

Cyber Resilience Act

Introducing the Cyber Resilience Act: the EU's new plan to make sure all digital products are safe from cyber threats. This important rulebook requires that devices and software are designed, updated, and maintained to protect users in our increasingly digital world. Experience a safer, more connected future where your security comes first.

From baby-monitors to smart watches, from apps to computer programs, connectable hardware and software are omnipresent in our daily lives. Less apparent to many users is the security risk such products 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 digital elements. The CRA addresses the inadequate level of cybersecurity in many products, and the lack of timely security updates. It also tackles the challenges consumers and businesses currently face when trying to determine which products are cybersecure and in setting them up securely, making it easier to identify hardware and software with the proper cybersecurity features.

The CRA introduces mandatory cybersecurity requirements for manufacturers, covering the planning, design, development and maintenance of such products. These obligations must be met at every stage of the value chain. The CRA also requires manufacturers to handle vulnerabilities during the lifecycle of their products. Some products of particular relevance for cybersecurity may need to undergo a third-party assessment by a notified body before they are sold on the EU market.

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 and national market surveillance authorities will ensure enforcement of the rules.

The CRA entered into force on 10 December 2024. The main obligations introduced by the Act will apply from 11 December 2027, with reporting obligations to apply as of 11 September 2026.

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:52020DC0605&from=EN>).

It complements other legislation in this area, specifically the [NIS2 Directive](#)

<https://digital-strategy.ec.europa.eu/en/policies/nis-directive>).

[Find out more about the implementation of the Cyber Resilience Act.](#)

<https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation>

Source URL: <https://digital-strategy.ec.europa.eu/policies/cyber-resilience-act>

© European Union, 2026 - [Shaping Europe's digital future](https://digital-strategy.ec.europa.eu/en)
(<https://digital-strategy.ec.europa.eu/en>) - PDF generated on 25/06/2026

Reuse of this document is allowed, provided appropriate credit is given and any changes are indicated (Creative Commons Attribution 4.0 International license).

For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

Source URL: <https://digital-strategy.ec.europa.eu/policies/cyber-resilience-act>