Procedure file

Basic information

COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	2022/0272(COD)
Awaiting Council's 1st reading position	

Cyber Resilience Act

Amending Regulation 2019/1020 2017/0353(COD)

Subject
2.10.03 Standardisation, EC/EU standards and trade mark, certification, compliance
3.30.06 Information and communication technologies, digital technologies
3.30.07 Cybersecurity, cyberspace policy
3.30.25 International information networks and society, internet
4.60.08 Safety of products and services, product liability
6.20.02 Export/import control, trade defence, trade barriers

Legislative priorities
Joint Declaration 2022
Joint Declaration 2023-24

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
ITRE Industry, Research and Energy		26/10/2022
	renew europe. DANTI Nicola	
	Shadow rapporteur	
	epp VIRKKUNEN Henna	
	S&D COVASSI Beatrice	
	CORRAO Ignazio	
	GAZZINI Matteo	
	ECR TOŠENOVSKÝ Evžen	
	BOTENGA Marc	

Committee for opinion	Rapporteur for opinion	Appointed
IMCO Internal Market and Consumer Protection (Associated committee)		16/12/2022
	renew europe. LØKKEGAARD Morten	
LIBE Civil Liberties, Justice and Home Affairs (Associated committee)	The committee decided not to give an opinion.	

Council of the European Union European Commission	Commission DG	Commissioner
	Communications Networks, Content and Technology	BRETON Thierry
European Economic and Social Committee		

Key events

15/09/2022	Legislative proposal published	COM(2022)0454	Summary
09/11/2022	Committee referral announced in Parliament, 1st reading		
20/04/2023	Referral to associated committees announced in Parliament		
19/07/2023	Vote in committee, 1st reading		
19/07/2023	Committee decision to open interinstitutional negotiations with report adopted in committee		
27/07/2023	Committee report tabled for plenary, 1st reading	A9-0253/2023	Summary
11/09/2023	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 71)		
13/09/2023	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 71)		
23/01/2024	Approval in committee of the text agreed at 1st reading interinstitutional negotiations	PE758.004 GEDA/A/(2024)000218	
11/03/2024	Debate in Parliament		
12/03/2024	Decision by Parliament, 1st reading	T9-0130/2024	Summary

Technical information

Procedure reference	2022/0272(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
	Amending Regulation 2019/1020 2017/0353(COD)
Legal basis	Treaty on the Functioning of the EU TFEU 114; Rules of Procedure EP 57
Other legal basis	Rules of Procedure EP 159
Mandatory consultation of other institutions	European Economic and Social Committee
Stage reached in procedure	Awaiting Council's 1st reading position
Committee dossier	ITRE/9/10122

Documentation gateway

Legislative proposal		COM(2022)0454	15/09/2022	EC	Summary

Document attached to the procedure		SEC(2022)0321	15/09/2022	EC	
Document attached to the procedure		SWD(2022)0282	15/09/2022	EC	
Document attached to the procedure		SWD(2022)0283	15/09/2022	EC	
Document attached to the procedure		N9-0088/2022 OJ C 452 29.11.2022, p. 0023	09/11/2022	EDPS	
Economic and Social Committee: opinion, report		CES4103/2022	14/12/2022	ESC	
Committee draft report		PE745.538	31/03/2023	EP	
Amendments tabled in committee		PE746.920	03/05/2023	EP	
Amendments tabled in committee		PE746.921	03/05/2023	EP	
Committee opinion	IMCO	PE742.490	30/06/2023	EP	
Committee report tabled for plenary, 1st reading/single reading		A9-0253/2023	27/07/2023	EP	Summary
Coreper letter confirming interinstitutional agreement		GEDA/A/(2024)000218	20/12/2023	CSL	
Text agreed during interinstitutional negotiations		PE758.004	20/12/2023	EP	
Text adopted by Parliament, 1st reading/single reading		T9-0130/2024	12/03/2024	EP	Summary

Cyber Resilience Act

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.

Cyber Resilience Act

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.

Cyber Resilience Act

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 manufacturers 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.

Transparency

KOLAJA Marcel	Shadow rapporteur for opinion	IMCO	30/11/2023	Eclipse Foundation AISBL Linux Foundation Europe Red Hat Limited the Mozilla Foundation
KOLAJA Marcel	Shadow rapporteur for opinion	IMCO	16/11/2023	Red Hat Limited
DANTI Nicola	Rapporteur	ITRE	16/11/2023	APCO Worldwide
DANTI Nicola	Rapporteur	ITRE	10/11/2023	OpenForum Europe AISBL
DANTI Nicola	Rapporteur	ITRE	09/11/2023	American Chamber of Commerce in Belgium CNH Industrial ChargePoint Network (Netherlands) BV IBM Corporation Microsoft Corporation Oracle Workday
COVASSI Beatrice	Shadow rapporteur	ITRE	06/11/2023	Apple Inc.
DANTI Nicola	Rapporteur	ITRE	03/11/2023	DIGITALEUROPE Samsung Electronics Europe

				Schneider Electric Siemens AG
DANTI Nicola	Rapporteur	ITRE	03/11/2023	GitHub, Inc.
DANTI Nicola	Rapporteur	ITRE	26/10/2023	NLnet Labs
COVASSI Beatrice	Shadow rapporteur	ITRE	25/10/2023	European Internet Forum
MELCHIOR Karen	Member	20/02/2024	Match Group	
MELCHIOR Karen	Member	15/02/2024	Apple Inc.	
FUGLSANG Niels	Member	22/06/2023	Confederation of Danish Industry	
REPASI René	Member	26/04/2023	Verbraucherzentrale Bundesverband	
KALJURAND Marina	Member	09/02/2023	Cybersecurity Coalition	