18 MARCH 2021

DIGITALEUROPE position on the NIS2 Directive

Executive summary

The review of the Directive on Security of Network and Information Systems (NIS2)[1] is an essential step towards a more resilient Europe, ensuring state-of-the-art risk management of current and emerging cyber threats to vital sectors of the EU economy and society.

One of the goals of the 2016 NIS Directive was to harmonise Member States' cybersecurity protection initiatives and to boost the EU's overall level of cybersecurity.[2] Despite attempts to achieve this goal, there remain variances and fragmentation standing in the way of a single European approach. This is compounded by increased complexity in the interplay between the NIS and other EU laws. These are among the areas for improvement that should be addressed as primary objectives of the review.

The revised NIS should:

- **Provide greater clarity on the scope of the proposal**, particularly with respect to the definitions of certain categories of 'important entities,' as well as the territorial jurisdiction for enforcement.
- **Ensure Member State harmonisation and regulatory consistency**. There remains a pressing need to enhance consistency and reduce Member State fragmentation. The NIS2 should also take into consideration, and align with, other regimes and legislative developments at EU level.
- **Streamline the reporting requirements and maintain proportionate obligations for entities**, notably preserving the voluntary nature of certification obligations.

[1] COM(2020) 823 final.

[2] Directive (EU) 2016/1148.

- **Foster international alignment with standards and existing industry best practices** in the area of risk management, especially in relation to supply chain security assessments, information sharing and vulnerability disclosure.
- **Promote and ensure consistent, predictable enforcement** at Member State level, with proportionate punitive measures.

Table of contents

Scope

DIGITALEUROPE has been supportive of the division between operators of essential services (OESs) and digital service providers (DSPs) under the current NIS. However, it is apparent that demarcations between an OES and a DSP may require more clarity and that other entities could be considered as essential or important to Member States' economies and societies.

In adapting the NIS2 scope, therefore, any misalignment and fragmentation in Member States' identification of essential or important entities should be avoided. A clear and harmonised scope will ensure predictable and consistent enforcement of the framework.

Essential entities

One of the most significant evolutions in the NIS2 proposal is the introduction of essential entities (EEs), a definition which replaces and expands upon the entities previously defined as OES.

In doing so, the NIS2 should encompass a proper gradation of requirements based on actual risk, including the distinction between the business-to-business (B2B) and business-to-consumer (B2C) contexts. Absent this, the NIS2 would risk becoming a 'blanket legislation' covering most ICT services without any real distinctions.

The list of EEs has expanded to incorporate entities involved in healthcare, including the manufacturing of vaccines, R&D facilities, manufacturers of medical devices for health emergencies and space infrastructure.[3] The NIS2 proposal has also included 'digital infrastructure' as an EE, including cloud computing services, content delivery network providers, trust service providers and public electronic communications networks.[4]

All the entities and subsectors that would now fall in scope as EEs should have clear and concise definitions, ensuring that entities only receive one single designation. Referring to broad types of entities could generate unnecessary uncertainty and burdensome compliance efforts for entities potentially falling under several categories.

The definitions should also make it clear that where a company carries out operations in furtherance of providing its own services, such operations are outside the scope of the NIS2. Notably, operations should not fall within scope of the NIS2 as a 'data centre service,' 'cloud computing service' or 'content delivery

[3] See Annex I of the NIS2 proposal.

[4] See Section 8 of Annex I, ibid.

network' where they are not provided as services to external entities or third parties.

Cloud computing and data centre services

The current definition of 'cloud service provider' (CSP) is broad and extends to almost all 'as a service' (aaS) providers. However, it should be borne in mind that cloud services are not critical as such, but only where they enable EEs' critical functions.

The proposal does not take into account the different modes of CSP deployment. Notably, in contrast to public cloud services, a private cloud offers a dedicated infrastructure to enterprise users that is fundamentally different in terms of security controls. As such, private cloud services should be excluded from the proposal's scope.

With respect to 'data centre services,' it should be considered that the sale and actual provision of such services may not be carried out by the same entity. In such a reselling scenario, the NIS2 should only apply to the entity that directly provides the service to the customer and not to the reseller of the service.

Important entities

The NIS2 expands the list of entities that were previously classified as DSPs[5] under the new category of 'important entities'[6] (IEs) subject to *ex post* supervision.[7]

In addition to maintaining online marketplaces and search engines, which were included as DSPs in the 2016 Directive, IEs now include the likes of postal and courier services, waste management, food production, manufacturing and social networking services.

The inclusion of these sectors would benefit from a more in-depth assessment. For example, the rationale of including social networking services is unclear insofar as no systematic risk exists to Member States' economies or societies.

On a general level, while IEs are subject to *ex post* supervision as opposed to *ex ante* for EEs, in practice, if the approach is not lighter in terms of requirements, resource allocation will represent an issue for both IEs and supervisory authorities.

[5] See Annex III of Directive (EU) 2016/1148.

[6] See Annex II of the NIS2 proposal.

[7] See Art. 30(1), ibid.

In addition, it would be important to clarify that, for groups of undertakings operating in several Member States, only entities performing ‘important’ activities should fall in scope of the proposal.

Manufacturing

The manufacturing section would bring into scope almost every manufacturing company in Europe.

A more detailed analysis of what types of manufacturing entities should be considered important is necessary, as well as further clarification in relation to territoriality. It should be clarified that obligations should only apply to manufacturing processes in the EU.[8]

If the rationale of including such broad manufacturing categories is to ensure the continuous and secure supply of devices, components and services to EEs, this is already addressed under the supply chain security obligation.[9] Supply chain security concerns aside, it is not clear why manufacturers of all types of products should fall under extensive risk management and notification obligations.[10]

It should also be considered that cybersecurity requirements for products are also being contemplated in the context of a proposed delegated act under the Radio Equipment Directive[11] and a future horizontal instrument on the security of connected devices also announced by the Commission as part of the Cybersecurity Strategy for the Digital Decade.[12]

In light of the above, we urge that manufacturers of computer, electronic and optical products as well as electrical products should be removed from the list of IEs.[13]

Exclusion of micro and small entities

The NIS2 proposal provides that entities that are defined as micro or small shall remain out of scope.[14] This approach recognises that imposing complex compliance obligations on SMEs would stifle growth. This being said, the NIS2

[8] See *Territoriality* section at p. 7 below.

[9] See Art. 18(2)(d) of the NIS2 proposal.

[10] See Arts 18 and 20, ibid.

[11] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2018-Internet-connected-radio-equipment-and-wearable-radio-equipment.

[12] JOIN(2020) 18 final.

[13] See Annex II, Sections 5.B-C of the NIS2 proposal.

[14] See Art. 2(1), ibid.

should also not shy away from including incentives through funding or education for SMEs to uptake cybersecurity measures.

However, the proposal also provides Member States with the opportunity to define what SMEs would be critical or important to the respective Member State economy or society.[15] This dual approach will likely cause fragmentation and legal uncertainty for SMEs operating in multiple Member States, as they may be within scope in one Member State but not another.

Supply chain

Since the cyber resilience and improved security of networks is broad and encompasses many moving parts and entities, the NIS2 proposal introduces a number of requirements to conduct supply chain security assessments for particular products and services.[16]

It is crucial that these assessments be risk based and non-discriminatory to ensure a competitive and harmonised single market, with coordinated Member State approaches. Targeted entities and industries should be involved in such risk assessments, as their expertise is fundamental to a successful consideration of complex supply processes.

Finally, the responsibilities of different entities of the supply chain should be clarified. Entities should only be responsible for the obligations that are under their control. For example, manufacturers should not receive duplicative or conflicting obligations as a supplier and a manufacturer.

Territoriality

The NIS2 proposal should be clearer in relation to its territorial reach. It should apply to entities that operate in the EU as opposed to non-EU entities in the same group of companies.

In the particular case of manufacturers, irrespective of whether they are included only as EEs or also as IEs, the proposal should be clear that only entities which have manufacturing facilities within the EU fall under the NIS2.

[15] See ‘irrespective of their size’ in Art. 2(2), ibid.

[16] See Recitals 43, 46 and 47 and Arts 5(2)(a), 18(2)(d) and 19, ibid.

Harmonisation and consistency

The 2016 Directive allowed Member States to update the OES list to include entities that were deemed critical to their respective economies or societies.[17] This caused extensive fragmentation across Europe.

While the NIS2 proposal acknowledges this shortcoming,[18] it maintains the NIS as a Directive and not a Regulation, allowing for some leniency with transposition but with the key difference of removing the obligation for Member States to produce a national OES list.[19]

While this is a welcome step, harmonisation needs to be further enhanced in relation to competent authorities, which can still be 'one or more' in each Member State.[20]

Finally, more guarantees should be adopted pursuant to Art. 5 to ensure that national cybersecurity strategies are developed in a coordinated and coherent manner.

Regulatory consistency

Ensuring regulatory consistency should be a key objective of the NIS2, given the envisaged scope expansion and concurrent legislative proposals. Horizontal and sectoral legal instruments should be sufficiently aligned, and regulatory overlaps should be avoided.

Legislation such as the General Data Protection Regulation (GDPR),[21] the revised Payment Services Directive (PSD2),[22] the eIDAS Regulation,[23] the European Electronic Communications Code (EECC)[24] and the proposed Regulation on digital operational resilience for the financial sector (DORA)[25] all have related but yet widely varied entity reporting requirements.

[17] See Recital 19 and Art. 5 of Directive (EU) 2016/1148.

[18] See Recital 4 of the NIS2 proposal.

[19] See Recital 5, ibid.

[20] See Art. 8(1) ibid.

[21] Regulation (EU) 2016/679.

[22] Directive (EU) 2015/2366.

[23] Regulation (EU) No 910/2014.

[24] Directive (EU) 2018/1972.

[25] COM/2020/595 final.

The NIS2 also proposes that sector-specific legislation shall have precedence over the NIS framework.[26] While this provision aims to create legal certainty, it may not succeed in practice.

Such precedence is helpful when sector-specific legislation regulates the entirety of the security aspects of all services provided by certain entities, not when it affects only a part of them.[27] For cross-sector services, regulatory consistency can only be properly achieved if the basic level of requirements applies identically across all sectors where entities operate.

To this end, sufficient alignment between the relevant NIS2 provisions and sector-specific legislation should be promoted. Firstly, it should be ensured that the NIS2 is finalised before other sector-specific legislation can be put forward, as the NIS2 should provide the baseline for other legislation to build upon. In addition, an EU-level procedure could be introduced under the NIS2 to assess whether sector-specific legislation takes precedence.

EECC

The Commission's proposal correctly identifies that the reporting and material resilience obligations under the EECC should be repealed and replaced by those in the NIS2.[28] This will enhance consistency, avoid overlaps and thereby improve legal certainty.

However, it is equally important to promote coherence of enforcement by subjecting electronic communications services to the supervision of the competent authority of their main establishment.[29] This is particularly important given the expanded scope of interpersonal communications services under the EECC, many of which are inherently cloud-based and cross-border in nature.

Finally, further clarification should be provided that ENISA will continue to be tasked with ensuring greater harmonisation regarding the application of cybersecurity obligations by the relevant competent authorities.[30]

[26] See Art. 2(6) of the NIS2 proposal.

[27] DORA, where cloud computing or data centre activities are affected only when used in the financial sector, is a case in point.

[28] See Art. 40 of the NIS2 proposal.

[29] See *Jurisdiction* section at pp. 16-17 below.

[30] As currently provided by Art. 40 EECC.

DORA

Whilst the DORA proposal foresees a clear hierarchy between DORA and the NIS2 for financial entities, it does not do the same for critical ICT third-party service providers.[31] This creates redundancy between the two frameworks.

A structural, workable solution must be found in order to avoid that two sets of authorities conduct overlapping supervision over the same services, and to ensure consistent resilience and security requirements for digital services in the EU.

To this end, cooperation between the Lead Overseer under DORA and the NIS2 national competent authorities should be formalised, and the substantive scope of their respective powers explicitly articulated.[32]

RCE Directive

Overlaps between non-cyber and cyber requirements must be avoided. The proposed Directive on the resilience of critical entities (RCE Directive), which was launched in parallel with the NIS2 proposal, recognises that is it necessary to achieve a coherent approach between the two instruments.[33]

To this end, further clarification could be provided in the final RCE Directive that the definition of 'resilience' targets physical, or non-cyber, aspects in order to avoid overlaps with the NIS2.[34]

Entity obligations

Encryption

Recital 54 of the NIS2 proposal appears to oblige electronic communications providers to adopt end-to-end encryption to improve the cybersecurity resilience of electronic communications.

[31] See Art. 29(5) of the DORA proposal.

[32] For further background, see *DIGITALEUROPE's response to the Commission's public consultation on the Digital Operational Resilience of Financial Services (DORA) legislative proposal*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2021/02/DIGITALEUROPE%E2%80%99s-response-for-the-Commission%E2%80%99s-public-consultation-on-the-Digital-Operational-Resilience-of-Financial-Services-DORA-legislative-proposal.pdf.

[33] See Recital 8 and Art. 1(2), COM(2020) 829 final.

[34] For example, by clarifying that the definition of 'resilience' under RCE targets physical, or non-cyber, aspects.

While encryption provides strong and dynamic levels of security to electronic communications – and in many cases represents the best practice in securing data and service integrity – the NIS2 should not suggest any mandates for specific security practices or technology.

Entities should be allowed to adopt security safeguards and measures that they deem best suited for the security of their service and consumer needs, while ensuring security-by-design principles, and the continuous development and application of new cryptographic standards and techniques should be allowed.

In addition, and more broadly, entities should not be undermined in their ability to offer end-to-end encryption – any obligations to the contrary, such as lawful intercept, would inherently undermine security.

Risk management

Consistent with the 2016 Directive's goal of creating a culture of risk management, and as further emphasised in the Cybersecurity Act,[35] the NIS2 should underscore the EU's continued role to facilitate the establishment and uptake of European and international standards for risk management.

Compared to a focus on security controls, a focus on risk and security outcomes tends to be more easily translatable across an organisation, including IT practitioners implementing security for different products and services, incident responders, managers of IT or business functions and executives.

In the absence of full harmonisation, the NIS2 should specify that, when laying down specific risk management measures, Member States should follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.[36] Such existing international standards should form the basis of the Commission's implementing acts to lay down technical and methodological specifications for the risk management measures that entities must undertake.[37] In this context, the NIS2 could also formally task ENISA with developing technical guidelines on security measures, mapped against relevant standards and certifications, as a means to demonstrate compliance for both EEs and IEs.[38]

[35] See Recital 49, Regulation (EU) 2019/881.

[36] For example, ISO/IEC 27001.

[37] See Art. 18(5) of the NIS2 proposal.

[38] See ENISA's current *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers*, available at https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers.

Certification

The NIS2 proposes that Member States may oblige EEs and IEs to certify certain products, processes and services pursuant to the Cybersecurity Act, and empowers the Commission to adopt delegated acts specifying which categories of EEs are required to obtain a certificate and under which scheme.[39] In addition, the NIS2 proposal is unclear as to whether the supply chain of identified EEs must also adhere to mandatory certification.

This would create *de facto* mandatory requirements that conflict with the voluntary nature of certification under the Cybersecurity Act, which sets out strict conditions for the Commission in assessing whether adopted European cybersecurity certification schemes can be mandated.[40]

Such recourse to mandatory certification is problematic, as certification schemes can incorporate strict measures that, if made compulsory, would ultimately stifle growth and innovation, with a significant impact in particular for SMEs, without proportional benefits for security.

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

Reporting requirements

The 2016 Directive ensured baseline reporting requirements and resilience amongst OESs and DSPs, and therefore had a very positive impact on the EU's cyber resilience as a whole.

We welcome efforts from the Cooperation Group and ENISA to develop standardised formats and common notification templates for incident reporting, which would streamline and simplify the overall reporting process for companies. ENISA should be empowered to adopt entity-specific definitions as guidance for Member States and affected entities. Where the Commission further specifies these cases and other aspects of the reporting procedure,[41] it should be clarified that such implementing acts will replace any existing national specifications in order to avoid a duplication of requirements.

The request for reporting potential threats and near misses could lead to unmanageable amounts of data without clear context or analysis – in most cases, too much for Computer Security Incident Response Teams (CSIRTs) to

[39] See Art. 21, ibid.

[40] See Art. 56(3) of the Cybersecurity Act.

[41] See Art. 20(11) of the NIS2 proposal.

even analyse. In addition, the concept of ‘near miss’ is not well defined and potentially misleading.[42] Sharing general cyber threats or near misses is not useful and would create unnecessary burden for organisations that would need to process and try to operationalise the information shared.

By contrast, periodic updates or threat analysis reports from relevant entities, complemented by dialogue to provide context, are more relevant and useful.

The NIS2 proposal also changes the timeframe for reporting incidents, obliging entities to report within 24 hours to their competent authorities or CSIRT, followed by a detailed final report within one month of the initial alert.[43]

It is important to understand that entities may not have enough information within this timeframe, which will likely lead to inaccurate reporting. The 24-hour timeframe will also require EEs and IEs to temporarily shift away their duties from solving and mitigating the incident – which should be the main priority within the first 24-72 hours – towards reporting to the CSIRTs.

An obligation to report within 72 hours would be more reasonable and would also be more closely aligned with the personal data breach notification regime in the GDPR.[44]

The NIS2 proposal acknowledges that double notification regimes could be burdensome and cause uncertainties regarding the format and procedures of notifications. It further states that Member States should establish a single-entry point for all notifications required under the NIS2, the GDPR and the ePrivacy Directive.[45] The content of this recital should be included in the main body of the Directive.

In addition, incidents can be extremely complex and involve multiple actors. For this reason, investigations are often not completed within 30 days. We therefore recommend that the period for the final report should be extended to at least 60-90 days.

Similarly, there should be greater clarity and a higher threshold for the notification of threats. EEs and IEs are required not only to report ‘significant incidents’ but also any incidents having the ‘potential’[46] to cause operational disruption or

[42] See Recital 39, ibid.

[43] See Arts 20(4)(a) and (c), ibid.

[44] See Art. 33 GDPR.

[45] See Recital 56 of the NIS2 proposal.

[46] See Art. 20(2), ibid.

financial losses to the entity, or material or non-material losses to natural or legal persons.

The definition of ‘significant incident’ could be clarified considering entity type and risk, including additional parameters such as the number of users affected, duration and geographical spread, consistent with the current Directive.[47] Such definitions should be harmonised as much as possible at EU level.

In addition, any requirements to notify incidents that have not yet happened, for example any threats, near misses or those with ‘potential’ effect, would translate into unnecessary burden for both entities and supervisory authorities. There is also a clear risk that these vague terms could be interpreted and applied inconsistently across Member States.

Finally, disclosure of a threat or incident to the public should be the responsibility of the affected entities themselves, not the competent authorities or CSIRTs. The proposal should provide some additional guidance as to when public disclosure should be considered in the public interest.

Databases of domain names and registration data

DIGITALEUROPE supports the inclusion of databases of domain names and registration data, which aims to restore access to domain name registration information (‘WHOIS’ data) to enable cybersecurity efforts.

However, the reference to top-level domain (TLD) registries is too narrow. There are many other types of organisations that provide domain name registration services such as proxy service providers, domain name resellers and brokers, and those providing ‘second-level’ domain information.[48]

It is also important to be able to identify the ‘ultimate beneficial owner,’ as this is the person who actually owns the domain even if the domain is registered under another name. While domains are sometimes registered by person A on person B’s behalf (‘pass-through’), the pass-through should be required to report the actual domain owner. Person B (the actual domain owner) should not be able to obscure their ownership of the domain. Any kind of anonymity of the domain owner effectively undermines the security value of this data.

Finally, historical data and a permanent record of historical changes to the data are essential for cybersecurity purposes. For example, domain names may

[47] See Art. 6 of Directive (EU) 2016/1148.

[48] In the domain name system (DNS) hierarchy, a second-level domain (SLD or 2LD) is a domain that is directly below a TLD. The SLD is generally the portion of the URL that identifies the website’s domain name.

change ownership over a period of time, and once sold to another user can be repurposed for malicious purposes.

Vulnerability disclosure

DIGITALEUROPE is encouraged by the reference to well-established and broadly adopted best practices and industry standards in the field of coordinated vulnerability disclosure and vulnerability handling.[49]

Vulnerability sharing works best when both sides stand to gain from the interaction and a trusted relationship can be fostered. As it currently stands, private companies often do not always stand to gain new insights from engaging with cyber authorities. The presumption of immediate disclosure is not always helpful in minimising risk and impact of incidents and, in some cases, exploited vulnerabilities.

We support ENISA's more central role in global coordinated vulnerability disclosure and management. However, it must be considered that the global cybersecurity community has been leveraging the CVE Program for decades.[50] DIGITALEUROPE therefore recommends that ENISA refrain from starting a new vulnerability registry and instead establish a European database that leverages the global CVE registry, providing details on risks, impacts and fixes for ICT products developed or used in the EU.

In addition, ENISA could play a stronger and more central role in the CVE registry by becoming a Root CVE Numbering Authority (CAN) and joining the CVE Program's Board.

With regard to CSIRTs, we recommend that they should not play the role of coordinator in multiparty coordinated disclosure processes. The owner of the technology is normally best positioned to lead the coordination effort, while in other cases CSIRTs may serve an optional coordination role.[51] While CSIRTs can play an important role, it should be at the discretion of the vulnerability reporter to decide whether to use a CSIRT to aid in the facilitation of the disclosure, according to existing standards and best practices.

[49] See Recital 29 of the NIS2 proposal. Relevant standards include ISO/IEC 29147 and 30111.

[50] https://cve.mitre.org/. The existing CVE registry, while hosted by MITRE and funded by the US Department of Homeland Security/Critical Infrastructure Security Agency (DHS/CISA), has an international Board and is maintained by about 150 organisations from across the world. Its CVE Numbering Authorities (CNAs) include organisations from Germany, the Netherlands, Romania, Spain and other EU countries.

[51] For example, in open-source protocol vulnerability situations.

Information sharing

Relevant stakeholders aside from NIS2-covered entities should be encouraged to participate in voluntary cyber threat information sharing.

The list of recommended information to be shared should be expanded and clarified to encompass data of most use to cybersecurity practitioners. Similarly, threat sharing should prioritise actionable, context-rich information beyond compromise indicators.

We believe that directing Member States to set rules on procedures and operational elements of threat-sharing arrangements is counterproductive and will discourage voluntary sharing.

Similarly, mandated notification to competent authorities when organisations join or leave information-sharing arrangements will undermine the value of, and the trust entities will have in, information-sharing mechanisms.

It is critical that entities not be obliged to share information until after the exposed threat has been patched. Sharing threats before a patch may lead to further exposure and ultimately make it more difficult to patch.

In addition, information sharing could be done on an anonymised basis or through networking opportunities that collate information and share as a group. This could result in immunity from prosecution or reduced sanctions for breaches.

Finally, DIGITALEUROPE recommends that a closer networking of NIS2-covered entities be facilitated by competent authorities to increase information sharing and learning from best practice. Such information sharing could be extended cross-border and facilitated by multiple competent authorities in more Member States. As well as leveraging competent authorities to facilitate information sharing, direct engagement between covered entities should also be supported and guidance provided on how to navigate the legal frameworks within which this could be facilitated.

Enforcement

Although it is imperative that the NIS2 be updated to take into consideration the realities of modern-day cybersecurity resilience and threats, it is equally important that NIS2 enforcement be harmonised and consistent across Member States.

Jurisdiction

The NIS2 should include clear jurisdiction rules for all entities that fall under its scope. This is essential to avoid ambiguity as to which Member State is allowed to enforce the obligations. To improve clarity and predictability, the criterion of main establishment should be used whenever possible.

The proposal currently subjects certain ‘digital infrastructure providers’ to the jurisdiction of their main establishment.[52] This approach is instrumental in streamlining the notification regime for digital companies, most of which operate across multiple Member States, and should hence be extended to all ‘digital infrastructure’ covered under point 8 of Annex I.

Supervision

Onsite inspections or audits should not be at random but set on a periodic basis and limited in frequency, ideally no more than annually.[53] Additionally, compulsory security scans can be overly burdensome and may subject entities to greater security vulnerabilities if the information is not appropriately protected.[54] They should hence be removed.

In addition, potentially banning entities from doing business if they are found non-compliant appears overly punitive.[55] There are numerous factors that may result in non-compliance. Similarly, personal criminal and civil liability against entity representatives for non-compliance is troublesome and overreaching.[56] Penalties, if any, should be at the entity level and not directed to a natural person, and should not be criminal in nature.

Penalties

Another key development in the NIS2 is the inclusion of potential administrative fines to EEs and IEs in the order of at least €10 million or up to 2% of total worldwide turnover,[57] reflective of the approach taken under the GDPR.[58]

[52] See Art. 24(1) of the NIS 2 proposal.

[53] See Art. 30(2)(a) of the NIS2 proposal.

[54] See Art. 30(2)(c), ibid.

[55] See Art. 29(5)(a), ibid.

[56] See Recitals 74-75, ibid.

[57] See Art. 31(4), ibid.

[58] See Art. 83(4) GDPR.

It is important to ensure that fines remain proportionate and take into consideration the specificities of each individual case. It is equally important to ensure that entities' good faith be taken into consideration, for example in situations where they may miss reporting deadlines due to unforeseen circumstances.

Moreover, further clarity is sought as to overlapping penalties envisaged in *lex specialis* such as DORA. Excessive penalties and legal uncertainty run the risk of being a market disincentive to the uptake of digital technologies.

Cooperation

We encourage the Cooperation Group to actively engage and cooperate with EEs and IEs, improving and streamlining collaboration amongst various groups and authorities that was not fully realised under the 2016 Directive. In addition, the Cooperation Group should ensure greater harmonisation of standards and consistency in approach across the EU.

Finally, although we agree that improvements must be made in relation to coordinated management of large-scale incidents that impact more than one Member State, the creation of a new network appears unnecessary. The NIS2 proposal adds the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) to the Cooperation Group and the CSIRTs Network.[59] We recommend that further clarity be introduced in the final text as to the cooperation relationship between these groups.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell

Privacy and Security Policy Officer

martin.bell@digitaleurope.org / +32 492 58 12 80

[59] See Art. 14 of the NIS2 proposal.

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world’s largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world’s best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK