bitkom

Position Paper

2026 May

NIS-2 Amendments

Summary

The NIS-2 Directive set the goal to establish a unified legal framework to uphold cybersecurity in critical sectors across the EU. By defining technical and methodological requirements for cybersecurity risk management measures, it aims to create a harmonised baseline level of protection. Bitkom continues to believe that NIS-2 can deliver a significant improvement in cybersecurity across the EU. However, the transposition into national law has proven difficult, and to date not all Member States have successfully completed transposition. Germany, for example, only put NIS-2 into force on the 6th of December 2025. These implementation challenges underscore that targeted improvements and amendments to NIS-2 are necessary. A key challenge underlying these implementation difficulties is the fragmented nature of national transposition, which continues to undermine the objective of a truly harmonised cybersecurity framework across the EU. Fragmented national transposition also directly undermines the integrity of the EU internal market: diverging national requirements lead to increased compliance costs, delayed incident handling, duplicate reporting obligations and inconsistent supervisory expectations for cross-border operators, without delivering a commensurate increase in cybersecurity or resilience. Cybersecurity objectives can only be achieved efficiently if rules are implemented and enforced in a coherent and uniform manner across all Member States.

Bitkom therefore welcomes key elements of the proposed amendments to NIS-2. For example, including operators of submarine data transmission infrastructure within the Directive's scope appropriately reflects the critical role submarine cables play for global connectivity and for economic activity across sectors. Bitkom also supports the reinforced approach in Article 21(5), which obliges the Commission to regularly assess the need for implementing acts introducing technical, methodological or sector-specific requirements to improve the functioning of the internal market. The explicit commitment to an open, transparent and inclusive consultation with relevant stakeholders and Member States is of central importance, as early and structured engagement with industry is a prerequisite for developing requirements that are practicable, technologically feasible and proportionate to the risk environment. While the proposal includes certain targeted clarifications of the Directive's scope, these remain selective and do not address broader issues of over-inclusiveness. A general

provision should therefore clarify that activities which constitute only an insignificant ancillary part of an entity's overall business should fall outside the scope of NIS-2. Such an approach would support a more proportionate application of the Directive and reflects practices already adopted in some Member States. Overall, amendments should prioritise EU-wide standardisation and prevent national gold-plating that would further fragment compliance across the internal market.

However, existing reporting and documentation obligations remain largely untouched and continue to be shaped by divergent national requirements. Bitkom considers it particularly important to reduce unnecessary administrative burdens that can impede effective incident response. In practice, companies continue to face significant uncertainty not only due to differing timelines and reporting formats, but also regarding the applicable legal framework for specific types of incidents, the competent authority, and the expected level of technical detail at each stage of the reporting process, as well as the definitions relevant for determining reporting obligations. Reporting requirements should be simplified and standardised. The introduction of additional, incident-specific rules risks further complicating an already fragmented framework. Instead, harmonised reporting templates, timelines and processes should be developed and aligned across relevant EU legislation, including, inter alia, NIS-2, CER, GDPR, CRA and other related frameworks, to ensure consistency and usability in practice. For cross-border operators, NIS-2 should move towards a single EU-wide reporting entry point or a coordinated one-stop-shop mechanism, allowing one notification to trigger coordinated handling across Member States. Furthermore, NIS-2 should introduce a clear intra-group provision to address inefficiencies arising from fragmented compliance obligations. For groups of undertakings, the controlling entity should be allowed to fulfil registration and reporting obligations on behalf of all relevant entities within the group. This would significantly reduce administrative duplication and ensure a more consistent and coordinated approach to compliance and incident handling.

The current 24-hour deadline for an initial notification to the responsible authority can impose significant operational strain on companies, especially SMEs, at precisely the time when resources must be concentrated on containment and recovery. A more workable and consistent approach would be to align the first notification timeline with the GDPR, allowing an initial notification after 72 hours, to help ensure early notifications are meaningful and based on sufficiently verified information, followed by a follow up report 14 days and a final report due one months after incident closure. More broadly, any meaningful burden reduction requires a systematic harmonisation of reporting obligations across relevant EU legislation, including, inter alia, the GDPR, the AI Act, eIDAS, the Cyber Resilience Act (CRA) and related frameworks. The current approach falls short of establishing such coherence. Diverging interpretations of key definitions, such as «significant incidents" under Article 23(3), persist across Member States. This poses a particular challenge for companies operating across the EU in several Member States, as it creates diverging expectations and requirements. To address this, the Commission should establish binding EU-wide definitions, thresholds and reporting templates through implementing acts. Sole reliance on non-binding guidance is insufficient to ensure consistent supervisory expectations across Member States. These challenges also highlight a more structural issue: the Directive-based

approach has led to fragmented national transposition and inconsistent legal frameworks across Member States. This fragmentation creates significant administrative overhead, particularly in a context where amendments to NIS-2 must again be implemented at national level while initial transposition is still ongoing in several Member States. In the medium term, a fully harmonised approach should be considered to ensure consistent implementation and reduce complexity for cross-border operators.

In addition to further harmonising reporting obligations, the effectiveness of NIS-2 could be strengthened by enabling affected entities, where appropriate, to access structured governmental support during the initial analysis and triage of significant incidents. Such support would help improve the assessment of root causes, potential systemic relevance, and possible cross-border or state-sponsored implications. Building on this, access to specialised technical expertise should be facilitated to support deeper investigations, impact mitigation, and, where necessary, digital recovery efforts. This would enhance collective situational awareness and overall incident response effectiveness, while maintaining the primary responsibility of the affected entities.

The ongoing revision of the European Cybersecurity Certification Framework (ECCF) under the CSA-2 should be closely aligned with the simplification of NIS-2 requirements. A clear presumption of conformity for entities holding relevant cybersecurity certifications would significantly increase legal clarity and reduce administrative overhead. To avoid further fragmentation, Member States should not introduce national gold-plating that deviate from EU-level certification schemes. Such national additional audits or certification requirements would undermine the harmonising effect of EU-level certification schemes and negate the intended benefits of a presumption of conformity. At the same time, certification must remain one possible pathway to demonstrate compliance with NIS-2, without becoming a mandatory baseline obligation. Entities should retain the flexibility to choose appropriate means to evidence conformity, reflecting differences in size, risk exposure, sectoral context and existing governance structures.

Bitkom sees a need to further refine several aspects of the proposal to ensure proportionality, legal certainty and effective implementation across Member States. The following amendments highlight areas where further clarification or adjustment is necessary to strengthen the Directive's practical impact and preserve coherence with existing obligations:

Revision to Art. 2 (a) (ii) (iv) (v) (Providers of European Digital Identity Wallets and providers of European Business Wallets)

The proposed revision with connection to No. 910/2014 (Regulation of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market). This Regulation applies to electronic identification schemes that have been notified by a Member State, and to trust service providers that are established in the Union. NIS-2 explicitly contains a «lex

specialis" mechanism: if sector-specific Union legal acts contain requirements on cybersecurity measures and/or reporting obligations that have "at least equivalent effect" and ensure that NIS-2 authorities have "direct" access to reports, these special regimes take precedence over NIS-2. eIDAS meets these criteria for trust services and the EUDI wallet, because eIDAS prescribes specific security measures, incident reporting within 24 hours and ongoing monitoring, eIDAS anchors official information flows to ENISA and (since the eIDAS amendment) structured cooperation with NIS-2 authorities, so that the required "direct access" to security reports is established. Therefore, a parallel submission to general NIS-2 obligations would create duplication of notification, supervision and sanctions, friction and legal uncertainty without measurably increasing cybersecurity. The targeted solution lies in the consistent application of the eIDAS regime including its – already standardised – interfaces to NIS-2 and there is no need to add the Digital Identity Wallets and European Wallets. Against this background, trust services should also be removed from the scope of NIS-2 in order to ensure harmonisation.

Revision to Art. 3(1) (Essential and important entities)

The proposed revision would shift the size thresholds for entities in scope from medium-sized companies to small mid-caps. As a result, entities listed in Annexes I and II, subject to specific derogations, would fall under NIS 2 once they reach small mid-cap status or above. Bitkom welcomes this increase in the threshold, as it would considerably ease administrative and compliance burdens for small and medium-sized organisations overall. At the same time, the transition to the revised scope must avoid legal uncertainty and unnecessary compliance investments by companies currently covered by NIS-2 but likely to fall outside its amended scope. Requiring such companies to invest in technology, personnel and internal processes only to exempt them shortly thereafter would undermine trust in the predictability of the regulatory process. However, the proposal still does not draw a sufficiently clear distinction between essential and important entities in terms of the obligations they must meet. In practice, both groups would continue to be subject to largely comparable measures, regardless of differences in their actual risk exposure or criticality. A stronger risk-based differentiation is therefore needed to ensure that requirements are calibrated to the role and threat profile of the respective entity.

Revision to Art. 24(4-6) (Use of cybersecurity certification schemes

The proposal would allow essential and important entities to obtain a cyber posture certificate under a European cybersecurity certification scheme to evidence compliance with applicable cybersecurity requirements, including conformity with relevant EU implementing acts or national transposition rules. Bitkom supports the underlying intention to use certification as a means of demonstrating compliance and welcomes

the potential of EUCF cyber posture certificates to provide a presumption of conformity. At the same time, any such approach should properly acknowledge existing standards and established procedures. Many organisations already rely on certifications based on internationally recognised frameworks, including ISO 27001. The European Commission should therefore actively encourage the use of these international standards and ensure that European certification pathways build on them, in order to avoid duplicative requirements and unnecessary additional administrative effort.

Revision to Art. 41 (Transposition)

Under the proposal, Member States would be required to adopt and publish the measures necessary to comply with the Directive no later than 12 months after its entry into force and to apply those measures from the day after that period expires. While timely transposition is important, Member States need adequate time to transpose NIS 2 into domestic law in a legally sound and practicable manner. Moreover, if the Directive were to apply immediately after the 12-month transposition period ends, entities would effectively lack any meaningful implementation phase. In addition to sufficient transposition periods, entities require predictable and harmonised EU-wide go-live logic; diverging national start dates or phased application should be avoided to ensure planning security. Bitkom therefore calls on the European co-legislators to ensure that companies are granted at least six months after the ratification of the national transposition act to adjust internal processes and compliance structures accordingly.

Revision to Annex I, point 1(a) (Electricity subsector)

The introduction of a 1 MW threshold in Annex I, point 1(a), is welcome, as it reflects a proportionate and risk-based approach to the application of cybersecurity obligations in the electricity subsector. However, the current drafting refers to an operator's total generation capacity, meaning the aggregated capacity of all generation assets operated by one entity. As a result, operators of multiple small-scale installations may still fall fully within scope, even where each individual installation remains well below 1 MW.

This significantly reduces the intended relief effect of the threshold, particularly for decentralised photovoltaic business models, which often rely on a large number of small generation units. To ensure that the exemption is effective and proportionate, the threshold should therefore be applied at the level of the individual generation installation, rather than on the basis of the operator's aggregated total capacity. This would better reflect the actual risk profile of the assets concerned and help avoid unnecessary regulatory burdens for genuinely small-scale operators.

Bitkom represents more than 2,300 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 700 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Felix Kuhlenkamp | Head of Security
P +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Responsible Bitkom committee
WG Security Policy