May 2026

The **Cyber Resilience Act**: far-reaching obligations for products with digital elements

The Cyber Resilience Act (CRA)[1] establishes, for the first time, an EU-wide horizontal regulatory framework for the cybersecurity of products with digital elements. The regulation applies from the design stage and covers the entire lifecycle—from risk assessment during production, through conformity assessment and CE marking prior to placing products on the market, to the reporting of security incidents and the implementation of corrective measures for products already made available on the market.

This creates significant compliance pressure for manufacturers, importers, and distributors. Anyone who places or makes available on the market products with digital elements must align their technical, organizational, and documentation processes with the CRA in a timely manner; this in particular concerns the so-called Software Bill of Materials (SBOM), which requires comprehensive documentation of the software components integrated into the product.

I. Background and purpose

The CRA aims to harmonize cybersecurity requirements for products with digital elements in the European Union. It is intended to raise the security level of connected products and strengthen the single market by establishing a uniform minimum standard for products with digital elements. Unlike sector-specific IT security regimes (e.g., the NIS 2 Directive), the CRA regulates connected products and their cybersecurity requirements throughout the entire lifecycle and does not address business operations as such.

Like the AI Act, the CRA follows the so-called New Legislative Framework. Accordingly, before being placed on the market, products must meet the relevant cybersecurity requirements and documentation obligations, undergo a conformity assessment procedure, and bear the CE marking. If security deficiencies are discovered at a later stage, manufacturers must meet reporting obligations and take

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202402847.

corrective actions. The Commission has published a non-binding draft guideline to support implementation of the CRA, especially for SMEs.[2]

II. Scope of application

The CRA applies to products with **digital elements made available on the Union market** (Art. 2(1) CRA). A product with digital elements is a software or hardware product and its remote data processing solutions. It also includes software or hardware components placed on the market separately, provided they are part of a product with digital elements (Art. 3(1) CRA). The decisive factor is that the intended or reasonably foreseeable use involves a **direct or indirect logical or physical data connection** to a device or network. In practice, this generally includes products that connect via wired or wireless interfaces for data transmission necessary to perform the product's functions.

Practical note: The material scope of the CRA is broad. It covers, in particular:

(i) stand-alone software, apps and computer programs;

(ii) hardware with embedded software, (e.g., IoT devices);

(iii) hardware components such as routers, firewalls, motherboards, or integrated circuits;

(iv) combined hardware and software products where the software is necessary for the product to perform its intended function.

In practice, it is important to distinguish products from services: Software-as-a-Service (SaaS) is not automatically a product within the scope of the CRA but may be classified as such where the SaaS constitutes a remote data processing solution of a product with digital elements—i.e., where the absence of such remote processing would prevent the product from performing one of its functions (Recitals 11, 12 CRA).

Practical note: SaaS may be subject to the requirements of the NIS2 Directive. In Germany, the NIS2-Directive was implemented by the revised German IT Security Act (BSIG).[3]

These obligations apply primarily to the **manufacturer**, i.e., the party that markets the product under its own name or trademark (Art. 3(13) CRA). In addition, there are obligations for **importers** (Art. 3(16) CRA), **distributors** (Art. 3(17) CRA), and – under specific conditions – **open-source software stewards** (OSS stewards) (Art. 3(14) CRA).

III. Obligations

1. Manufacturer obligations

a. Cybersecurity and documentation requirements, Art. 13 CRA in conjunction with Annexes I and II to the CRA

Manufacturers must **design, develop, and produce** products to ensure a level of cybersecurity commensurate to the risks involved. A key requirement is a documented **cybersecurity risk assessment** that is based on the intended purpose and reasonably foreseeable use of the product and must be kept up to date throughout the support period.

In particular, the products must meet the following requirements:

- secure default configuration and protection against unauthorized access;

[2] https://digital-strategy.ec.europa.eu/de/news/commission-publishes-feedback-draft-guidance-assist-companies-applying-cyber-resilience-act

[3] Siehe hierzu die Mandanteninformation zur Umsetzung der NIS2-Richtlinie (unter https://www.sza.de/de/thinktank/cybersicherheit-nis2-richtlinie-deutschland-cyber-resilience-act).

- maintenance of confidentiality, integrity, and availability;
- limitation of attack surfaces and appropriate logging;
- secure deletion and reset functions;
- vulnerability handling and provision of security updates during the support period.

The **support period** must be determined by the manufacturer and must be based on the expected lifetime of the product; it shall generally be at least five years, unless the product is expected to have a shorter lifetime (Art. 13(8) CRA). The disclosure of the support period is part of the mandatory information that must be provided to the user pursuant to Annex II to the CRA.

The **cybersecurity risk assessment** must be included in the technical documentation and made available to the competent market surveillance authorities upon request. The SBOM is of particular importance in this context (Annex I, Part II, No. 1 to the CRA). The **SBOM** is a formal record of the components included in the software elements of a product which also involves software obtained from third parties (Art. 3(39) CRA). It effectively establishes an obligation to document the software supply chain, at least with regard to the components directly integrated into the product. This is likely to involve a significant documentation effort for product manufacturers. The Federal Office for Information Security (BSI) has already issued a technical guideline that providers of products with digital elements can use as a reference in this context.[4]

The harmonized standards, the references to which are published in the Official Journal of the European Union, play a crucial role in fulfilling the obligations under the CRA. If a product meets the requirements of the relevant standards, it is presumed to be in compliance with the essential cybersecurity requirements under Article 27(1) CRA.

b. Conformity assessment (Art. 32 CRA), EU declaration of conformity (Art. 28 CRA) and CE marking (Art. 30 CRA)

Before being placed on the market, the product must undergo a conformity assessment procedure. The product category and the associated risk determine whether internal control is sufficient or whether a notified body must be involved. The classification is based on the function and intended use of the product, as specified in particular in Annexes III and IV to the CRA.

- Non-critical products: internal controls are sufficient;
- Important products classified as Class I under Annex III to the CRA (e.g., password managers, products with VPN functionality, software for detecting, removing, and quarantining malware): internal control is possible provided that all applicable requirements are covered by a relevant harmonized standard, a common specification, or a relevant certification scheme; otherwise, conformity assessment involving a notified body is required;
- Class II products under Annex III to the CRA (e.g., firewalls, intrusion detection systems, and intrusion prevention systems) and critical products under Annex IV to the CRA (smart cards or similar devices): conformity assessment involving a notified body is generally mandatory.

The product's conformity with the requirements of the CRA is documented by the **EU declaration of conformity** (Art. 28 CRA), through which the manufacturer assumes responsibility for the product's conformity. In addition, products must generally bear a CE marking (Art. 30 CRA).

c. Reporting and disclosure requirements

Under Article 14 of the CRA, manufacturers must notify actively exploited vulnerabilities and severe

[4] Abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03183/BSI-TR-03183-2.pdf?__blob=publicationFile&v=3

incidents having an impact on the security of the product with digital elements to the designated Computer Security Incident Response Team (CSIRT) and the European Union Agency for Cybersecurity (ENISA). According to the German draft of the CRA Implementation Act, the role of the CSIRT in Germany is to be carried out by the BSI.

The CRA provides for a tiered reporting system:

- Early warning within 24 hours of becoming aware of the situation;
- Further information within 72 hours;
- Final report within 14 days of the availability of a corrective or risk mitigation measure for actively exploited vulnerabilities, or within one month for severe incidents having an impact on the security of the product with digital elements.

In addition to reporting obligations to the BSI and ENISA, there is also a duty to inform users in the event of actively exploited vulnerabilities and severe incidents having an impact on the security of the product (Art. 14(8) CRA). This includes notifying users of risk mitigation and corrective measures. In addition, upstream providers of software components must also be informed, if necessary, if the respective components contain vulnerabilities (Art. 13(6) CRA).

> **Practical note:** It is crucial for affected companies to establish reporting channels, responsibilities, and approval processes in advance. The short deadlines can only be met if appropriate incident response mechanisms are in place.

2. Obligations of importers, distributors, and OSS stewards

Importers must verify, prior to placing the product on the market, that it meets the requirements of the CRA. This includes, in particular, to ensure that the conformity assessment has been carried out, that the technical documentation has been drawn up, and that a CE marking and an EU declaration of conformity are available (Art. 19(1) CRA). Distributors have similar but less extensive obligations (Art. 20 CRA). If there are indications of non-conformity, importers and distributors may not place or make available products on the market. If they place the product on the market under their own name or brand, they are themselves considered manufacturers (Art. 21 CRA).

The CRA addresses OSS stewards only under strict conditions. An OSS steward is a legal entity that is not itself a manufacturer but provides ongoing support for specific free and open-source software for commercial use and ensures its continued existence (Art. 3 No. 14 CRA). In particular, OSS stewards must develop and document a cybersecurity strategy and cooperate with market surveillance authorities. They are also required to report severe incidents having an impact on the security of the product with digital elements and actively exploited vulnerabilities (Art. 24 CRA).

IV. Enforcement

The CRA is enforced by the market surveillance authorities of the Member States. According to the German draft of the CRA Implementation Act, the BSI is to be designated as the competent market surveillance authority. Market surveillance authorities are granted extensive powers, in particular the power to request information (Art. 53 CRA), to carry out inspections (Art. 60 CRA), and to order corrective actions as well as withdrawal and recall measures (Art. 54(1) CRA). The Regulation is thus conceptualized as a classic product supervision regime with significant supervisory powers of the market surveillance authorities.

Violations may result in substantial fines. The regulation provides that fines of up to EUR 15 million or up to 2.5% of global annual turnover may be imposed (Art. 64(2) CRA). However, this does not apply to OSS stewards, who are not subject to the penalty provisions of Art. 64 CRA (Art. 64(10)(b) CRA). The CRA may also have implications for the standard of care in private relationships. Failure to comply with the CRA may therefore result in liability claims under contract and tort law.

V. Entry into force and application

The CRA entered into force on December 10, 2024, however, its material provisions apply only at a later stage (Art. 71 CRA):

- **June 11, 2026**: Application of the provisions on the notification of conformity assessment bodies;
- **September 11, 2026:** Application of the reporting requirements for actively exploited vulnerabilities and having an impact on the security of the product with digital elements (Art. 14 CRA);
- **December 11, 2027:** Full implementation of the CRA's substantive obligations.

Products placed on the market before December 11, 2027 are subject to the CRA only if they undergo a substantial modification after that date (Art. 69(2) CRA).

VI. Practical implications

For companies that market digital products, there is a high probability that they will be affected by the CRA. In this case, cybersecurity must be considered from the design stage. In particular, the SBOM, i.e. the requirement that the components included in the software of a product can involve significant documentation effort on the part of the manufacturers.

Failure to comply with the CRA can result in substantial fines and civil liability. Given the complex regulatory and technical requirements, we advise affected companies to start implementing appropriate security and reporting measures as soon as possible. We would be happy to assist you in this process.

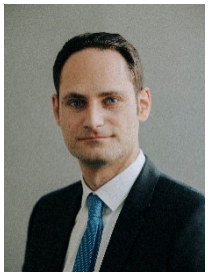
This client information contains only a non-binding overview of the subject area addressed in it. It does not replace legal advice. Please do not hesitate to contact us for this client information and for advice:

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, LL.M. (Dresden / Exeter)
Rechtsanwalt | Counsel
Commercial | Privacy and Data Security | Intellectual Property | IT Law

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

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

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

Serpil Dilbaz, LL.B.
Rechtsanwältin | Associate
Privacy and Data Security | Intellectual Property | IT Law

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