TaylorWessing

# EU Cyber Resilience Act (CRA)

### Purpose

The CRA harmonises cybersecurity requirements for products with digital elements across EU Member States, establishing a conformity assessment process to demonstrate compliance with cybersecurity standards, resulting in CE marking. It details obligations for economic operators in design, development, and production phases to ensure ongoing product cybersecurity, with specific reporting requirements for manufacturers. It also sets out market surveillance rules.

### Scope

Applies to products with digital elements intended for data connections to devices or networks, excluding those covered by certain Union acts. It affects all economic operators – manufacturers, importers, and distributors – who make these products available on the EU market, from design and development through to market placement and the entire period of use, ensuring cybersecurity throughout the product's lifecycle from the Act's entry into force.

### Application

The Cyber Resilience Act (CRA) was published in the Official Journal in November 2024. It will generally apply from 11 December 2027. Article 14 (manufacturer reporting obligations for actively exploited vulnerabilities) will apply from 11 September 2026, and Chapter IV (conformity assessment bodies) will apply from 11 June 2026. Products placed on the market before 11 December 2027 are only subject to the regulation if substantially modified, except for Article 14, which applies to all such products.

### Definition of products with digital elements

The CRA defines **products with digital elements** as any software or hardware product, including their remote data processing solutions and components sold separately. It applies to products intended to be or foreseeably used with a direct or indirect data connection to a device or network. This includes connected devices (consumer and industrial IoT), operating systems, and high-risk AI systems. Exclusions are sector-specific regulated devices, SaaS unless integral to the product, and free non-profit open source software to support innovation and research.

### Essential requirements

The CRA outlines essential requirements for products with digital elements to ensure cybersecurity. These products must be designed, developed, and produced to achieve an appropriate level of cybersecurity, addressing risks identified in cybersecurity assessments. Key requirements include ensuring products are free of known exploitable vulnerabilities, offering secure default configurations, enabling timely security updates (with user-friendly opt-out options), and protecting data confidentiality, integrity, and availability.

Manufacturers must implement controls against unauthorised access, minimise data collection to what is necessary, and ensure resilience against attacks. They should also provide mechanisms for users to securely remove data and settings, and maintain a policy for coordinated vulnerability disclosure. Furthermore, manufacturers are required to regularly test product security, address and remediate vulnerabilities promptly, and ensure security updates are provided separately from functionality updates. Compliance with these requirements, including the ability to handle vulnerabilities effectively, is crucial in the procurement process, particularly for national security and defence purposes, without conflicting with existing Union law obligations.

### Obligations of manufacturers

Under Article 13, manufacturers of products with digital elements must ensure these products meet the essential cybersecurity requirements. This involves conducting a thorough cybersecurity risk assessment during all phases of the product lifecycle, documenting and updating it as needed, and integrating third-party components, including open source software, with due diligence to avoid compromising cybersecurity. Manufacturers must report vulnerabilities in components, including open source ones, and address them promptly, sharing fixes with the original developers. They must document cybersecurity aspects systematically, determine a support period reflecting the product's expected use, and ensure security updates are available for at least 10 years after the product is marketed or for the entire support period, whichever is longer. Additionally, these products must undergo conformity assessment procedures to demonstrate compliance with the essential cybersecurity requirements. Products must bear identifying information, and manufacturers must provide contact details and user instructions, maintain a single point of contact for users, and ensure the product's technical documentation and EU declaration of conformity are accessible to market surveillance authorities for at least 10 years. They must also provide a copy of the EU declaration of conformity (or a simplified version) with the product, facilitate user communication, and take corrective measures if non-conformities are found. For free and open source software, the CRA allows additional cybersecurity requirements for procurement or use for national security or defence purposes, provided these are necessary, proportionate, and consistent with Union law. The CRA supports innovation by excluding not-for-profit open-source software from its scope.

### Important and critical products with digital elements

Article 7 defines important products with digital elements, which fall into two classes (Class I and II) as listed in Annex III. These include identity management systems, browsers, password managers, VPNs, operating systems, routers, and smart home devices. Products are deemed important if they perform functions critical to the cybersecurity of other products, networks, or services (e.g., authentication, access control), or pose a significant risk of adverse effects on a large number of other products or user safety through direct manipulation (e.g. network management).

Article 8 specifies critical products with digital elements, listed in Annex IV, requiring a European cybersecurity certificate with at least a "substantial" assurance level. These include hardware devices with security boxes, smart meter gateways, and smartcards. Critical products are determined based on their critical dependency by essential entities (as per Directive (EU) 2022/2555), the potential for incidents and vulnerabilities to cause serious disruptions to critical supply chains. The Commission can update the lists and criteria for important and critical products through delegated acts, considering cybersecurity risks and market impacts.

### Open source software

The CRA distinguishes between commercial and non-commercial activities regarding free and open source software (FOSS). FOSS is defined as software with openly shared source code, accessible, usable, modifiable, and redistributable under a free license. Only FOSS made available on the market for commercial activities falls within the CRA's scope. Development funding or the nature of development (commercial or non-commercial) is not considered when determining this. Products incorporating FOSS components are deemed commercial only if the component is monetised by its original manufacturer. Support activities, such as regular updates or financial assistance, do not by themselves constitute commercial activity. Non-profit organisations developing FOSS and not monetising it are excluded from commercial classification. Open source software stewards, who provide sustained support for FOSS intended for commercial use, are subject to specific obligations under a light-touch regulatory regime. This includes cybersecurity policies and cooperation with market surveillance authorities to mitigate risks. They cannot affix CE markings to the products they support. Hosting FOSS on repositories does not constitute making it available on the market unless it is distributed commercially. To aid manufacturers using non-commercial FOSS, the Commission may establish voluntary security attestation programs or European cybersecurity certification schemes. The CRA aims to balance cybersecurity needs while supporting FOSS development, ensuring that non-commercial open-source software remains free from stringent regulatory burdens.

### Enforcement and penalties

Fines of up to:

- EUR 15,000,000 or 2.5 % of annual turnover (whichever is higher) for failing to meet cybersecurity requirements
- EUR 10,000,000 or 2 % of annual turnover (whichever is higher) for other regulatory breaches
- EUR 5,000,000 or 1 % of annual turnover (whichever is higher) for providing inaccurate information to authorities