EU Cyber Resilience Act

New EU cybersecurity rules ensure safer hardware and software.

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 Commission's proposal for a new Cyber Resilience Act (CRA) aims to safeguard consumers and businesses buying or using products or software with a digital component. The Act would see inadequate security features become a thing of the past with the introduction of mandatory cybersecurity requirements for manufacturers and retailers of such products, with this protection extending throughout the product lifecycle.

The problem addressed by the proposed regulation is two-fold. First is the inadequate level of cybersecurity inherent in many products, or inadequate security updates to such products and software. Second is the inability of consumers and businesses to currently determine which products are cybersecure, or to set them up in a way that ensures their cybersecurity is protected.

The proposed Cyber Resilience Act would guarantee:

- harmonised rules when bringing to market products or software with a digital component;
- a framework of cybersecurity requirements governing the planning, design, development and maintenance of such products, with obligations to be met at every stage of the value chain;
- an obligation to provide duty of care for the entire lifecycle of such products.

When the proposed regulation enters into force, software and products connected to the internet

would bear the CE marking to indicate they comply with the new standards. Requiring manufacturers and retailers to prioritise cybersecurity, customers and businesses would be empowered to make better-informed choices, confident of the cybersecurity credentials of CE-marked products.

The proposed regulation announced in the 2020 EU Cybersecurity Strategy, would complement existing legislation, specifically the NIS2 Framework. It would apply to all products connected directly or indirectly to another device or network except for specified exclusions such as open-source software or services that are already covered by existing rules, which is the case for medical devices, aviation and cars.

The European Parliament and the Council will now deliberate on the proposed Cyber Resilience Act. Upon entry into force, stakeholders will have 24 months in which to adapt to new requirements, with the exception of a more limited 12-month grace period in relation to the reporting obligation on manufacturers.

Proposed Regulation - Cyber Resilience Act

Factsheet - Cyber Resilience Act

Impact Assessment - Cyber Resilience Act

Follow the latest progress and learn more about getting involved.

- Follow the Commission's work on cybersecurity @CyberSec_EU

Related Content

Big Picture

Cybersecurity Policies

The European Union works on various fronts to promote cyber resilience, safeguarding our communication and data and keeping online society and economy secure.

See Also

European Cybersecurity Competence Network and Centre

The European Cybersecurity Network and Cybersecurity Competence Centre help the EU retain and develop cybersecurity technological and industrial capacities.

Stakeholder Cybersecurity Certification Group

The Stakeholder Cybersecurity Certification Group was established to provide advice on strategic issues regarding cybersecurity certification.

The EU Cybersecurity Act

The Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.

The EU cybersecurity certification framework

The EU cybersecurity certification framework for ICT products enables the creation of tailored and risk-based EU certification schemes.

NIS Directive

The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.
