Cyber Resilience Act

2022/0272(COD) - 20/11/2024 - Final act

PURPOSE: to lay down a horizontal Union regulatory framework establishing comprehensive cybersecurity requirements for all products with digital elements.

LEGISLATIVE ACT: Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

CONTENT: the regulation establishes:

- rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products;

- essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;

- essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;

- rules on market surveillance and enforcement of the above-mentioned rules and requirements.

Scope

The regulation will apply to all products that are **connected either directly or indirectly to another device or to a network**. Consumer products with digital elements categorised as important products with digital elements present a higher cybersecurity risk by performing a function which carries a significant risk of adverse effects in terms of its intensity and ability to damage the health, security or safety of users of such products, and should undergo a stricter conformity assessment procedure.

This includes, in particular: (i) identity management systems and privileged access management software and hardware, including authentication and access control readers and biometric readers; (ii) password managers; (iii) software that searches for, removes or quarantines malicious software; (iv) products with digital elements with virtual private network (VPN) functions; (v) routers, modems for connecting to the internet; (vi) smart home general purpose virtual assistants; (vii) smart home products with security features, including smart door locks, security cameras, baby monitors and alarm systems; (viii) connected toys; or (ix) personal wearable products. Exceptions are provided for products for which cybersecurity requirements are already set out in existing EU rules, such as medical devices, aeronautical products and cars.

Stakeholder consultation

When preparing measures for the implementation of this regulation, the Commission will consult and take into account the views of relevant stakeholders, such as relevant Member State authorities, private sector undertakings, including microenterprises and small and medium-sized enterprises, the open-source software community, consumer associations, academia, and relevant Union agencies and bodies as well as expert groups established at Union level.

Essential requirements

Manufacturers will ensure that all products with digital elements are designed and developed in accordance with the essential cybersecurity requirements set out in the Regulation. They will also carry out a **cybersecurity risk assessment** of a product with digital elements and take the results of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements, with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including on the health and safety of users.

The cybersecurity risk assessment will be documented and updated during a **support period**. When placing a product with digital elements on the market, the manufacturer will ensure that vulnerabilities in that product are managed effectively and in accordance with the essential requirements. When identifying a vulnerability in a component, including an open-source software component, that is integrated into the product with digital elements, the manufacturer will report the vulnerability to the person or entity that maintains the component, and address and remediate the vulnerability.

Manufacturers will: (i) systematically document, in a manner that is proportionate to the nature and the cybersecurity risks; (ii) ensure that each security update, which has been made available to users during the support period, remains available after it has been issued for a minimum of 10 years after the product with digital elements has been placed on the market or for the remainder of the support period; (iii) set up a single point of contact that enables users to communicate easily with them, including for the purpose of reporting on and receiving information about the vulnerabilities of the product with digital element; (iv) ensure that products with digital elements are accompanied by the information and instructions for the user.

Reporting obligations of manufacturers

A manufacturer will notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator and to ENISA.

The manufacturer will also submit: (i) an **early warning** notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available; (ii) a **vulnerability notification**, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability. To simplify the reporting obligations of manufacturers, a single reporting platform will be established by ENISA.

For example, software and hardware products will bear the **CE marking** to indicate that they comply with the regulation's requirements. The CE marking must be affixed in a visible, legible and indelible manner to the product containing digital elements.

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.

ENTRY INTO FORCE: 10.12.2024.

APPLICATION: from 11.12.2027.