Cyber Resilience Act

2022/0272(COD) - 15/09/2022 - Legislative proposal

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

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of EUR 5.5 trillion by 2021. Such products suffer from two major problems adding costs for users and the society: (i) a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and (ii) an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner. In a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply chain, often propagating across the borders of the internal market within a matter of minutes. This can lead to severe disruption of economic and social activities or even become life threatening.

While the existing Union legislation applies to certain products with digital elements, there is no horizontal Union regulatory framework establishing comprehensive cybersecurity requirements for all products with digital elements. It is therefore necessary to lay down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market.

CONTENT: with this proposal, the Commission seeks to lay down horizontal cybersecurity rules which are not specific to sectors or certain products with digital elements.

Subject matter

Based on the new legislative framework for product legislation in the EU, the proposal 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 draft Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network. It will not apply to products for which cybersecurity requirements are already set out in existing EU rules, for example on medical devices, aviation or cars.

Objectives

It has two main objectives aiming to ensure the proper functioning of the internal market:

- create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufactures take security seriously throughout a products life cycle;

- create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

Obligations for manufacturers, importers and distributors

Obligations would be set up for economic operators, starting from manufacturers, up to distributors and importers, in relation to the placement on the market of products with digital elements, as adequate for their role and responsibilities on the supply chain.

The essential cybersecurity requirements and obligations mandate that all products with digital elements shall only be made available on the market if, where dully supplied, properly installed, maintained and used for their intended purpose or under conditions, which can be reasonably foreseen, they meet the essential cybersecurity requirements set out in this draft Regulation.

The essential requirements and obligations would mandate manufacturers to factor in cybersecurity in the design and development and production of the products with digital elements, exercise due diligence on security aspects when designing and developing their products, be transparent on cybersecurity aspects that need to be made known to customers, ensure security support (updates) in a proportionate way, and comply with vulnerability handling requirements.

Notification of conformity assessment bodies

Proper functioning of notified bodies is crucial for ensuring a high level of cybersecurity and for the confidence of all interested parties. Therefore, the proposal sets out requirements for national authorities responsible for conformity assessment bodies (notified bodies). Member States will designate a notifying authority that will be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies.

Conformity assessment process

Manufacturers should undergo a process of conformity assessment to demonstrate whether the specified requirements relating to a product have been fulfilled. Where compliance of the product with the applicable requirements has been demonstrated, manufacturers and developers would draw up an EU declaration of conformity and will be able to affix the CE marking.

Market surveillance

Member States should appoint market surveillance authorities, which would be responsible for enforcing the Cyber Resilience Act obligations.

In case of non-compliance, market surveillance authorities could require operators to bring the non-compliance to an end and eliminate the risk, to prohibit or restrict the making available of a product on the market, or to order that the product is withdrawn or recalled. Each of these authorities will be able to fine companies that don't adhere to the rules.

Application

To allow manufacturers, notified bodies and Member States time to adapt to the new requirements, the proposed Regulation will become applicable 24 months after its entry into force, except for the reporting obligation on manufacturers, which would apply from 12 months after the date of entry into force.