Cyber Resilience Act

2022/0272(COD) - 12/03/2024 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 517 votes to 12, with 78 abstentions, legislative resolution on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

This Regulation applies to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amends the proposal as follows:

Important products with digital elements (Annex III)

Certain categories of products with digital elements should be subject to **stricter conformity assessment procedures**. Consumer products with digital elements categorised in this Regulation 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 applies to smart home products with security functionalities, such as smart door locks, baby monitoring systems and alarm systems, connected toys and personal wearable health technology.

The Commission is empowered to adopt delegated acts to **amend Annex III** of the Regulation by including in the list a new category within each class of the categories of products with digital elements and specifying its definition, moving a category of products from one class to the other or withdrawing an existing category from that list.

Critical products with digital elements (Annex IV)

The categories of products with digital elements referred to in the Regulation have a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products or to the health, security or safety of its users through direct manipulation.

The Commission is empowered to adopt delegated acts to supplement this Regulation to determine which products with digital elements that have the core functionality of a product category that is set out in Annex IV to this Regulation are to be required to obtain a **European cybersecurity certificate** at assurance level at least ‘substantial’ under a European cybersecurity certification scheme, to demonstrate conformity with the essential requirements set out in Annex I to this Regulation or parts thereof, provided that a European cybersecurity certification scheme covering those categories of products with digital elements has been adopted and is available to manufacturers.

Stakeholder consultation

When preparing measures for the implementation of this Regulation, the Commission should 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.

In order to respond to the needs of professionals, Member States with, where appropriate, the support of the Commission, the European Cybersecurity Competence Centre and ENISA, while fully respecting the responsibility of the Member States in the education field, should promote measures and strategies aiming to **develop cybersecurity skills** and create organisational and technological tools to ensure sufficient availability of skilled professionals in order to support the activities of the market surveillance authorities and conformity assessment bodies.

Obligations of manufacturers

Manufacturers should undertake an assessment of the cybersecurity risks associated with a product with digital elements. The cybersecurity risk assessment should be documented and updated as appropriate during a **support period**.

From the placing on the market and for the support period, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements should immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.

Manufacturers should, upon identifying a vulnerability in a component, including in an open source-component, which is integrated in the product with digital elements **report the vulnerability** to the person or entity manufacturing or maintaining the component, and address and remediate the vulnerability.

Manufacturers should:

- **determine the support period** so that it reflects the length of time during which the product is expected to be in use, taking into account, in particular, reasonable user expectations, the nature of the product, including its intended purpose, as well as relevant Union law determining the lifetime of products with digital elements;

- 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;

- 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.

Reporting obligations of manufacturers

A manufacturer should 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 should 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. A manufacturer should notify any severe incident having an impact on the security of the product with digital elements.

Manufacturers as well as other natural or legal persons may notify any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements on a **voluntary basis** to a CSIRT designated as coordinator or ENISA. In order to simplify the reporting obligations of manufacturers, a **single reporting platform** should be established by ENISA.