bitkom

At a glance

NIS Directive 2.0 – Bitkom Position

What is this about?

The European co-legislators seek 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 by updating the *Directive 2016/1148 concerning measures for implementing an equivalent and commonly high level of security in network and information systems across the Union* (NIS Directive).

Bitkom's view

Bitkom sees the imperative need for a more harmonised and future-proofed cybersecurity framework and therefore welcomes the renewed NIS Directive. The already reached compromise strikes a reasonable balance between targeted regulatory interventions and strengthening the EU's cyber-resilience holistically. However, entering the trilogue negotiations between the co-legislators, several crucial points require further consideration and respective amendments. This accounts particularly to:

- **Incident reporting.** Demanding initial reporting within 24 hours and an "initial notification as an early warning" – without specifying how such an early-warning-system could even work in practice – runs counter to the complexity of cyberattacks. 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. Bitkom is concerned that private entities misspend their important, limited resources – needed to be working on incident mitigation and remediation – in a time-critical situation on distributing little useful information to authorities.
- **Coordinated vulnerability disclosure (CVD) and vulnerability handling.** Bitkom welcomes ENISA playing a more central role in global CVD efforts, supports Member States establishing national policies for CVD and – to make efforts a success – strongly encourages close alignment with well-established and broadly adopted international standards such as ISO/IEC 29147 (2018) and 30111 (2019) rather than starting a new ENISA vulnerability registry.
- **Cybersecurity risk management measures.** Instead of listing certain – even though useful – cybersecurity measures, Bitkom recommends to rather refer to (minimum) standards (ISMS+BCM, e.g. ISO27001 + ISO 22301). This would not only help to provide a high degree of legal certainty for essential and important entities but also be the best fit to the envisioned state-of-the-art, risk-based, "all-hazard" approach.
- **Public administration.** Bitkom supports an enlarged definition of what is seen as the European critical infrastructure baseline and welcomes the chosen risk-based approach. However, considering the significant scope extension for private entities, it is inappropriate to exclude public administrations – as proposed by the Council. It neither complies with the ambitions to protect the citizens nor does it seem reasonable in the wake of the threat landscape for public entities.
- **Trust service providers.** To achieve the goal of a fully harmonized market for trust service providers, the scope of the NIS2 should not be expanded on trust service providers. It should rather be ensured that only one regime (the fully harmonizing eIDAS Regulation) is applicable for them with implementing acts established by the Commission and there is only one responsible supervisory body in each Member State. The regulations provided by the NIS2 Directive can also be integrated in the eIDAS Regulation (f.e. in Art. 19).
- **Legislative harmonisation at European level.** Since the NIS 2.0 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. Hence, Bitkom appreciates the EP´s proposal that the EC should issue guidelines which Articles of NIS2 apply, if they would exceed the DORA requirements ("gap analysis"), which would facilitate harmonisation.

NIS Directive 2.0 – Bitkom Position for the trilogue negotiations

3 January 2022

General remarks

Bitkom is utterly convinced that the overarching objectives of the *Directive 2016/1148 concerning measures for implementing an equivalent and commonly high level of security in network and information systems across the Union* (NIS Directive):

- increase the capabilities of Member States when it comes to mitigating cybersecurity risks and handling incidents,
- improve the level of cooperation amongst Member States in the field of cybersecurity and the protection of essential services, and
- promote 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 Bitkom welcomes and supports the 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 essential and important entities, hardware 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 security requirements based on the guiding principles 'Security by Design' and 'Security by Default' for critical products as well as by following the concept of 'Zero Trust'.

As before, Bitkom's 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.

Bitkom
Federal Association
for Information Technology,
Telecommunications and
New Media

Sebastian Artz
Head of Cyber- & Information Security
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Having said this, Bitkom appreciates the highly professional and fast handling of the legislative process and welcomes the already reached compromise for a renewed NIS-Directive. Instead of repeating unheard aspects from previous Bitkom position papers at this advanced point of discussion, Bitkom seeks to focus hereafter on those aspects that are still under discussion among the three co-legislators and that would benefit from a more industry-friendly orientation when striving for more cyber-resilience in Europe.

Content

General provisions (Chapter I)

Article 2: Scope

Bitkom supports an enlarged definition of what is seen as the European critical infrastructure baseline and welcomes the chosen risk-based approach. However, considering the significant scope extension for private entities, it is inappropriate to exclude public administrations – as proposed by the European Council. It neither complies with the ambitions to protect the citizens nor does it seem reasonable in the wake of the threat landscape for public entities. Organizations of the public administration are also exempt from the obligations of Art. 17 and the sanction regime – laid down in Art. 29, para 5. – is not applicable for employees of the public sector, whereas in the private domain the management organization remains responsible for cybersecurity action plans. Considering the evolving threat landscape, this is a disproportionate policy towards public and private managements, and hence not justifiable. Recent cyberattacks on public entities have demonstrated its impact on the public in general. Although the exclusion of entities with core activities in the areas of Defense, National and Public Security, Justice, Parliaments and Central Banks is comprehensible, common minimum standards should be agreed and laid down in separate regulation, to be proposed by the European Commission.

We welcome the European Commission's proposal to clarify (in Recital 69) that the GDPR considers processing of personal data for ensuring network and information security a legitimate interest. The Parliament built upon the Commission's intent by adding a new Article (Article 2, 6a) to help member states to reinforce this legal basis when transposing implementing NIS 2.0 in national laws. We the negotiators to accept the Parliament's approach, which would also help to create legal clarity for cybersecurity stakeholders.

All entities need legal certainty to implement the measures required in the NIS 2.0. The required security measures also cover the processing of personal data. The Commission only explains in a recital (69) which activities fall under GDPR, 6, 1f) in the context of NIS 2.0 activities. Personal data may be used for cybersecurity purposes under GDPR, art. 6, 1f (legitimate interest), but always require the data processor to perform a balancing test between processing personal data for a "legitimate interest" and the fundamental rights and freedoms of the data subject under the GDPR. If EU legislators want to promote cybersecurity – the prerequisite for privacy and data protection – they should consider introducing a new article in NIS 2.0 that provides a solid legal basis for activities under NIS 2.0. In Recital 69, the Council states that "the processing of personal data by essential and important entities [...] could be considered necessary for compliance with the legal

obligation (GDPR 6.1 c) [...]." This is not enough. Bitkom is in favor of the proposal made by the European Parliament to introduce the proposed new article (2, 6a new):

- *"Essential and important entities, CSIRTs and providers of security technologies and services, shall process personal data, to the extent strictly necessary and proportionate for the purposes of cybersecurity and network and information security, to meet the obligations set out in this Directive. That processing of personal data under this Directive shall be carried out in compliance with Regulation (EU) 2016/679, in particular Article 6 thereof."*

Regarding trust service providers, Bitkom suggests to delete in the NIS2 directive Art. 2 (2) (ii) and (iii), Art. 39 and „-Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014" in Annex I No. 8 due to the following reasons:

- Annex I No. 8 and Art. 2 (2) (ii) and (iii) expand the scope of the NIS2 Directive to qualified and non-qualified trust service providers. Art. 39 provides the deletion of Art. 19 of the eIDAS Regulation, which establishes security requirements for trust service providers, including technical and organisational measures to manage security risks and information obligations.
- These provisions counteract the goal of the eIDAS Regulation to ensure a fully harmonised framework by causing a fragmentation of provisions and supervisory responsibilities. A regulation such as eIDAS enjoys priority of application over national legislation in comparison to a directive which Member States must implement as national law. If the subject matter of trust services, which is "harmonised" by the existing eIDAS Regulation, is now "removed" from the eIDAS Regulation and regulated by a Directive, which must be transposed nationally, this would represent a clear deterioration in terms of harmonisation and the creation of a digital single market in Europe. The currently discussed proposal of NIS 2.0 undermines – at least temporarily and without necessity – a relatively advanced harmonisation and thus worsens the market situation of trust service providers.
- Hence, it should rather be ensured that only one regime (the fully harmonizing eIDAS Regulation) is applicable with implementing acts established by the Commission and there is only one responsible supervisory body in each Member State. The regulations provided by the NIS2 Directive can also be integrated in the eIDAS Regulation (f.e. in Art. 19), with the advantage that trust service providers can offer their services in a fully harmonized market, which a directive is not able to achieve.

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 but also software providers who offer storage space in a cloud in connection with their virtually usable software products. 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 is 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.

Coordinated cybersecurity regulatory frameworks (Chapter II)

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, Commission-led platform facilitates information sharing across stakeholders and brings more clarity to the often-lingering question of what to report to whom. However, several important points must be taken into consideration:

- Bitkom supports member states establishing national policies for coordinated vulnerability disclosure and management and 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 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 database, the focus should be primarily on those vulnerabilities that pose the greatest risk.

- We support ENISA playing a more central role in global coordinated vulnerability disclosure and management efforts. However, we caution against ENISA starting a new vulnerability registry. This will be redundant, introduce bureaucracy, and harm cybersecurity efforts. Instead, ENISA should:
  - Establish a European vulnerability database that leverages the global CVE registry. A European database could provide details on risks, impacts, and fixes in EU languages and focus on ICT products developed or used in the EU.
  - Play a stronger role in the global CVE registry by 1) becoming a "Root CVE Numbering Authority (CNA)" to it and 2) joining the global CVE program's board of directors.

- 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 co-legislators are 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.

- 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 through Art. 32.

- 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 awareness 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.

Cybersecurity risk management and reporting obligations (Chapter IV)

Article 18: Cybersecurity risk management measures

Strong risk management frameworks play a core part in mitigating cybersecurity threats. Bitkom supports cybersecurity trainings; the use of cryptography; the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within an entity as proposed by the European Parliament in Article 18 paragraph 2 points fa, fb and fc. However, those cybersecurity measures are only a fraction of useful measures. Instead of listing an uncomprehensive list of certain cybersecurity measures, Bitkom recommends to rather refer explicitly to (minimum) standards (ISMS+BCM, e.g. ISO27001 + ISO 22301). This would not only help to provide a high degree of legal certainty for essential and important entities but also be the best fit to the envisioned state-of-the-art “all-hazard”

approach. The European Parliament proposes the following amendment in Article 18 paragraph 1:

- *Member States shall ensure that essential and important entities take appropriate and proportionate technical**, operational** and organisational measures to manage the risks posed to the security of network and information systems which those entities use **for their operations or for** the provision of their **services and prevent or minimise the impact of incidents on recipients of their services and on other** services. Having regard to the state of the art **and to European or international standards**, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.*

Bitkom supports this.

Regarding supply chain security, 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.

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) implementation of the 5G toolbox across Member States has shown the importance of closely monitoring and aligning the chosen procedures.

As stated before, 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. Critical ICT services, systems, and products shall be hierarchical and focusing

on and sensitive functions. Any non-technical risk factors must be developed in accordance with the private sector.

Article 20: Reporting obligations

The European Commission's NIS 2.0 proposal includes a section on mandatory security incident reporting. Bitkom is concerned that the definitions of what must be reported and by when (within 24 hours) will, in practice, result in little useful information being available and tie up important resources that are supposed to be working on incident mitigation and remediation and would not be useful to EU governments in terms of improving cybersecurity.

In September 2021, global companies came together to publish the *Global Policy Principles for Security Incident Reporting*, a set of recommendations on how policymakers can develop meaningful incident reporting systems. These include providing at least a 72-hour reporting window after a company has verified an incident and limiting incident reporting to confirmed or verified incidents (these principles, linked above, provide useful explanations of why these approaches are better for security). Demanding initial reporting within 24 hours does not consider the complexity of attacks in global enterprises. 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. From Bitkom's point of view, the European Parliament has found an acceptable compromise in its position (Art. 20, 4a), stating that:

- *"4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT: (a) an initial notification of the significant incident, which shall contain information available to the notifying entity on a best efforts basis as follows: (i) with regard to incidents that significantly disrupt the availability of the services provided by the entity, the CSIRT shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident; (ii) with regard to incidents that have a significant impact on the entity other than on the availability of the services provided by that entity, the CSIRT shall be notified without undue delay and in any event within 72 hours of becoming aware of the incident."*

The Parliament, recognizing the challenges with short reporting windows, proposed (for Article 20) that for any period shorter than 72 hours, only incidents that impact availability

of services (the “A” in the confidentiality- integrity-availability (C-I-A) triad) should be reported. Bitkom supports this. While Bitkom continues to believe the 72-hour window is ideal, this compromise greatly improves the Commission’s original proposal. Of the three, it is more reasonable to report incidents impacting availability in that timeframe because often times loss of availability is much clearer within a 24-hour window.

Besides the time window, Bitkom sees the need for action in the Council and the parliamentary version regarding the type of event that shall be reported. Bitkom recommends focusing exclusively on actual security incidents and specific threats. If all non-manifested "near misses" risks/threats as well as all "cyber-threats" had to be reported proactively, this would disproportionately increase the effort for reporting companies without providing useful information for authorities. With regard to the duty to inform customers about cyber-threats, it seems disproportionate to report general threats in addition to company- or sector-specific threats to a company, as this would not only lead to unnecessary effort, but also does not seem appropriate (e.g. incorrect/incomplete assessment of the threat situation). These regulations should be specified with clear definitions and ideally criteria developed together with industry or even sector-specific if necessary, especially if companies could be subject to penalties in case of lacking/incorrect reporting of threats. Bitkom is in favor of voluntary reporting of "near misses" and cyber-threats, as provided for in Article 27. In addition, it remains unclear what the European Parliament as well as the European Council understand as an early warning (Article 20 paragraph 4 point a). What kind of information shall be submitted as an early warning and how does an early warning system look like? The term “early warning” requires a clear definition.

In general, 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. Even if the NIS Directive still has to be transposed into national law, Bitkom would like to point out here that the structures and future processes should be coordinated as far as possible, should not contain duplicate reports for the same incidents, and reports in the respective mandate should be used, passed on or recycled by several supervisors. Bitkom sees greater

need for coordination between the supervisory authorities concerned (e.g. between the BaFin and the BSI).

To this end, having a single-entry point is of utmost importance. 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.

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 as well as the Digital Operational Resilience Act (DORA regulation) should not introduce even more complexity to the reporting landscape.

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 too far when suggesting that Member States may obligate entities to adopt EU certification schemes. 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 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.

Against this backdrop, Bitkom appreciates the European Parliament's approach that foresees the inclusion of internationally recognised certification schemes as a basis for certification.

Finally, 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 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.

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.

Supervision and enforcement (Chapter VI)

Article 29: Supervision and enforcement for essential entities

In case of a cyber-incident, the combined effort of all concerned should be focused on mitigating the implications for Europe's society and industry rather than initiating an unnecessary blame-game. Therefore, Bitkom appreciates the deletion of Article 29 paragraph 4 point i, proposed by the European Council, as naming and shaming will not enhance Europe's cyber-resilience.

Regarding the responsibilities of members of management bodies (Article 29 paragraph 5b), Bitkom appreciates that the ITRE Committee changed Article 29 paragraph 5b insofar as a temporary ban against any person holding managerial responsibilities at chief executive officer or legal representative level in that essential entity is now considered only as an ultima ratio. In addition, Bitkom welcomes the deletion of any reference to other employees as they do not have the necessary decision powers within an entity to implement certain measures regarded as necessary by law if a CEO withholds the necessary money for such activities.

Article 29 & 30 paragraph 2 point (c) make use of the term "security scan" without properly defining what is meant by that. Bitkom supports the text introduced by the European Council limiting security scans. Intrusive and unannounced "security scans" are problematic with regard to cyber security as, if done incorrectly, could trigger a cyber incident of its own.

Article 31: General conditions for imposing administrative fines

Bitkom appreciates the range of fines proposed by the European Council including a differentiation between essential and important entities. The co-legislators should agree on the framework proposed by the European Council, i.e. 4 million Euro or two per cent of annual turnover in the case of essential entities; and 2 million Euro or one per cent of annual turnover in the case of important entities respectively.

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.