bitkom

At a glance

NIS Directive 2.0

Overall assessment: Bitkom sees the imperative need for a more harmonised and future-proofed cybersecurity framework and therefore welcomes the Commission's initiative. The proposal for a renewed NIS-Directive strikes a reasonable balance between targeted regulatory interventions and strengthening the EU's cyber-resilience holistically. However, several crucial points require further consideration and respective amendments:

- **The need to ensure consistency and alignment with other regimes and legislative developments,** in order to truly harmonise the European and national level in the field of cybersecurity and critical infrastructure protection. Since the new proposal remains a Directive, Bitkom calls upon the Commission to pay close attention to Member States transposition of the Directive. Maintaining or even introducing new cross-country fragmentation must be avoided at any cost. At European level, the EECC, the new CER Directive, the proposed DORA regulation as well as the Cybersecurity Act must go hand in hand with the renewed NIS Directive. This requires consistent and clear definitions, coherent across the entire regulatory landscape.

- **The risk of double regulation structures and an uneconomic bureaucratic burden.** This holds particularly true for electronic communications providers and data center operators. Reporting requirements must follow the 'one-stop-shop-principle'. To set up an efficient reporting channel it is crucial to specify proportionate reporting obligations and grant entities at least 72 hours for reporting an incident. A final report should not be demanded before the finalization of the forensic analysis and the introduction of measures required for ensuring business continuity.

- **The too extensive scope expansion with respect to important entities.** Although Bitkom supports an enlarged scope of the NIS2-Directive, the extension must follow risk- and criteria-based guidance. A 'network and information systems' Directive should not confound the maintenance of supply chains per se with the criticality of the IT to ensure the supply of a good or a service. The renewed NIS Directive should be viewed and thought through from the latter point of departure. It is the functional risk relevance that must be decisive in determining the scope. This also implies that all actors of the digital value chain assume their responsibilities. Only a fair burden sharing will ultimately lead to a secure Digital Economy.

- **The foreseen mandatory certification based on EU CSA schemes.** Despite the benefits of CSA Schemes, the European Commission would be better advised to publish horizontal cybersecurity requirements based on the principles of the NLF, which are then specified by European harmonised standards. In any case, there should be no diverging certification requirements between the national and the European level.

- **The unused potential of providing real-time information about the threat-landscape.** Instead of mere biennial PDF policy reports, Bitkom calls for machine-readable datasets and corresponding interfaces (APIs) that allow for automated evaluation in real time. An easily-understandable dashboard with well-defined indicators of the threat-landscape would be of great value.

Bitkom position on the proposal for a renewed Directive on security of network and information systems

March 2021

Preliminary Remarks

The Directive (EU) 2016/1148 concerning measures for implementing an equivalent and commonly high level of security in network and information systems across the Union (hereafter referred to as the NIS Directive) has been reviewed and updated by the European Commission. With its proposal for a revised NIS Directive the Commission seeks to improve the resilience and incident response capacities of public and private entities, competent authorities and the Union as a whole in the field of cybersecurity and the protection of critical infrastructure. Bitkom closely monitored and participated in the process of the revised legislative proposal, published on 16 of December 2020. We shared our position with the Commission about the combined Evaluation Roadmap/Inception Impact Assessment and provided substantial input during the consultation period. In addition, we recently commented on the German counterpart to the European Directive, the German IT Security Law, which is under revision and will include additional obligations and measures for 5G infrastructure security, such as mandatory certification for security critical components and a trustworthiness assessment of the supplier. Based on its solid and comprehendsive knowledge, Bitkom would like to share its position regarding the new proposal of the NIS Directive.

Bitkom is utterly convinced that the overarching objectives of the NIS Directive:

- Increasing the capabilities of Member States when it comes to mitigating cybersecurity risks and handling incidents,
- Improving the level of cooperation amongst Member States in the field of cybersecurity and the protection of essential services, and
- Promoting a culture of cybersecurity across all sectors vital for our economy and society

are not only of significant importance but even of greater relevance today when compared to the situation in 2016. In the same vein, cyber threats have increased manifold since the adoption of the first NIS Directive. That is why we welcome and support the Commissions undertaking in ramping up cyber resilience across Europe. The basic premise for ensuring a high level of cybersecurity across Europe is that all relevant stakeholders – including Operators of Essential Services (OES), Digital Service Providers (DSP), Hardware

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Sebastian Artz
Information Security & Security Policy
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder0

and Software manufacturers as well as regulators and policymakers – work together on a trustful and cooperative basis, assuming their respective responsibilities within the ecosystem. One hand must reach into the other, because the dangers in cyberspace start at the weakest spot. It must be ensured, that the burden for security and risk management of the digital economy in the EU is shared fairly and that all actors in the digital value chain contribute to this. We see the need to evenly regulate the digital value chain, including basic security requirements such as 'Security by Design' for critical products.

As before, our position is guided by the urgent need to create a more coherent and harmonised level playing field across the Union. We are convinced that common and harmonised cybersecurity rules at EU level are the most efficient way to achieve a higher level of cyber resilience. We highlight the clear need to deepen the harmonization of the European Digital Single Market and to avoid new forms of fragmentation.

Having said this, Bitkom welcomes the European Commission's proposal for a renewed NIS2-Directive which strives for a more harmonised and future-proofed cybersecurity framework. In line with Bitkom's recommendations during the consultation, the Commission opted for targeted regulatory intervention instead of adopting an entirely new legislative act and prioritizes an extension of the scope of the Directive. Both is to be welcomed and considered reasonable. However, Bitkom must call into question whether the degree of extension is chosen wisely and in a way that allows us to leverage Europe's cyber-capacities effectively. While the NIS1-Direcitve differentiated between OES and DSP giving the private sector the necessary leeway in order to develop its own content-tailored solutions and innovative ideas to significantly strengthen Europe's cyber-resilience, the NIS2-Directive withdraws the »light touch approach« for DSP. In the future, a distinction is to be made between 'Essential Entities' and 'Important Entities'.

Bitkom recognizes the European Commission's aim to simultaneously address cyber and non-cyber threats by developing the new Critical Entities Resilience (CER) Directive (COM (2020) 829). Although we are well aware of the fact that cyber-related issues are not yet fully congruent with all (physical) threat vectors to critical infrastructures, the division into IT and physical security is becoming increasingly blurred. This development is likely to continue in the years to come. In the context of critical infrastructure protection, we encourage the Commission to also understand cybersecurity as a means to an end for safety. Subdivisions based on the motivation of the attackers are irrelevant in most cases. Cybercriminals, governmental organizations or terrorists use the same procedures and affect ultimately the same objectives to which we are committed (business continuity, readiness for response/resilience, better prevention). Furthermore, the orientation by sectors is not necessarily appropriate. Attacks are

also launched against processes and procedures without any particular technical reference. The security of networks and systems can only be achieved holistically. Technology, organization, and the human factor must be included and also reflected in legislation. What is needed is a European harmonization of the included sectors as well as of the requirements (general and sectoral). This remains difficult to convey to a regional and sectoral structure of authority.

Despite the desired »single point of contact« strategy, the draft creates numerous other bodies and committees as well as cross-border integration of various authorities. A simplification of the administrative work for companies will certainly not be achieved in this way. This should be considered when further elaborating the draft. In addition, a coordinated approach by the Member States and the EU Commission would be desirable when creating new regulations. In this way, it should be avoided that some Member States already bring national regulations in motion in the run-up to new European regulations, as in Germany with the IT Security Law 2.0. This approach harbors the risk of subsequent adjustments to national regulations in line with European requirements. This creates additional and avoidable effort for the legislature, executive and the obligated companies. Instead of creating new bodies and committees, Bitkom calls for a closer cooperation between existing institutions and stakeholders. The European Commission should foster community-building and public private partnerships.

With respect to the required alignment of NIS and CER Directive, entities being classified as essential under the NIS2-Directive should be classified as critical under the CER Directive. As a consequence, the European Commission and Member States should provide critical and essential entities with one single point of contact where these entities are supposed to register, and where they can notify both cyber incidents and incidents according to Article 13 (1) of the CER Directive. Either Member States should identify what constitutes both critical and essential in their country (CER-logic), or the EU should do so for all Member States (NIS2-logic).

Last but not least, it must be underlined that innovation cycles in the field of technology are rather short and that the breakthrough potential of new ideas can hardly be envisioned beforehand. That is why it is crucial to give recent technological advances and new trends enough regulatory leeway. Any update of the EU cybersecurity policy is recommended to aim not too high but to better step back from the idea of introducing new forms of regulation before a technology has proven to be of economic, political or societal importance.

bitkom

Content

I. Chapter: General provisions

Article 2: Scope

The scope of the NIS2-Directive will be broader in comparison to its predecessor (Directive (EU) 2016/1148). The scope extents both to essential entities (Annex I), i.e. certain entities active in the sectors energy (electricity, district heating and cooling, oil, gas, hydrogen), transport (air, rail, water, road), banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space, and important entities, i.e. entities active in the following sectors postal and courier services, waste management, manufacture, production and distribution of chemicals, food production, processing and distribution, manufacturing of (a) medical devices and in vitro diagnostic medical devices, (b) computer, (c) electronic and optical products, (d) electrical equipment, (e) machinery and equipment, (f) motor vehicles, trailers and semi-trailers and (g) transport equipment, digital providers, online marketplaces, online search engines, and social networking services platforms. Only most Micro and Small entities are exempt from the Directive. Member States will establish a list of micro and small entities that fall under the Directive.

Bitkom supports an enlarged definition of what is seen as the European critical infrastructure baseline. However, referring to broad types of entities could be counterproductive and generate burdensome compliance efforts for entities that would fall under several categories. Clarity is needed to make sure that an entity can only receive one single designation. This would help contain the breadth of responsibilities and ensure consistency of internal compliance processes for the different services provided by such entity.

Having said this, it is to be welcomed that the Commission opted for considering Cloud Service Providers (CSPs) as essential entities as this approach achieves greater consistency in terms of legal obligations. In addition, Bitkom welcomes the fact that digital service providers, who provide services in multiple Member States will fall under the jurisdiction of the Member State in which they have their main headquarter. This is critical as it will avoid any regulatory overlaps as many digital service providers do in fact operate across multiple borders. As the same holds true for several digital infrastructure providers, Bitkom recommends considering digital infrastructure providers under the main establishment jurisdiction in order to ensure consistency and harmonisation. Either way, the scope of the Directive also includes »public electronic communications networks or publicly available electronic communications«. This essentially corresponds to the scope of Article 40 EECC, which is why this could result in the risk of double regulation. As Operators of telecommunication infrastructures are already covered by extensive legislation,

they should not be object to new obligations. The integration of Art. 40 & 41 would run counter to this objective and impose unnecessary and unilateral new burdens on the telecoms sector. Therefore, the mentioned provisions laid out in the EECC should be repealed and replaced by those in the NIS2-Directive and we recommend that this be maintained during the discussions of the proposal. This transition will in our view enhance the consistency of the legal framework, avoid overlaps and thereby improve legal certainty.

Although Bitkom recognizes the necessity to include more sectors under the scope of the NIS2-Directive, essential and important entities will have to implement the same measures regardless of their potential risk to other entities. Bitkom advocates a risk-based approach that enables all companies to ensure a risk-adequate level. It should not be forgotten, that the protection of networks and systems against any form of disruption is in the innermost interest of private entities

During the consultation process, Bitkom argued that any expansion and harmonization must be guided by scientific reasoning and should not be the outcome of political interests. This refers in particular to the influence of the ongoing Covid-19 pandemic. The public discourse has been marked by a different, sometimes misleading, understanding of critical infrastructures. The term was less seen under the aspect of what is worth protecting but more under the aspect of what has to function and has to be maintained. That is why **Bitkom recommend to stay focused on cyber threats within the scope of the NIS Directive and to not confound the maintenance of supply chains with the criticality of the IT to ensure the supply of a good or a service. The NIS Directive should be viewed and thought through from the latter point of departure.** Consequently, the scope of the revised Directive must be in accordance with the most serious threats for network and information systems. The Commission should stick to clear definitions and avoid any (scientifically) unjustified inflation of what should be considered as critical infrastructure. Such impulse-guided scope expansion would only lead to even more fragmentation in the aftermath of the global health crisis. In tangible terms, the NIS2-Directive incorporates, among others, entities involved in healthcare in order to include the manufacturing of vaccines, R&D facilities and manufacturers of medical devices for health emergencies. A clear definition and concise description of what exactly constitutes as a manufacturer of medical devices and also what is considered in the scope of a vaccine R&D facility would provide industry and in particular the healthcare sector with much needed clarity.

The insufficiently used (NIS) criticality prism, in particular regarding the supply chain understanding, seems to have resulted in the broad understanding of important entities, especially with respect to those entities defined under the manufacturing sector.

Besides the need to carefully (re-)examining all newly captured (important) entities by viewing each entity through the criticality prism, a common European reference system in terms of the parameterized and comprehensible determination of (sector-specific) thresholds would be of great use in practice.

By expanding the scope, the current proposal does not sufficiently address the reality of B2B environment, where one essential service provider might be the client of another essential service provider. The contractual obligations of service providers in these circumstances are not acknowledged, which could lead to legal ambiguity and overlap in reporting obligations. What is more, a business client acting as an essential entity, and that uses third-party digital servicers or digital infrastructure to serve multiple end users, would be better positioned to assess the impact and gravity of an incident than the 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.

The term »cloud computing service providers« in Annex I No.8 is relatively wide and imprecise. The current wording, for example, includes not only the providers of mere distributed storage and computing capacities, such as Amazon Web Services, iCloud or Magenta Cloud, but also software providers who offer storage space in a cloud in connection with their virtually usable software products (e. g. Microsoft Office 365). Due to further virtualization of information technology, the very broad definition could lead to successively more and more services falling under this category. Almost every service uses hosting as a partial service. To avoid this, the NIS Directive should distinguish 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. It should be clarified that the addressee of the regulations on cloud computing should not be all providers of any cloud-based software products, but only those providers whose services enable essential utility services. Companies which therefore use a »digital service« to provide their SaaS without the focus of their own SaaS being on the provision of cloud capacity to users – which are therefore »one link further down« in the »chain« of providers – should be explicitly excluded from the scope of application. This is all the more so because »cloud computing service providers« – unlike in NIS1-Directive – are now included under »essential entities« and are thus subject to far-reaching obligations.

Almost the same applies to the term »Providers of online marketplaces« in Annex II No. 6. Unlike the »Cloud computing service providers«, the former are not assessed as

»Essential Entities« but as »Important Entities«. Nevertheless, the problem regarding the classification is comparable: there is also no explicit distinction between providers whose service is primarily an online marketplace and those providers who merely »offer« such a service as a subordinate service to another service.

Article 3: Minimum harmonisation

The weakness of the first NIS Directive has been the lack of harmonization, e. g. critical infrastructures are defined differently across Europe. The objective of the review of the NIS Directive should be to overcome the fragmented legal environment at European and national level, and from an Internal Market perspective. However, this challenge is missed by the current proposal. The NIS2-Directive should increase the ambition for a better European harmonization.

Article 4: Definitions

Harmonised definitions are necessary to ensure consistent and uniform implementation of legislation. It would therefore be important for NIS 2.0 to align its definitions, such as data center or cloud computing, with international standards, for example the ISO norms. To be more specific, Data centers are now part of the essential entities but would also be assessed according to the EU security requirements according to the EU regulation, i. e. based on the ISO certifications analogous to Art. 22. This means that the industry standard in the data center & hosting sector that has so far been applicable to the German IT Security Law would only be applicable for hosting or there would be double regulation. The EU regulation with reference to the ISO standards is generally to be welcomed. The special regulation for hosting would then make no sense under the IT Security Law, especially since cloud services also contain hosting elements. Bitkom calls for a close alignment between the definitions of the NIS 2.0 and the national transpositions. This has not been the case for the NIS 1.0 and its national transpositions.

II. Chapter: Coordinated cybersecurity regulatory frameworks

Article 5: National cybersecurity strategy

The importance of national strategies to increase cybersecurity is obvious. In general, a national cybersecurity strategy is something that specifies *where* you want to go, rather than determining the *how*. In contrast, the Commission also specifies operational points for a Member State's Cybersecurity Strategy. Although unusual, this approach leaves Member States with less room for interpretation and avoids new fragmentation. This is to be welcomed. However, it is even more important that the basic orientation is well chosen so that all Member States run in the right direction.

Article 5 (1c) reads: »an assessment to identify relevant assets and cybersecurity risks in that Member State«. The expression »relevant assets« requires a clear definition.

Article 6: Coordinated vulnerability disclosure & European vulnerability registry

Bitkom welcomes the introduction of a coordinated approach to reporting and closing security gaps. Having a single, easily accessible and Commission-led platform facilitates information sharing across stakeholders and brings more clarity to the often lingering question of what to report to whom. That's why Bitkom welcomes the approach from the NIS 2.0 that mandates ENISA to establish a vulnerability registry. However, several important points must be taken into consideration:

- Vulnerability discovery and coordinated vulnerability disclosure must be footed on a trustworthy basis. Hence, there can hardly be an active involvement or cooperation with intelligence services. If the Commission foresees any hacking by governmental agencies, we have to negate such intents.

- A crucial – but so far neglected – aspect is the importance of understanding information sharing not as a one-way street. Any successful coordinated vulnerability disclosure procedure is a two-way business, requiring public entities, including intelligence services, to share their gained knowledge about vulnerabilities with the private sector so that security gaps can be addressed as fast and as effectively as possible. This accounts for any security vulnerability, regardless of whether it is an unintentional bug in the product or an intentional backdoor. In addition, the two-directional fashion of reporting vulnerabilities also requires the establishment of feedback loops towards companies to showcase what ENISA has been achieved with the provided information. The more detailed and including qualitative effects of said data-collection, the higher the awaren-

ess and the acceptance in the stakeholder groups to contribute. On the contrary, it is counterproductive when an entity that shares information about vulnerabilities with federal institutions is contacted over and over again to provide further details. That does not incentivize companies nor matches the spirit of the regulation. The Commission should leverage these soft factors.

- Sharing information, depending on when and with whom, is critical. A presumption of immediate disclosure is not always helpful in minimising risk and impact of incidents and, in some cases, exploited vulnerabilities. The Commission is well advised to also establish an information sharing mechanism that allows for anonymised reporting or through networking opportunities that collate information and share as a group. This could result in immunity from prosecution or reduced sanctions for breach.

- Bitkom encourages alignment with well-established and broadly adopted best practices and industry standards in the field of coordinated vulnerability disclosure (CVD) and vulnerability handling. We strongly support alignment with these practices, as articulated in ISO international standards such as ISO/IEC 29147 (2018) and 30111 (2019), given the globally intertwined nature of technology and vulnerability management processes. When building the desired European vulnerability registry, the focus should be primarily on those vulnerabilities that pose the greatest risk.

- Competent authorities should encourage and facilitate closer networking within the groups of essential and important entities in order to foster information sharing and learning from best practices. Such information sharing could be extended cross-border and facilitated by multiple competent authorities in numerous jurisdictions.

- While it is true that personal data may be exposed due to a cybersecurity incident, it is all the more important that there is no confusion about reporting obligations and timelines. Art. 32(3) also seems to undermine the one-stop-shop principle of the GDPR. The Directive should make clear that the GDPR is not undermined though Art. 32.

Article 7: National cybersecurity crisis management frameworks

Bitkom welcomes the EU Commission's proposal that every Member State has to adopt a national cybersecurity incident and crisis response plan. When developing and drafting such plans, Member States should be required to consult essential and important entities.

Article 8: National competent authorities and single points of contact

Despite the intended »single point of contact« strategy, the draft creates numerous additional bodies and committees as well as cross-border integration of various authorities. A simplification of the administrative burden for companies will not be achieved in this way.

Article 9 & 10: Computer security incident response teams (CSIRTs) and their tasks

In general, we strongly welcome the exchange of the CSIRTs and consider their dialog as required and desirable for strengthening cyber-resiliencies in the EU. It is a key task in the upcoming years to enhance a trustworthy ecosystem that allows governmental and enterprise CSIRTs to collaborate. The dialog should also include the globally well organised CERT and CSIRT community. In tangible terms, experiences with non-profit platforms such as the German CERT Association (»Deutscher CERT Verbund«) have proven for years that trustful cooperation based on a voluntary commitment by companies works. The Commission should take advantage of this.

However, we do not see the need to introduce any additional tasks neither for the Cooperation Group nor the CSIRTs network. Instead of extending responsibilities and information duties, the focus should be put on improving the quality of already assigned tasks in the first place. When it comes to the involvement and influence of secret services, we take a critical stance and reject any secret transmission of discovered vulnerabilities without informing manufactures. Such behavior would undermine trust and security on a broader scale and runs counter to the objective of improving the security of information systems as unpatched systems pose a threat to cybercriminals.

Having said this, Bitkom considers the operational powers of the supervisory authorities, in particular the CSIRTs and the national cybersecurity authorities (Art. 29 (2)), as too extensive. This refers in particular to Article 10 (2e) according to which CSIRTs shall have the task of: »providing, upon request of an entity, a proactive scanning of the network and information systems used for the provision of their services«. Proactive scanning activities are highly critical. Vulnerability analysis must have responsive disclosure as its objective. In addition, it must be ensured that CSIRTs do not interfere too extensively in the sovereign realm of enterprises. Apart from these concerns, the described tasks of the CSIRTs seem reasonable.

III. Chapter: Cooperation

In the light of the past experiences of our members, we strongly recommend to put the persisting communication bottlenecks into the centre of the discussion. Instead of enforcing legal compliance by means of new legal measures, we encourage a closer cooperation between the Commission, the EU Member States and the private sector. To this end, the Commission is asked to consider the broad range of impactful and promising German public-private initiatives that have already been put in place. Most notably, the alliance for cybersecurity, launched by Bitkom together with the Federal Office for Information Security (BSI) in 2012, and the UP KRITIS may serve as European role models to enhance the cross-border information sharing and to strengthen the cooperation mechanisms of the member states in the area of network and information security.

Resolving communication impasses is not only of utmost importance for addressing shortcomings and inconsistencies of the past. New communication bottlenecks are looming and must be consequently addressed in a proactive manner by the Commission – in close consultation with the Member States – before the new directive comes into being. If not properly addressed, we run risk of introducing new inconsistencies, negative feedback loops and fragmentation while actually striving for European harmonization. With this, we refer primarily to the simultaneously conducted revision of the German IT-Security Law.

Article 11: Cooperation at national level

Having a single entry point will be very important to avoid confusion about what to report to whom while losing valuable time. Near misses should not be required to be included in the reporting because (a) it is unclear what would constitute a »near miss« and (b) a »near miss« could be the result of a functioning cybersecurity defense so including these in a cybersecurity incident registry would create a misleading impression of a company's cybersecurity capabilities.

Article 14: The European cyber crises liaison organisation network (EU-CyCLONe)

Although Bitkom agrees that improvement must be made in relation to cooperation of large-scale incidents that impact more than one Member State, it does not seem necessary to create a new network, the European Cyber Crisis Liaison Organisation Network (EU – CyCLONe). The NIS 2.0 proposal has put forward three separate networks, the Cooperation Group, the CSIRT Network and the EU-CyCLONe. In order to avoid any

overlaps and improve clarity for entities, we highly recommend that clear, concise guidelines be adopted in order to ensure consistency with Member States transposition of the NIS 2.0.

Article 15: Report on the state of cybersecurity in the Union

A biennial report will be outdated by the time it is published. A shorter interval is necessary to actually create value for business and society. Instead of mere biennial PDF documents for policymakers, Bitkom calls for machine-readable datasets and corresponding interfaces (APIs) for automated evaluation in real time, ideally in form of a dashboard with well-defined indicators of the threat-landscape.

IV. Chapter: Cybersecurity risk management and reporting obligations

Article 17: Governance

Bitkom recognizes that management bodies are responsible for the cybersecurity strategy of an essential or important entity. This step will help to significantly increase the awareness for cybersecurity issues among top-level management. However, the European Commission must first publish a definition of management bodies. In addition, requirements for training of management personnel must be limited to reasonable extent. Members of the management body do not necessarily have to undergo an advanced training in order to be able to carry out assessments of cyber security risks themselves. For this purpose, there are specialists in the companies, such as CISOs, who brief them in an adequate and comprehensible form. In either way, personal accountability for non-compliance is a step too far, especially if the goal is to ensure appropriate cybersecurity awareness in companies across sectors.

Article 18: Cybersecurity risk management measures

Strong risk management frameworks play a core part in mitigating cybersecurity threats. Consistent with the NIS Directive's goal of creating a culture of risk management, and as further emphasized in the Cybersecurity Act, the NIS review should underscore the EU's continued role to facilitate the establishment and take-up of European and international standards for risk management. Therefore and instead of referring to the »state of the

art«, reference to (minimum) standards (ISMS+BCM, e.g. ISO27001 + ISO 22301) should be introduced. This would also help to provide a high degree of legal certainty for essential and important entities.

When the European Commission adopts implementing acts according to paragraph five or delegated acts according to paragraph six, it must ensure consistency between already existent national requirements and those to be adopted by the EU Commission. In Germany, for example, the national legislator has introduced, or is in the process of introducing the measures to be taken by enterprises. These are laid down in Germany's IT Security Law 2.0, and for the telco sector additionally in § 109 Telecommunication Law (§164 new) and the respective the security catalogue. Hence, there is an increased likelihood that the European Commission's delegated or implementing acts will deviate from the German regulatory framework in future, and hence, that German entities will be confronted with contradicting regulatory requirements. This must be avoided at any cost.

Moreover, the proposal remains unclear concerning the concrete implications of the requirements stipulated in Article 18 number 2d concerning »supply chain security«. Supply chain risk assessments should be based on hard evidence; the inclusion of »non-technical factors« in the assessment bears the risk of unjustified politization. Since number 2d includes »security-related aspects concerning the relationships between each entity and its suppliers or service providers« it is unclear, how essential and important entities shall ensure that a supplier or service provider complies with the requirements deemed necessary by the EU Commission. Henceforth, an essential or important entity should not by liable if a supplier or service provider is non-compliant, at least as long as an important or essential entity did everything it could contract-wise to ensure that the supplier or provider maintains a risk-adequate level of cybersecurity. In contrast, if essential and important entities were required to utilize certified ICT products and services only to guarantee supply chain security this would render business processes much more complex and ultimately increase product/service costs.

The NIS 2 proposal should envisage that Member States put further emphasis on educating and even possibly providing funding in some instances for SMEs in order to secure them. SMEs should be targeted by incentivizing them to proactively deal with their cybersecurity.

Article 19: EU coordinated risk assessments of critical supply chains

Since the cyber resilience and improved security of networks is broad and encompasses many moving parts and entities, having a requirement for the Commission to conduct supply chain security assessments for particular technologies is highly recommended and welcomed. This will ensure that the EU is up to date and abreast of recent developments in particular with emerging technologies. The ongoing (and partly diverging) implementtation of the 5G toolbox across Member States has shown the importance of closely monitoring and aligning the chosen procedures.

In general, supply chain risk assessments should be based on hard evidence; the inclusion of »non-technical factors« in the assessment bears the risk of unjustified politization. Article 19 Nr.1 reads: »The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.« The expression »where relevant« remains unspecified und requires further clarification. Any non-technical risk factors must be developed in accordance with the private sector.

In particular, any supply chain risk assessment under the NIS2-Directive must be viewed through the criticality-prism of network and information systems, outlined under Article 2. Otherwise we run the risk of losing focus and regulate (sector-specific supply chain) aspects that might be important but would be better addressed in other pieces of legislation. Therefore, it is of particular importance to focus on the functional risk relevance of companies that produce services and hardware and software components for companies covered by the NIS Directive itself.

Article 20: Reporting obligations

There is an urgent need to have a clearly defined reporting process. So far, our members face highly inefficient, redundant and non-transparent reporting structures across sectors, requiring entities to inform different (public) institutions about the very same incident while having to comply with distinct processes and timelines. Nobody wants to report too much, but too little is punishable. This makes it even more confusing for companies to report the required information to the responsible entity before the respective deadline. Instead of reporting each and every port scan, incident notification requirements should also follow a risk-based and priority-driven approach. More reporting to ever more stakeholders will not lead automatically to more security.

Having a single entry point is of utmost importance to avoid confusion about what to report to whom while losing valuable time. Such a single entry point should significantly reduce the overhead for reporting entities, for example by making use of a standardized and user-friendly online reporting tool that allows entities to notify distinct institutions about an incident by sending encrypted messages and without generating subsequent queries from different sides. In practice, essential and important entities only benefit from a threat notification obligation, if there is an institution – potentially the ENISA – that:

- systematically classifies the threats,
- organizes the automatic distribution of the threat information to participating parties and other demanding public entities,
- maintains strategic threat intelligence information, and
- reports about the trends and focuses on understanding the »most critical activities to reduce the risks«.

This should be seen in accordance with the demanded threat-landscape dashboard (article 15) to share up-to-date, anonymized and machine-readable incident information with essential and important entities.

Regarding Article 20 (5), feedback by supervising authorities within 24 hours of a reported incident could be beneficial. However, it remains unclear what is meant by reporting without undue delay »after having become aware of the incident«. »Awareness« needs further clarification. In addition, demanding initial reporting within 24 hours as well as a final report within one month (Article 20, 4) does not take into account the complexity of attacks in global enterprises. The time period is too short. For setting up an efficient reporting channel it is crucial to specify proportionate reporting obligations and grant entities at least 72 hours for reporting an incident. A final report should not be demanded before the forensic analysis is finished and measures necessary to ensure business continuity were put in place.

With the newly proposed expansion of the scope of the NIS and with additional legislative proposals being discussed simultaneously, it is now more important than ever to ensure a high level of consistency amongst all other legislations. This refers in particular to legislation such as the General Data Protection Regulation (GDPR), Payment Services in the internal market Directive (PSD2) and the EECC all have related reporting requirements, which vary with regards to entities reporting timeframes, level of information/detail and potential non-compliance penalties. The newly proposed CER-Directive should not introduce even more complexity to the reporting landscape.

Information-sharing and publication of security incidents may enhance security, but it is crucial that only essential and anonymized information is distributed if not explicitly agreed otherwise (Article 20, 6+7).

Besides the need for a more precise definition of the term »significant incident«, near misses should not be required to be included in the reporting because (a) it is unclear what would constitute a »near miss« and (b) a »near miss« could be the result of a functioning cybersecurity defense so including these in a cybersecurity incident registry would create a misleading impression of a company's cybersecurity capabilities. Above all, there should be no obligation to inform users about a »near miss«. Users or the public should only be informed if any action needs to be taken (i. e. changing passwords or to make users aware of a serious ongoing attack).

Article 21: Use of European cybersecurity certification schemes

While we are clearly in favor of certification, we reject the idea of introducing mandatory certification requirements or the prohibition of the general use of uncertified components on a broad scale. There is a distinction between certification and the provision of evidence. Providing evidence may be useful but not in form of a one-dimensional certification obligation. Any form of legally enforced mandatory certification would run counter to the logic of how companies operate on national, European and international markets. That's why national, European and international certification schemes must be valid, usable and recognized by the NIS. From our point of view, voluntary certification is found to be the best way forward. It gives companies the necessary leeway but also allows different companies to position themselves in various niches on the market.

Bitkom is in favor of promoting the use of certification schemes, especially if they are developed with stakeholder and industry engagement. Certification can play a pivotal role in ensuring trust with users and society by showcasing careful compliance to specific regimes, but there are also the cost-effective elements to schemes that companies must take into consideration before adopting.

However, the NIS 2 proposal goes ways to far when suggesting that Member States may obligate entities that are defined as an OES to adopt EU certification schemes. This would mean that, for example Cloud Service Providers, now defined as an OES will be obligated to adopt either national Cloud schemes (C5, SecNum) and potentially the EU Cloud Security (EUCS) scheme that is still being discussed and developed by the Commission and ENISA. This new provision is problematic as it essentially circumvents the Cybersecurity Act in which the promotion and adoption of certifications should be

conducted on a voluntary basis. Since the vastly increased scope of entities that now fall into the scope of the NIS, the majority of European ICT business would now be legally mandated to adopt what was once a voluntary approach to certification. In addition, the NIS 2 proposal is relatively unclear with regards to whether identified essential entities supply chain must also adhere to mandatory certification. If the certification requirements are also required for supply chain security, this would be extremely burdensome for the industry and could have significant impact in particular for SMEs, which should be out of scope.

Against this backdrop, Bitkom disapproves the sole focus on specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881, especially since these schemes were always intended to be voluntary. Rather, we urge the European Commission to propose a legislative act containing horizontal cybersecurity requirements based on the NLF as currently discussed in the European Commission's DG GROW and DG CNECT, and supported by the European Council's Conclusions on the cybersecurity of connected devices as approved on December 2, 2020.

Together with the German standardization bodies, DIN and DKE, and the BDI we support the introduction of mandatory, horizontal cybersecurity requirements based on the principles of the New Legislative Framework (NLF). When introducing a respective legislative proposal, the following recommendations should be considered:

- To achieve overarching cyber resilience, generally binding protection targets should be defined by law and these should then be specified by harmonised European standards (hEN), that reflect the dynamic development of the state of the art.

- Protective measures and resilience against cyber-attacks must be based on the specific application and the associated threat situation. The NLF allows the coverage of different risk levels and follows the necessary risk-based approach. In this context, it is the responsibility of the manufacturer as the economic actor placing the product on the market to determine the intended area of use (and thus the threat level) of the product.

- CE marking, by combining conformity assessment and market surveillance, acts as an anchor of trust for private and commercial customers alike.

- The Digital Single Market will only be successful if nationally isolated solutions are avoided and compatibility with international standards is ensured.

- With a bridge between the cybersecurity requirements of a product-centered horizontal NLF-based EU legislative act and the schemes under the EU Cybersecurity Act (CSA), the two approaches can complement each other. Thus, coherent cybersecurity requirements can be guaranteed for the products falling into the scope of the two legislative acts.

- Coherent cybersecurity requirements allow the manufacturer to choose between harmonised European standards (hEN) and CSA schemes to perform the conformity assessment according to NLF-based EU legislation. If a hEN is applied, the manufacturer can use the presumption of conformity.

Details on the proposal for introducing horizontal, mandatory cybersecurity requirements based on the NLF can be found here: https://english.bdi.eu/publication/news/eu-wide-cybersecurity-requirements/

Last but not least, and despite the undeniable added value of certification, it must be highlighted that certification needs time and resources. The more complex the systems and products and the more we certify, the longer it takes to deploy. The duration of certification procedures should not be left out of scope, certification is not an end in itself.

Article 22: Standardisation

Bitkom welcomes the technology-neutral approach adopted by the European Commission regarding recommendations for the implementation of cybersecurity risk mitigating measures. Furthermore and in contrast to IT Security Law 2.0, Article 22 refers to European and internationally recognized standards such as ISO 27001 and ISO 22301 for ISMS and Business Continuity Management, which we very much welcome. This will facilitate the spread of such universal standards. As these standards are regularly and professionally revised, it is ensured that the current state of the art is always implicitly represented.

Article 24: Jurisdiction and territoriality

With regards to the jurisdiction of DSPs, and now certain digital infrastructure providers (CSPs, electronic communication network providers) that fall into scope as essential entities, subjecting these entities to the jurisdiction of their main establishment simplifies the notification regime. We therefore welcome the approach taken by the Commission that the jurisdiction of these entities falls within the scope of where they have defined as their main establishment. The jurisdiction of cloud computing and datacenter operators

within its main establishment in the European Union is essential to avoid unnecessary bureaucratic costs.

However, and while the eIDAS reform aims at further harmonising the market for trust services in Europe, putting trust services under individual Member State jurisdiction in NIS 2 contradicts these attempts. Trust services should also fall under the jurisdiction of one member state. Also, these services are also inherently cross-border similar to the services mentioned in 24(1) which all fall under the jurisdiction of their main establishment.

In terms of directly applicable security measures, jurisdiction is largely irrelevant due to the Implementing Regulation and the ENISA guidance. However, the divergence in security measures applying to DSPs' customers can create additional burden that is not addressed by either the Implementing Regulation for DSPs or the jurisdiction regime for DSPs. In practice, the divergence in oversight regime for essential entities and DSPs is negligible.

Article 25: Registry for essential and important entities

The registration of essential entities is already required by the German BSIG. Instead of direct notification of the entities to ENISA, a notification procedure should be agreed between the BSI or generally the national regulatory authorities of the MS and ENISA. Otherwise, there is a risk that duplicate notifications will be necessary.

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. Moreover, effective cybersecurity measures, including encryption, would need to be in place to protect the information in such a registry.

V. Chapter: Information sharing

Article 26: Cybersecurity information-sharing arrangements

Art. 22 is intended to enable the exchange of information between the affected companies regarding cybersecurity (e.g., about threat scenarios, weak points, etc.). With the support of ENISA, the member states should define specific processes and technical specifications for the secure exchange of information. The objective is achieved in Germany in particular through the UP KRITIS. When dealing with an incident, the players share the necessary information with each other. In the same vein and instead of a network of the entities themselves, the national regulatory authorities should implement their own network in order to centralize the exchange of information.

VI. Chapter: Supervision and enforcement

Article 29: Supervision and enforcement for essential entities

The kind of information that competent authorities can request based on Art. 29 to exert their supervisory power is broad and unspecific. For example, it is unclear what »evidence« means with regard to the implementation of cybersecurity policies. Paragraph (5) is too broad and does not seem to be justified. In addition, it remains unclear which criteria referred to in point (d) are considered to be »fair and transparent«. The Directive also establishes responsibilities and sanctions directed at single employees »exercising managerial functions«, since the term »management« is too broadly used in companies across the Union (cf. Art. 29 Paragraph5 (b) and Paragraph 6). The Commission should refrain from introducing such a far-reaching personal liability of individual employees.

Article 30: Supervision and enforcement for important entities

Complementing the comments made under Article 29, Bitkom opposes audits and on-site inspections on cybersecurity. Such processes must be urgently streamlined to ensure minimum impact on business processes.

Article 31: General conditions for imposing administrative fines

In order to ensure that all entities implement the cybersecurity risk mitigation measures laid down in Article 18 and fulfil their reporting obligations pursuant to Article 20 the introduction of administrative fines seems justified. However, the penalty cap of 2 percent of the worldwide annual turnover is too high; the directive should further specify in which cases such a maximum penalty should apply. Instead of referring to the annual turnover, the maximum level of administrative fines should not exceed a maximum of two million EUR. In general, the Commission would be well advised not to forego the potential of incentivizing essential and important entities. Such approach is currently missing in the proposal.

Article 32: Infringements entailing a personal data breach

While it is true that personal data may be exposed due to a cybersecurity incident, it is all the more important that there is no confusion about reporting obligations and timelines. Art. 32(3) also seems to undermine the one-stop-shop principle of the GDPR. The Directive should make clear that the GDPR is not undermined though Art. 32.

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.