August 2026

Cybersecurity Update: Proposed Amendments to the NIS2 Directive and Proposal for a New Cybersecurity Act

In spring 2026, the European Commission presented a cybersecurity package that includes proposed amendments to the NIS 2 Directive and a proposal for a new Cybersecurity Act (CSA 2). While the amendments to the NIS2 Directive are aimed at clarifying and simplifying the existing framework, the new CSA 2 is intended to establish a harmonized framework for the security of information and communication technology (ICT) supply chains and for cybersecurity certification. This may impose additional compliance requirements on affected companies.

I. Reform objective: Simplification and harmonization

The Commission seeks to simplify compliance with the NIS2 Directive, which has so far been criticized as administratively burdensome, while at the same time promoting harmonization. The Cybersecurity Package is intended to improve the interaction between the NIS2 Directive, the proposed CSA 2, and sector-specific legislation. The proposed reform therefore aims to streamline procedures and enhance coherence, while also strengthening the overall level of cybersecurity within the European Union.

Against this background, the package seeks to reduce national fragmentation while strengthening European certification mechanisms and coordinated supervisory structures. While the amendments to the NIS2 Directive primarily provide for targeted clarifications and simplifications, the CSA 2 introduces a more far-reaching EU-wide framework for trusted ICT supply chains.

II. Amendments to the NIS2 Directive[1]

1. Scope of the NIS2 Directive

The Commission proposes several targeted but practically significant **clarifications regarding the scope of application of the NIS2 Directive**. Among other things, operators of submarine data transmission infrastructure, including landing stations and the terrestrial parts of the submarine cable are to be classified as essential entities (Annex I, point 8, NIS2 Directive as amended). According to the Commission, this is intended to ensure that all operators of submarine data transmission infrastructure are covered by the NIS2 Directive, in light of the increasing risks to such infrastructure and its resulting high criticality (Recital 6 of the NIS2 Amending Directive). Furthermore, certain sectors, including healthcare, electricity, hydrogen, as well as the manufacture, production and distribution of chemicals, are further specified to reduce uncertainty (Annex I, points 1a, 1e, and 5; Annex II, point 3, NIS2 Directive as amended).

Practical note: In Germany, the scope of the NIS2-related obligations is determined by Section 28 BSIG. In addition to the entities listed in Annexes 1 and 2 to the BSIG it also covers operators of critical entities. In May 2026, a draft of the KritisVO[2] (Critical Infrastructure Ordinance) was published, providing detailed rules for the classification of critical entities under Section 28 BSIG.

A new category of undertakings, referred to as "**small mid-caps**", is also to be introduced. This category comprises undertakings employing fewer than 750 persons and having an annual turnover not exceeding EUR 150 million, or whose annual balance sheet total does not exceed EUR 129 million (Art. 6(2) NIS2 Directive, as amended). Although small mid-caps will continue to fall within the scope of the NIS2 Directive where they operate in sectors covered by the Directive, they shall be classified as "important entities" rather than "essential entities" in order to limit their compliance burden (Art. 3(1)(a) and (2) NIS2 Directive, as amended).

Practical note: Under the current German implementation regime, important entities and particularly important entities – the latter corresponding to essential entities in the terminology of the NIS2 Directive – are generally subject to the same core obligations.[3] These include, in particular:

- risk management measures (Section 30 BSIG);
- reporting, registration, and notification obligations (Sections 32 – 35 BSIG);
- implementation, oversight, and training obligations of management bodies (Section 38 BSIG)

The classification of an entity as an "important entity" or a "particularly important entity" may affect the extent of the required risk management measures, as such measures must be proportionate to the entity's risk exposure (Section 30(1) BSIG).

2. Harmonization of Technical Security Requirements

In addition, the proposal aims to further specify the technical and methodological requirements for risk management measures **by means of Union-wide binding implementing acts**. Once such implementing acts have been adopted, Member States can no longer impose further requirements (Art. 21(5), fifth

[1] https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act

[2] available at: https://ag.kritis.info/wp-content/uploads/2026/05/260526_Entwurf-Kritisverordnung.pdf

[3] https://www.sza.de/assets/downloads/2026-01-05-SZA-Mandanteninformation-Nis2-CRA.pdf

subparagraph, in conjunction with Art. 5 NIS2 Directive, as amended).

This considerably limits Member States' scope for national approaches, for example with regard to the design of technical security measures. At present, Art. 5 NIS2 Directive provides that Member States are generally not prevented from adopting or maintaining provisions that ensure a higher level of cybersecurity. At the national level, Section 30(5) BSIG provides the possibility, under certain conditions, to impose cybersecurity measures that go beyond the requirements laid down in such implementing acts.

3. Supply Chain Security

The Commission expressly addresses concerns frequently raised in practice regarding heterogeneous and **extensive supply chain questionnaires**. Therefore, Commission guidelines shall establish uniform requirements as to the structure, format, and level of detail of such information requests (Recital 9 of the NIS2 Amending Directive).

4. Reporting and Information Obligations

The Commission proposes to **harmonize the collection of information relating to ransomware attacks**. Entities will therefore be required, upon request, to disclose whether a ransom was paid and, where applicable, the amount and the recipient of the payment (Art. 23(12) and (13) NIS2 Directive, as amended).

Certain entities will furthermore be required to notify **the Federal Office for Information Security (BSI) more rapidly about any changes to the information submitted in the registration process** (currently specified in Section 34 BSIG). This concerns the entities referred to in Section 60(1) BSIG, including providers of data center services and online marketplaces, as well as social networking service platforms. The existing three-month deadline (Section 34(2) BSIG) is to be reduced to two weeks (Art. 27(3) NIS2 Directive, as amended). This two-week deadline already applies to the less extensive registration obligation under Section 33 BSIG, which covers all undertakings falling within the scope of the NIS2 Directive (Section 33(5) BSIG).

5. Strengthening the Role of ENISA

The EU Agency for Cybersecurity (ENISA) is to assume a stronger role in the coordination of supervisory activities concerning undertakings operating in more than one Member State. Article 27(1) of the NIS2 Directive, as amended, provides, inter alia, for a **central register of all undertakings falling within the scope of the NIS2 Directive** (whereas the register currently covers only certain categories of entities). In addition, ENISA is to support cross-border supervisory activities (Art. 37a NIS2 Directive, as amended).

III. New Cybersecurity Act[4]

1. Supply Chain Security

Title IV of the CSA 2 establishes a uniform EU-wide framework for the security of so-called "**trusted ICT supply chains**". It is not primarily concerned with technical vulnerabilities of individual products, but rather with structural risks arising, in particular, from third-country suppliers associated with economic espionage, cyberattacks, or state-sponsored campaigns against the Union or its Member States may emanate (Recital 129 CSA 2). The trusted ICT supply chain framework applies to undertakings operating in highly critical and critical sectors within the meaning of Annexes I and II to the NIS2 Directive, including the energy, telecommunications, healthcare, transport, and digital infrastructure sectors (Art. 98(1) CSA 2).

The Commission is to be empowered to **designate third countries as countries posing cybersecurity concerns** (Art. 100 CSA 2). Relevant factors include, inter alia, the extent to which the state may exercise influence over undertakings, the absence of rule-of-law safeguards, and documented state-sponsored

[4] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act

cyberattacks. Such designation is linked to the classification of "**high-risk suppliers**", namely undertakings established in, or controlled by, such countries (Art. 2(39) CSA 2). These high-risk suppliers may, inter alia, be excluded from certain EU funding programmes and public procurement procedures (Art. 100(4)(e) and (f) CSA 2).

Furthermore, the Commission is to be empowered to designate **specific ICT components or systems as "key ICT assets"** (Art. 102 CSA 2). Such designation depends on whether the components or systems perform essential and sensitive functions for entities covered by Annexes I and II to the NIS2 Directive.

Where such key ICT assets originate from high-risk suppliers, the Commission is to be empowered to **prohibit undertakings falling within the scope of the NIS2 Directive from using, installing or integrating such assets** (Art. 103(1) CSA 2). However, the Commission's may also impose mitigating measures and prohibitions concerning the use of key ICT assets supplied by "non-high-risk" suppliers (Art. 103(2) and (7) CSA 2).

With regard to mobile communication networks, the CSA 2 already contains a definition of key ICT assets, including, inter alia, core network functions of 5G networks. Where such components originate from high-risk suppliers, they are to be phased out gradually (Art. 110 in conjunction with Annex II, point 1, CSA 2). The use, installment and integration of such key ICT assets are to be prohibited (Art. 111(1) CSA 2).

The authorities already designated under the NIS2 Directive are to be responsible for enforcing the supply chain security obligations (Art. 112(1) CSA 2); in Germany, this will generally be the BSI. To this end, the authorities are to be granted extensive **supervisory and enforcement powers** (Art. 114 CSA 2). In addition, infringements of these obligations may give rise to **penalties** of up to 7% of the worldwide annual turnover of the preceding financial year (Art. 115 CSA 2).

2. Certification

In addition to these supply chain-related obligations, the CSA 2 is also intended to reform the **European cybersecurity certification framework**. Under the current legal framework, cybersecurity certificates may already be issued based on European cybersecurity certification schemes developed by ENISA and adopted by the Commission. Where required by national or Union legal acts, such **certificates may demonstrate compliance with cybersecurity requirements set out in those acts**. However, this generally applies only where the certification has been carried out by a third-party conformity assessment body (Art. 78(2) CSA 2). This approach is reflected, for example, in Art. 42(2) AI Act and Art. 27(8) of the Cyber Resilience Act. Both provisions already provide that European cybersecurity certificates may give rise to a presumption of conformity with respect to certain cybersecurity requirements laid down in those regulations. The CSA 2 would, however, introduce a practically significant new feature: certification could extend not only to products, services or processes, but also to an entity's entire "cyber posture" (Art. 71(2)(c) in conjunction with Art. 2(29) CSA 2).

3. Expansion of ENISA's Role

In line with the NIS2 Amending Directive, the CSA 2 aims to strengthen the role of ENISA. ENISA will retain its support and advisory functions, but is to receive, in particular, additional financial and personnel resources.

IV. Outlook and Practical Implications

The proposed amendments to the NIS2 Directive and the CSA 2 highlight the growing importance of cybersecurity regulation at the Union level. For companies, the focus on supply chain security is particularly relevant, as existing procurement and contractual structures may need to be reviewed and, where necessary, adapted. This would add to the already demanding obligations under the BSIG and the

Cyber Resilience Act[5] and may further expand the compliance requirements for affected companies. European cybersecurity certification, including at organizational level, is becoming increasingly important as a structured compliance tool.

While the EU legislative process is still ongoing, affected companies should assess potential risks in their ICT supply chains at an early stage, particularly where critical components are sourced from potential high-risk suppliers.

Cybersecurity is also increasingly in focus at national level. In addition to the above-mentioned draft KritisVO, this is reflected in the Federal Government's draft Cybersecurity Act, published in May 2026.[6] The draft is aimed in particular at expanding the supervisory and intervention powers of the Federal Police (Bundespolizei), the Federal Criminal Police Office (BKA), and the BSI with a view to strengthening state cyber-defence capabilities. It provides, inter alia, for additional duties for providers of publicly available telecommunications services and for commercial providers of digital services to cooperate and provide information (Section 15(6) BSIG, as amended; Section 41a(9) Federal Police Act (BPolG), as amended; Section 68c(2) Federal Criminal Police Office Act (BKAG), as amended). Furthermore, the Federal Police and the BKA are to be granted more extensive powers for cyber-defence purposes (Section 41a BPolG, as amended; Sections 68a-f BKAG, as amended).

[5] See also: https://www.sza.de/en/thinktank/cyber-resilience-act-obligations-products-with-digital-elements/

[6] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/cyberabwehr-regierungsentwurf.pdf?__blob=publicationFile&v=2

This client information contains only a non-binding overview of the subject area addressed in it. It does not replace legal advice. Please do not hesitate to contact us for this client information and for advice:

Dr. Thomas Nägele
Rechtsanwalt | Partner
Compliance, Internal Investigations | Privacy and Data Security| Intellectual Property | IT Law | Litigation & Arbitration

T +49 621 4257 222
E Thomas.Naegele@sza.de

Dr. Simon Apel
Rechtsanwalt | Partner
Intellectual Property | Privacy and Data Security

T +49 621 4257 386
E Simon.Apel@sza.de

Alexander Stolz
Rechtsanwalt | Counsel
Commercial | Privacy and Data Security | Intellectual Property | IT Law

T +49 621 4257 222
E Alexander.Stolz@sza.de

Serpil Dilbaz
Rechtsanwältin | Senior Associate
Privacy and Data Security | Intellectual Property | IT Law

T +49 621 4257 222
E Serpil.Dilbaz@sza.de

Hannah Bräunche
Rechtsanwältin | Associate
Intellectual Property | Privacy and Data Security | Commercial

T +49 621 4257 386
E Hannah.Braeunche@sza.de