Cyber Resilience Act

2022/0272(COD) - 27/07/2023 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Industry, Research and Energy adopted the report by Nicola DANTI (Renew, IT) 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.

The committee responsible recommended that the European Parliament's position adopted at first reading under the ordinary legislative procedure should amend the proposal as follows:

Security updates

The amended text stated that manufacturers should ensure, where technically feasible, that products with digital elements clearly differentiate between security and functionality updates. Security updates, designed to decrease the level of risk or to remedy potential vulnerabilities, should be installed **automatically**, in particular in the case of consumer products.

Enhancing skills in a cyber resilient digital environment

Members stressed the importance of professional skills in the cybersecurity field, proposing education and **training** programmes, collaboration initiatives, and strategies for enhancing workforce mobility.

Point of single contact for users

In order to facilitate reporting on the **security of products**, manufacturers should designate a point of single contact to enable users to communicate directly and rapidly with them, where applicable by electronic means and in a user-friendly manner, including by allowing users of the product to choose the means of communication, which should not solely rely on automated tools.

Manufacturers should make public the information necessary for the end users to easily identify and communicate with their points of single contact.

Guidelines

The amended text included provisions for the Commission to issue guidelines to create clarity, certainty for, and consistency among the practices of economic operators. The Commission should focus on how to facilitate compliance by microenterprises, small enterprises and medium-sized enterprises.

Conformity assessment procedures for products with digital elements

Harmonised standards, common specifications or European cybersecurity certification schemes should be in place for six months before the conformity assessment procedure applies.

Mutual recognition agreements (MRAs)

To promote international trade, the Commission should endeavour to conclude Mutual Recognition Agreements (MRAs) with third countries. The Union should establish MRAs only with third countries that are on a comparable level of technical development and have a

compatible approach concerning conformity assessment. The MRAs should ensure the same level of protection as that provided for by this Regulation.

Procedure at EU level concerning products with digital elements presenting a significant cybersecurity risk

Where the Commission has sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk in light of non-technical risk factors, Members considered that it should inform the relevant market surveillance authorities and issue targeted recommendations to economic operators aimed at ensuring that appropriate corrective actions are put in place.

Revenues generated from penalties

The revenues generated from the payments of penalties should be used to strengthen the level of cybersecurity within the Union, including by developing capacity and skills related to cybersecurity, improving economic operators' cyber resilience, in particular of microenterprises and of small and medium-sized enterprises and more in general fostering public awareness of cyber security issues.

Evaluation and review

Every year when presenting the Draft Budget for the following year, the Commission should submit a detailed assessment of ENISA's tasks under this Regulation as set out in Annex VIa and other relevant Union law and shall detail the financial and human resources needed to fulfil those tasks.