Basic information

2022/0272(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Procedure completed
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	DANTI Nicola (Renew)	26/10/2022
	Shadow rapporteur VIRKKUNEN Henna (EPP) COVASSI Beatrice (S&D) CORRAO Ignazio (Greens/EFA) TOŠENOVSKÝ Evžen (ECR) GAZZINI Matteo (ID) BOTENGA Marc (The Left)	

Committee for opinion	Rapporteur for opinion	Appointed
IMCO Internal Market and Consumer Protection (Associated committee)	LØKKEGAARD Morten (Renew)	16/12/2022
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

Date	Event	Reference	Summary
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 72)		
13/09/2023	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 72)		
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
12/03/2024	Results of vote in Parliament		
10/10/2024	Act adopted by Council after Parliament's 1st reading		
23/10/2024	Final act signed		
20/11/2024	Final act published in Official Journal		

Technical information

Procedure reference	2022/0272(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
Amendments and repeals	Amending Regulation 2019/1020 2017/0353(COD)
Legal basis	Rules of Procedure EP 57_o Treaty on the Functioning of the European Union TFEU 114
Other legal basis	Rules of Procedure EP 165

Mandatory consultation of other institutions	European Economic and Social Committee
Stage reached in procedure	Procedure completed
Committee dossier	ITRE/9/10122

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE745.538	31/03/2023	
Amendments tabled in committee		PE746.920	03/05/2023	
Amendments tabled in committee		PE746.921	03/05/2023	
Committee opinion	IMCO	PE742.490	30/06/2023	
Committee report tabled for plenary, 1st reading/single reading		A9-0253/2023	27/07/2023	Summary
Text agreed during interinstitutional negotiations		PE758.004	20/12/2023	
Text adopted by Parliament, 1st reading/single reading		T9-0130/2024	12/03/2024	Summary

Council of the EU

Document type	Reference	Date	Summary
Coreper letter confirming interinstitutional agreement	GEDA/A/(2024)000218	20/12/2023	
Draft final act	00100/2023/LEX	23/10/2024	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2022)0454	15/09/2022	Summary
Document attached to the procedure	SEC(2022)0321	15/09/2022	
Document attached to the procedure	SWD(2022)0282	15/09/2022	
Document attached to the procedure	SWD(2022)0283	15/09/2022	
Commission response to text adopted in plenary	SP(2024)350	22/07/2024	

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	CZ_CHAMBER	COM(2022)0454	14/11/2022	
Contribution	BG_PARLIAMENT	COM(2022)0454	19/12/2022	
Contribution	PT_PARLIAMENT	COM(2022)0454	21/12/2022	

Contribution	NL_SENATE	COM(2022)0454	23/05/2023	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
EDPS	Document attached to the procedure	N9-0088/2022 OJ C 452 29.11.2022, p. 0023	09/11/2022	
EESC	Economic and Social Committee: opinion, report	CES4103/2022	14/12/2022	

Additional information

Source	Document	Date
EP Research Service	Briefing	20/12/2024
European Commission	EUR-Lex	

Meetings with interest representatives published in line with the Rules of Procedure

Rapporteurs, Shadow Rapporteurs and Committee Chairs

Transparency

Name	Role	Committee	Date	Interest representatives
KOLAJA Marcel	Shadow rapporteur for opinion	IMCO	30/11/2023	Eclipse Foundation AISBL Linux Foundation Europe Red Hat Limited the Mozilla Foundation
DANTI Nicola	Rapporteur	ITRE	16/11/2023	APCO Worldwide
KOLAJA Marcel	Shadow rapporteur for opinion	IMCO	16/11/2023	Red Hat Limited
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	GitHub, Inc.
DANTI Nicola	Rapporteur	ITRE	03/11/2023	DIGITALEUROPE Samsung Electronics Europe Schneider Electric Siemens AG

DANTI Nicola	Rapporteur	ITRE	26/10/2023	NLnet Labs
COVASSI Beatrice	Shadow rapporteur	ITRE	25/10/2023	European Internet Forum
DANTI Nicola	Rapporteur	ITRE	25/10/2023	Confederazione Generale dell'Industria Italiana
DANTI Nicola	Rapporteur	ITRE	20/10/2023	Samsung Electronics Europe
DANTI Nicola	Rapporteur	ITRE	18/10/2023	European Telecommunications Network Operators' Association
DANTI Nicola	Rapporteur	ITRE	12/10/2023	Eclipse Foundation AISBL
COVASSI Beatrice	Shadow rapporteur	ITRE	18/07/2023	ENISA
DANTI Nicola	Rapporteur	ITRE	26/06/2023	Google
VIRKKUNEN Henna	Shadow rapporteur	ITRE	13/06/2023	British Chamber of Commerce | EU & Belgium
COVASSI Beatrice	Shadow rapporteur	ITRE	12/05/2023	I-COM
COVASSI Beatrice	Shadow rapporteur	ITRE	05/05/2023	PAGOPA
KOLAJA Marcel	Shadow rapporteur for opinion	IMCO	04/05/2023	DEKRA e.V.
KOKALARI Arba	Shadow rapporteur for opinion	IMCO	03/05/2023	Google
DANTI Nicola	Rapporteur	ITRE	26/04/2023	BUSINESSEUROPE
DANTI Nicola	Rapporteur	ITRE	24/04/2023	Eclipse Foundation AISBL OpenForum Europe AISBL Red Hat Limited Apache Software Foundation NLnet Labs
VIRKKUNEN Henna	Shadow rapporteur	ITRE	21/04/2023	Microsoft Corporation
KOKALARI Arba	Shadow rapporteur for opinion	IMCO	18/04/2023	Digitaleurope Meta Intel Bosch
MALDONADO LÓPEZ Adriana	Shadow rapporteur for opinion	IMCO	17/04/2023	Representación Permanente de España Ante la Unión Europea
VIRKKUNEN Henna	Shadow rapporteur	ITRE	14/04/2023	Kaupan liitto ry - Finnish Commerce Federation
VIRKKUNEN Henna	Shadow rapporteur	ITRE	14/04/2023	BUSINESSEUROPE
KOLAJA Marcel	Shadow rapporteur for opinion	IMCO	14/04/2023	Eclipse Foundation AISBL
MALDONADO LÓPEZ Adriana	Shadow rapporteur for opinion	IMCO	12/04/2023	OpenForum Europe
MALDONADO	Shadow rapporteur		12/04/2023	Federación de Consumidores y Usuarios

LÓPEZ Adriana	for opinion	IMCO		
VIRKKUNEN Henna	Shadow rapporteur	ITRE	12/04/2023	Apple Inc.
KOKALARI Arba	Shadow rapporteur for opinion	IMCO	11/04/2023	Ericsson
VIRKKUNEN Henna	Shadow rapporteur	ITRE	11/04/2023	ITI - The Information Technology Industry Council
VIRKKUNEN Henna	Shadow rapporteur	ITRE	30/03/2023	Finnish Information Security Cluster – Kyberala ry
DANTI Nicola	Rapporteur	ITRE	28/03/2023	CEMA - European Agricultural Machinery Industry Association Federazione Nazionale Costruttori Macchine per l'Agricoltura
LØKKEGAARD Morten	Rapporteur for opinion	IMCO	21/03/2023	Apple Inc. TIC Council BDI Federation of German Industries BEUC BSA The Software Alliance Confideration of Danish Industries Digital Europe ETNO Kapersky Microsoft Samsung Xiaomi
COVASSI Beatrice	Shadow rapporteur	ITRE	08/03/2023	The American Chamber of Commerce to the EU, Ericsson Brussels, DIGITALEUROPE, Bureau Européen des Unions de Consommateurs (BEUC), Bitkom, I-Com, BSA | the Software Alliance, UNIFE - The European Rail Supply Industry Association, Trellix, TIC Council, IBM, ETNO, Free Software Foundation Europe, Enedis, Federation of German Industries (BDI), Microsoft, Broadcom, DEKRA, Telefónica, S.A., DEUTSCHE TELEKOM AG, Kaspersky, ACEM, Xiaomi, ESMIG, CECIMO, Renault Group, TÜV, Huawei, SAP, Twilio, Samsung Electronics, APPLIA, Privacy International, Retail Europe, Samsung Electronics, Siemens
VIRKKUNEN Henna	Shadow rapporteur	ITRE	06/03/2023	Huawei Technologies
VIRKKUNEN Henna	Shadow rapporteur	ITRE	02/03/2023	(ISC)2
VIRKKUNEN Henna	Shadow rapporteur	ITRE	01/03/2023	TIC Council
VIRKKUNEN Henna	Shadow rapporteur	ITRE	01/03/2023	Siemens AG
VIRKKUNEN Henna	Shadow rapporteur	ITRE	01/03/2023	BEUC – The European Consumer Organisation
VIRKKUNEN Henna	Shadow rapporteur	ITRE	27/02/2023	Independent Retail Europe (formerly UGAL - Union of Groups of Independent Retailers of Europe)
VIRKKUNEN Henna	Shadow rapporteur	ITRE	27/02/2023	American Chamber of Commerce to the European Union
DANTI Nicola	Rapporteur	ITRE	27/02/2023	Alliance for IoT and Edge Computing Innovation IVZW Apple Inc. Association des Constructeurs Européens de Motocycles Bitkom e.V. Bureau Européen des Unions de Consommateurs DEKRA e.V. Independent Retail Europe (formerly UGAL - Union of Groups of Independent Retailers of Europe) International Information System Security Certification Consortium, Inc. Okta OpenForum Europe AISBL

				Privacy International UNIFE Verband Deutscher Maschinen- und Anlagenbau e.V.
MALDONADO LÓPEZ Adriana	Shadow rapporteur for opinion	IMCO	27/02/2023	Representación Permanente de España Ante la Unión Europea
DANTI Nicola	Rapporteur	ITRE	21/02/2023	Associazione Italiana Internet Provider
VIRKKUNEN Henna	Shadow rapporteur	ITRE	14/02/2023	DEKRA e.V.
VIRKKUNEN Henna	Shadow rapporteur	ITRE	08/02/2023	Cybersecurity Coalition
VIRKKUNEN Henna	Shadow rapporteur	ITRE	07/02/2023	Lenovo Group Limited
DANTI Nicola	Rapporteur	ITRE	07/02/2023	Istituto per la Competitività
VIRKKUNEN Henna	Shadow rapporteur	ITRE	01/02/2023	Google
VIRKKUNEN Henna	Shadow rapporteur	ITRE	31/01/2023	DIGITALEUROPE
MALDONADO LÓPEZ Adriana	Shadow rapporteur for opinion	IMCO	31/01/2023	The European Consumer Organisation
VIRKKUNEN Henna	Shadow rapporteur	ITRE	26/01/2023	Xiaomi
VIRKKUNEN Henna	Shadow rapporteur	ITRE	26/01/2023	BSA | The Software Alliance
DANTI Nicola	Rapporteur	ITRE	25/01/2023	APPLiA (Home Appliance Europe) BUSINESSEUROPE Broadcom DIGITALEUROPE Ericsson European Cyber Security Organisation European Telecommunications Network Operators' Association GSMA Europe Huawei Technologies IBM Corporation Microsoft Corporation SMEunited aisbl Siemens AG Splunk TIC Council Xiaomi Technology Netherlands B.V.
VIRKKUNEN Henna	Shadow rapporteur	ITRE	12/01/2023	Ericsson
VIRKKUNEN Henna	Shadow rapporteur	ITRE	11/01/2023	Ministry of Transport and Communications of Finland Permanent Representation of Finland to the EU
VIRKKUNEN Henna	Shadow rapporteur	ITRE	11/01/2023	Technology Industries of Finland (Teknologiateollisuus ry)
VIRKKUNEN Henna	Shadow rapporteur	ITRE	08/12/2022	Federation of Finnish Enterprises

Other Members

Transparency		

Name	Date	Interest representatives
MELCHIOR Karen	20/02/2024	Match Group
MELCHIOR Karen	15/02/2024	Apple Inc.
FUGLSANG Niels	22/06/2023	Confederation of Danish Industry
REPASI René	26/04/2023	Verbraucherzentrale Bundesverband
KALJURAND Marina	09/02/2023	Cybersecurity Coalition

Final act

Regulation 2024/2847
OJ OJ L 20.11.2024 — Summary

Corrigendum to final act 32024R2847R(02)
OJ OJ L 02.07.2025

Corrigendum to final act 32024R2847R(04)
OJ OJ L 17.10.2025

Corrigendum to final act 32024R2847R(01)
OJ OJ L 05.12.2024

Delegated acts

Reference	Subject
2025/2839(DEA)	Examination of delegated act
2025/3036(DEA)	Examination of delegated act

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.

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.

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 product's 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

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.