Council of the EU

PRESS
EN

PRESS RELEASE
752/24
10/10/2024

Cyber resilience act: Council adopts new law on security requirements for digital products

The Council adopted today a new law on cybersecurity requirements for products with digital elements with a view to ensuring that products, such as connected home cameras, fridges, TVs, and toys, are safe before they are placed on the market (**cyber resilience act**). The new regulation aims to fill the gaps, clarify the links, and make the existing cybersecurity legislative framework more coherent, ensuring that products with digital components, for example **'Internet of Things'** (IoT) products, are made secure throughout the supply chain and throughout their lifecycle.

Key elements of the new regulation

The new law introduces EU-wide **cybersecurity requirements** for the design, development, production and making available on the market of hardware and software products, to avoid overlapping requirements stemming from different pieces of legislation in EU member states. For example, software and hardware products will bear the **CE marking** to indicate that they comply with the regulation's requirements. The letters 'CE' appear on many products traded on the extended single market in the European Economic Area (EEA). They signify that products sold in the EEA have been assessed to meet high safety, health, and environmental protection requirements.

The regulation will apply to all products that are **connected** either directly or indirectly to another device or to a network. There are some exceptions for products for which cybersecurity requirements are already set out in existing EU rules, for example medical devices, aeronautical products, and cars.

Finally, the new law will allow consumers to take cybersecurity into account when **selecting and using** products that contain digital elements, making it easier for them to identify hardware and software products with the proper cybersecurity features.

Next steps

Following today's adoption, the legislative act will be signed by the presidents of the Council and of the European Parliament and published in the EU's official journal in the coming weeks. The new regulation will enter into force twenty days after this publication and will apply 36 months after its entry into force with some provisions to apply at an earlier stage.

Background

First announced by Commission President von der Leyen in her State of the Union address in September 2021, the cyber resilience act was mentioned in the Council conclusions of 23 May 2022 on the development of the European Union's cyber posture, which called upon the Commission to submit its proposal by the end of 2022.

On 15 September 2022, the Commission submitted the proposal for a cyber resilience act, which will complement the existing EU cybersecurity framework: the directive on the security of network and information systems (NIS directive), the directive on measures for a high level of cybersecurity across the Union (NIS 2 directive) and the EU cybersecurity act. Following interinstitutional negotiations ('trilogues'), a provisional agreement was reached between the co-legislators on 30 November 2023.

- Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber resilience act), 10 October 2024
- Cyber resilience act, Council's negotiating mandate, 19 July 2023
- Regulation on horizontal cybersecurity requirements for products with digital elements (cyber resilience act), Commission proposal, 15 September 2022
- Your life online: How the EU is making it easier and safer for you (feature story)

Press office - General Secretariat of the Council of the EU
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press