CONFEDERATION OF INDUSTRY
OF THE CZECH REPUBLIC

PRAGUE, 26 FEBRUARY 2021

Comments on the draft NIS2 Directive

We support the modernization of the NIS Directive and its objectives. While we support the general aims of the Commission, we have some comments that should be addressed:

Overlaps with other proposals:

Policymakers should ensure seamless and clear application between horizontal legislative proposals v.s lex specialis. In order to support Member States in strengthening their respective capabilities and competences, and improve (cyber)security and resilience, NIS2 should ensure that there are no overlaps or double reporting required amongst all cyber related legislative proposals, while at the same time acknowledging the attributes of different sectors.

We see a potential risk in overlap between NIS2 and the proposal for Regulation on Digital Operational Resilience in Financial Sector (DORA). There is also another risk of overlap with the European Electronic Communication Code (EECC) in practice. While the EECC is *lex specialis* to NIS2 and NIS2 risk management and notification requirements will prevail, electronic communication providers that are subject to the EECC will have to design and invest in a notification process compliant with the EECC requirements and then redefine it again once NIS2 and transposition laws enter into effect. This will generate unnecessary duplication of compliance burdens and costs.

Risk Management approach:

NIS 2.0 introduces a far more comprehensive risk management approach that is generally welcomed. However, further clarifications are needed. From an industry perspective it is crucially important that reference is made when defining technical elements, formats and procedures to the underlying international standards, schemes and protocols in this area such as ISO 27000 series which underpin global cyber security risk management practices, as well as associated protocols and formats in common use for incident description.

Reporting obligations / timescales:

Art. 30 proposes 24 hours for an initial notification report with information to make the competent authorities aware of the incident. Despite the minimum amount of information required, this constitutes an extremely short timescale in view of the priority for businesses to rectify the problem and restore continuity of services should such have been disrupted. Exposing information about an incident before a patch is applied or operations restored, makes operators and their customers vulnerable to increased hacker attacks. Thus, we suggest adopting the language and timeframe similar to Art. 33 of GDPR, whereas a breach should be reported without undue delay, but no later than 72 hours. This would ensure harmonization between the Union's legislative instruments and clarity for service providers.

PHONE (+420) 225 279 111 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADDRESS FREYOVA 948/11, 190 00 PRAGUE 9, CZECH REPUBLIC
THE CONFEDERATION OF INDUSTRY OF THE CZECH REPUBLIC HAVE SIGNED UP TO THE EU TRANSPARENCY REGISTER AND THE ASSOCIATED CODE OF CONDUCT. REGISTER IDENTIFICATION NUMBER: 785320514128-81.

MEMBER OF BUSINESSEUROPE

Recital 55, and Art. 20 also propose to capture not only incidents but significant potential threats or so-called near misses in reporting obligations. Decreasing the threshold to near misses will likely result in an overflow of notifications and a decreased efficiency from regulators. It also raises questions about the provenance of such information, the reliability and related liability issues. Such information is better curated in threat information sharing fora such as ISACS – this is covered in the proposal by Information sharing (Art. 26)

Whereby, essential and important entities may exchange relevant information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. This exchange of information should take place within trusted communities and implemented through specific arrangements (entities must notify their participation in these agreements to the competent authorities). Entities outside the scope of NIS 2.0 may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses.

Incident notification to the regulator:

By expanding the scope and number of service providers classified as **essential entities**, the current proposal does not in the current language take into account common practices in the enterprise cloud environment whereby one essential service provider is the user or client of another essential service provider's services. The contractual obligations of service providers in these circumstances are not acknowledged, which could lead to legal ambiguity and / or overlap in reporting obligations, the cloud provider having to report an incident affecting its client to the regulator. Only the cloud user can assess the impact and gravity of an incident of another essential entity providing the digital services or infrastructure. Under the current proposal, a cloud provider or any other digital infrastructure provider deemed as essential, would have to report to the regulator without having the necessary information or overview of end users affected. We would thus recommend to include a clarification in NIS2 similar to the one in Art. 16(5) of the NIS Directive, "[w]here an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator." In addition, lliability exemptions or safe harbours for notifying incidents should be maintained in consistency with Articles 14(3) and 16(3) of the NIS Directive. Otherwise, if mandated, a reporting obligation that would go against confidentiality and contractual obligations in a typical cloud service agreement. Any deviation from this would amount to a breach of contract and the obvious risk of reputational loss for both the client and the digital service provider.

Certification:

We recognize the potential value and benefits of demonstrating compliance with NIS via a certification against a European cybersecurity scheme. However, to extend that compliance with such scheme could become mandatory in certain sectors, we recommend including more flexibility in the NIS2 to allow functionally equivalent international certifications, such as ISO 27001, to satisfy this requirement as well. Given the length of the EU scheme development and implementation cycle, there would not be enough EU schemes to cover the broad range of ICT products, processes and services covered by NIS2. Overall, forcing companies to comply with multiple overlapping control frameworks runs the risk of missing important details and weakening compliance with any single standard.

Oversight regime and penalties:

In line with a larger scope which classifies more service providers as essential operators, a **much more intrusive oversight regime** for operators of essential services is envisaged in Art.29.2. Moreover, Art 31.4

introduces on site audits and other measures with **potential severe penalties** (up to 2% of global turnover) for non-compliance. This is a significantly more intrusive regime than under the current Directive and other "lex-specialis" in other sectors, such as DORA for Financial Services.

We believe a proportionate sanction and oversight regime is appropriate, that would allow service providers to operate seamlessly across different sectors. Criminal sanctions and penalties as currently proposed are excessive and could lead to a market disincentive to use transformational technologies such as cloud computing, which has proved particularly important to allow organisations to operate in the COVID-19 environment.

Recital 70. Management body compliance: We welcome the idea of an enhanced focus on cyber training at all levels of management. However, personal accountability for non-compliance as foreseen under Art 16 would in this regard a step too far, if the goal is to ensure appropriate cybersecurity acumen.

Encryption:

We appreciate the benefit of encryption as a measure to manage the risks. Encryption is an effective mechanism to mitigate the risk of unauthorized access to data. Appropriate use of encryption should be consistent with industry practice and standards, such as FIPS 140-2 and FIPS 140-2 Level 3, as well as international and European certification schemes for information security (ISO 27001) and cloud security (ISO 27017, BSI C5, and the proposed ENISA EUCS).

Supply Chain assessment:

We support the focus on NIS2 on supply chain security. However, supply chain security is very complex as it requires the intervention of multiple stakeholders in a coordinated approach. It is unclear how the performance of coordinated sectoral risk assessments to be performed by the Cooperation Group would ensure a highest level of security across a particular supply chain. Such assessment should be consistent with risk management and notification requirements applicable under NIS2 to both important and essential entities and performed by those entities, with a risk-based approach, in accordance with supply chain security standards and practices recognized internationally.

We recommend that the Commission take into account industry led global initiatives in this area such as the Charter of Trust for Cybersecurity's recommendations for baseline security requirements in the digital supply chain. Such baseline requirements need to be supplemented by a security by design approach to products and services.

Registry:

The mere existence of a registry with information about all cyber establishments in the Union, can in itself represent a cybersecurity risk. If the registry is to be created, all information shared with ENISA need to be treated with the highest degree of confidentiality and encryption.

CVD:

We question whether the development of a central vulnerability registry is the right use of ENISA resources – such a list would need to be up to date and accurate to be useful. If this information is gathered from other sources its utility is questionable. There are also risks of inaccurate or inconsistent reporting.