Cyber Resilience Act

From baby-monitors to smart-watches, products and software that contain a digital component are omnipresent in our daily lives. Less apparent to many users is the security risk such products and software may present.

The Cyber Resilience Act (CRA) (https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act) aims to safeguard consumers and businesses buying software or hardware products with a digital component. The Cyber Resilience Act addresses the inadequate level of cybersecurity in many products, and the lack of timely security updates for products and software. It also tackles the challenges consumers and businesses currently face when trying to determining which products are cybersecure and in setting them up securely. The new requirements will make it easier to take cybersecurity into account when selecting and using products that contain digital elements. It will be more straightforward to identify hardware and software products with the proper cybersecurity features.

The Cyber Resilience Act introduces mandatory cybersecurity requirements for manufacturers and retailers, governing the planning, design, development, and maintenance of such products. These obligations must be met at every stage of the value chain. The act also requires manufacturers to provide care during the lifecycle of their products. Some critical products of particular relevance for cybersecurity will also need to undergo a third-party assessment by an authorised body before they are sold in the EU market.

The regulation applies to all products connected directly or indirectly to another device or network except for specified exclusions such as certain open-source software or services products that are already covered by existing rules, which is the case for medical devices, aviation and cars. Products will bear the **CE marking** (https://single-market-economy.ec.europa.eu/single-market/ce-marking_en) to indicate that they comply with the CRA requirements. The new rules will rebalance responsibility towards manufacturers, who must ensure their products with digital elements meet cybersecurity standards for the EU market. This will allow buyers to make more informed decisions, trusting the cybersecurity of CE-marked products.

The Cyber Resilience Act entered into force on 10 December 2024. The main obligations introduced by the Act will apply from 11 December 2027.

Additionally, the Cyber Resilience Act Expert Group (CRA Expert Group) (https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3967) is being set up. The expert group will assist and advise the Commission on issues relevant to the implementation of the Cyber Resilience Act (CRA).

The Cyber Resilience Act builds on the 2020 EU Cybersecurity Strategy (https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy) and EU Security Union Strategy (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020DC0605&from=EN). It complements other legislation in this area, specifically the NIS2 Directive (https://digital-strategy.ec.europa.eu/en/policies/nis-directive).
