results in the area of food distribution vary, with only half of the respondents supporting the idea of being included in the scope.[1] Thus, it is important to find a way to assess the criticality of the supply of each entity. Our recommendation is the following:

The NIS 2 Directive should follow, as the 2016 NIS Directive, a risk-based approach and the size of each entity should not be the only factor to determine whether an entity should or should not be in scope. Nevertheless, we should make sure that the Directive is not exposing small and medium-sized enterprises to high compliance costs and extensive administrative burden if it has not been proven that these entities pose a critical threat to the well-functioning of the society or the security of the population. In this context, we would support to remove SMEs from the scope in at least the food distribution sector (a sector where we are able to assess the consequences) which are not critical in securing food supply to the population of a member state. In particular, we recommend that when the supply of more than 0.5% of the population of the respective member state is provided by an establishment, this establishment should be deemed important in the sense of this directive. This would also adequately take into account the different economic conditions (e.g. price level) within the member states.

[1] https://data.consilium.europa.eu/doc/document/ST-14150-2020-ADD-4/en/pdf (page 41)

Lastly, **a differentiation between essential and important entities as well as ex-ante and ex-post measures could also lead to greater legal certainty as now the same obligations apply to all categories**. In this context, important entities could report incidents only on a voluntary basis.

Last but not least, we stress that there is a need to offer assistance to SMEs for compliacne with the rules aimed at strengthening cyber resilience. member states should provide such assistance via governmental policies and agencies, addressing the specific needs of SMEs, in relation to guidance and support in improving their resilience to cybersecurity threats. Thus we believe that **the scope of article 5, par. 2 (h) should be extended to SMEs** in scope of this directive.

Legislative duplication (Article 7/8/18)

Existing national legislation should be taken into account while revising the NIS 2 Directive. To ensure legal certainty and avoid fragmentation of the Single Market, especially for companies that operate across different EU member states there is a need for maximum harmonization. However, the question arises whether minimum harmonization (Art. 3) would not lead to fragmentation, and companies operating across borders would have to comply with different national requirements across the EU. National fragmentation will lead to a significant increase of compliance costs. **The European Commission must ensure consistency between national requirements already in place and new requirements proposed in the NIS 2.0 and offer clear guidelines for the transposition of the directive, in the member states.**

European Vulnerability Registry (Article 6)

The Directive provides for the development of a European Vulnerability Register by ENISA. Paragraph 2 states: "*The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated*." **We believe that a public central database will have great appeal to cybercriminals and consider it therefore very risky**. This is especially true if mitigation for the vulnerability is lacking. We note that vulnerabilities should only be made public if mitigation is available and deployed. In addition, a clear deadline should be included in this article regarding publication, so that entities have sufficient time to fix the vulnerability.

Risk management measures and reporting obligations (Article 18/20)

We welcome the **risk-based approach** followed in the context of the risk management obligations placed on businesses under Article 18, however, we note that 18(3) is far too detailed and could lead to disproportionate burdens for many businesses. According to this provision businesses will also be responsible for others in their supply chains, obliging them to take account of specific vulnerabilities of each supplier and services provider in their supply chain. This is not realistic and can be extremely burdensome. Companies often face large, global suppliers in the supply chain against whom they have little or no leverage so it is unclear how they will manage to ensure that every supplier or service provider will comply with the requirements. An essential or important **entity should not be liable if a supplier is non-compliant**, at least when they did everything they could to ensure that the supplier maintains a risk-adequate level of cybersecurity. **The responsibility for supply chain security lies with the manufacturers or suppliers of the respective solutions** as only they have the full knowledge of data storage, data processing services they use, and the security services and processes they manage. Therefore, **the responsibility for security in the supply chain should not be shifted to the operators due to their limited sphere of knowledge and influence. Instead, it should be addressed directly with the manufacturers and service providers at the multinational and regulatory level**.

Furthermore, with regards to Article 18(4), **the time taken to rectify should be in line with the risk**. Meaning the risk associated with the non-compliance should be assessed without undue delay, but the implementation time for corrective measures should and must depend on the risk associated with the non-compliance and the effort needed to implement the corrective measures.

Finally, NIS 2.0 Directive includes extensive and very detailed reporting obligations in terms of process under Article 20. While we overall recognize the importance of timely and adequate reporting of incidents to strengthen the resilience of the entire ecosystem, **we believe that the obligation to report potential incidents is not reasonable. This would lead to increased administrative burden while it is not always very clear whether a major threat could have resulted in a significant incident.** Moreover, the obligation to inform customers of potential issues could cause unnecessary distrust in services and may ultimately reduce confidence in digitalization. If there is a need to report at all, it should be possible to do so on a confidential basis and to one specific competent authority.

Certification schemes (Article 21)

This article allows member States to create an obligation for essential and important entities to certify certain ICT products, ICT services and ICT processes. This might seriously limit the number of options in the procurement process for entities and thus directly intervenes in businesses' operations. Another important point to consider is the cost-increasing effect of certification for both suppliers and the purchasing entity. Therefore, it must be made clear under which circumstances a member state can enforce certification. **As long as the number of certification schemes is very limited, member states should be cautious about imposing this requirement and should limit themselves to recommending the use of certification schemes**. Moreover, we believe entities should have the possibility to use alternative approaches to demonstrate compliance and internationally recognized certification schemes. **We believe that the present article should be deleted**.

Overlapping with GDPR (Article 6/20/32)

It is important to provide clarity about the interaction between the present directive and the GDPR rules. **Any confusion regarding reporting obligations and timelines should be avoided**. Lastly, Article 32(3) seems to undermine the one-stop-shop of GDPR.

Sanctioning regime (Article 31)

The Directive instructs member states to ensure that administrative fines imposed on essential and important entities are **effective, proportionate and dissuasive**. We believe that high fines on entities are not the most effective way to ensure compliance. **We support a more collaborative approach ensuring compliance that would create incentives for companies to train and build secure and resilient digital infrastructure**. It is not realistic to believe that a 100% security against cyberattacks is possible. In return, we need governments and companies' to work together to better oppose and take actions against cyber criminals, including an increase of highly skilled "nation-state attackers". Finally, we note that any imposed fines should be based on the tangible damage of a cyber incident and the type of incident each company could be reasonably held responsible for.

Contact:
Savvina Papadaki - +32 2 738 06 41 - papadaki@eurocommerce.eu
Transparency Register ID: 84973761187-60