Basic information

2023/0108(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Procedure completed
Managed security services Amending Regulation 2019/881 2017/0225(COD) **Subject** 3.30.06 Information and communication technologies, digital technologies 3.30.07 Cybersecurity, cyberspace policy 3.30.25 International information networks and society, internet	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
ITRE Industry, Research and Energy	CUTAJAR Josianne (S&D)	02/05/2023
	Shadow rapporteur NIEBLER Angelika (EPP) GROOTHUIS Bart (Renew) NIINISTÖ Ville (Greens/EFA) TOŠENOVSKÝ Evžen (ECR)	

Committee for opinion	Rapporteur for opinion	Appointed
IMCO Internal Market and Consumer Protection	Chair on behalf of committee CAVAZZINI Anna (Greens/EFA)	23/05/2023
LIBE Civil Liberties, Justice and Home Affairs	The committee decided not to give an opinion.	

Council of the European Union

Council configuration	Meetings	Date
Employment, Social Policy, Health and Consumer Affairs	4064	2024-12-02

European Commission

Commission DG	Commissioner
Communications Networks, Content and Technology	BRETON Thierry

European Economic and Social Committee

Key events

Date	Event	Reference	Summary
18/04/2023	Legislative proposal published	COM(2023)0208	Summary
01/06/2023	Committee referral announced in Parliament, 1st reading		
25/10/2023	Vote in committee, 1st reading		
25/10/2023	Committee decision to open interinstitutional negotiations with report adopted in committee		
26/10/2023	Committee report tabled for plenary, 1st reading	A9-0307/2023	Summary
08/11/2023	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 72)		
09/11/2023	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 72)		
20/03/2024	Approval in committee of the text agreed at 1st reading interinstitutional negotiations	GEDA/A/(2024)001687 PE760.887	
24/04/2024	Decision by Parliament, 1st reading	T9-0354/2024	Summary
24/04/2024	Results of vote in Parliament		
02/12/2024	Act adopted by Council after Parliament's 1st reading		
19/12/2024	Final act signed		
15/01/2025	Final act published in Official Journal		

Technical information

Procedure reference	2023/0108(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
Amendments and repeals	Amending Regulation 2019/881 2017/0225(COD)
Legal basis	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/9/11804

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE752.802	07/09/2023	

Specific opinion	IMCO	PE749.983	21/09/2023	
Amendments tabled in committee		PE753.562	21/09/2023	
Committee report tabled for plenary, 1st reading/single reading		A9-0307/2023	26/10/2023	Summary
Text agreed during interinstitutional negotiations		PE760.887	20/03/2024	
Text adopted by Parliament, 1st reading/single reading		T9-0354/2024	24/04/2024	Summary

Council of the EU

Document type	Reference	Date	Summary
Coreper letter confirming interinstitutional agreement	GEDA/A/(2024)001687	21/03/2024	
Draft final act	00093/2024/LEX	19/12/2024	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2023)0208	18/04/2023	Summary
Commission response to text adopted in plenary	SP(2024)394	08/08/2024	

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	CZ_CHAMBER	COM(2023)0208	29/06/2023	
Contribution	PT_PARLIAMENT	COM(2023)0208	20/07/2023	
Contribution	CZ_SENATE	COM(2023)0208	01/08/2023	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
EESC	Economic and Social Committee: opinion, report	CES2408/2023	13/07/2023	

Additional information

Source	Document	Date
EP Research Service	Briefing	19/10/2023
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**
CUTAJAR Josianne	Rapporteur	ITRE	14/11/2023	ISC2
GROOTHUIS Bart	Shadow rapporteur	ITRE	24/10/2023	DIGITALEUROPE
CUTAJAR Josianne	Rapporteur	ITRE	10/10/2023	Lenovo Group Limited
CUTAJAR Josianne	Rapporteur	ITRE	15/09/2023	European Commission, DG CNECT
CUTAJAR Josianne	Rapporteur	ITRE	14/09/2023	TIC Council
CUTAJAR Josianne	Rapporteur	ITRE	29/08/2023	ENISA
CUTAJAR Josianne	Rapporteur	ITRE	27/07/2023	FERMA - Federation of European Risk Management Associations
CUTAJAR Josianne	Rapporteur	ITRE	18/07/2023	Board of Cyber
CUTAJAR Josianne	Rapporteur	ITRE	06/07/2023	Leonardo Cyber and Security Solutions
CUTAJAR Josianne	Rapporteur	ITRE	06/07/2023	Red Alert Labs IoT Security
CUTAJAR Josianne	Rapporteur	ITRE	06/07/2023	ESET Slovak
CUTAJAR Josianne	Rapporteur	ITRE	05/07/2023	European Commission, DG CNECT

Other Members

Transparency		
Name	**Date**	**Interest representatives**
DANTI Nicola	12/10/2023	Leonardo S.p.A.

Final act	
Regulation 2025/0037 OJ OJ L 15.01.2025	Summary
Corrigendum to final act 32025R0037R(01) OJ OJ L 24.01.2025	

Managed security services

2023/0108(COD) - 15/01/2025 - Final act

PURPOSE: to create European cybersecurity certification schemes for managed security services.

LEGISLATIVE ACT: Regulation (EU) 2025/37 of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services.

CONTENT: this regulation is part of the Cybersecurity legislative package which also includes a new regulation on cyber solidarity.

European certification schemes

This **targeted amendment** to the Cybersecurity Regulation aims to strengthen the EU's cyber resilience by allowing for the adoption in the future of European certification schemes for **'managed security services'**.

Managed security services, such as services related to cybersecurity incident management, penetration testing, security audits and consulting, including expert advice, related to technical support, have gained in importance for incident prevention and mitigation.

Managed security service providers have been the target of cyberattacks and, due to their high integration in operators' activities, they represent a particular risk. It is therefore important that essential and important entities exercise enhanced due diligence when selecting their managed security service providers.

The targeted amendment will contribute to **improving the quality of managed security services** and increasing their comparability, facilitate the emergence of reliable cybersecurity service providers and avoid fragmentation of the internal market. It will contribute to achieving the target of **75%** of EU businesses starting to use cloud computing services, big data or artificial intelligence or of more than **90%** of SMEs, including microenterprises, reaching at least a basic level of digital intensity and of essential public services being accessible online.

Role of the European Union Agency for Cybersecurity (ENISA)

ENISA will play an important role in the preparation of candidate European cybersecurity certification schemes. ENISA will:

- promote the use of European cybersecurity certification with a view to avoiding fragmentation of the internal market;

- contribute to the establishment and maintenance of a **European cybersecurity certification framework**;

- promote the development and implementation of Union policy on cybersecurity certification of ICT products and managed security services;

- compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services, ICT processes and managed security services ;

- facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services, ICT processes and managed security services.

Following a request from the Commission, ENISA will prepare a **candidate scheme** that meets the applicable requirements set out in the Regulation. When preparing a candidate scheme, ENISA will consult in a timely manner all relevant stakeholders through a formal, open, transparent and inclusive consultation process. For each candidate scheme, ENISA will set up an ad hoc working group to provide it with specific advice and expertise.

Information and consultation on the European cybersecurity certification schemes

The Commission will make **publicly available** the information on its request to ENISA to prepare a candidate scheme. During the preparation of a candidate scheme by ENISA, the European Parliament, the Council or both may request the Commission and ENISA to present relevant information on a draft candidate scheme on a quarterly basis.

Security objectives of European cybersecurity certification schemes

A European cybersecurity certification scheme for managed security services will be designed to achieve, as appropriate, at least the following security objectives:

- that the managed security services are provided with the requisite competence, expertise and experience;

- that the provider has established internal procedures to ensure that the managed security services are provided at all times to a sufficient level of quality;

- that data accessed, stored, transmitted or processed in the context of the provision of managed security services are protected against accidental or unauthorised access, storage, disclosure, destruction or other processing, or against loss or alteration or unavailability;

- that the availability of and access to data, services and functions is restored in a timely manner in the event of a physical or technical incident;

- that a record is kept and made available for the assessment of the data, services or functions that have been accessed, used or otherwise processed, at what times and by whom and to ensure that it is possible to evaluate these elements.

The Commission will **regularly evaluate** the effectiveness and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme should be made mandatory, through relevant provisions of Union law.

A **new Annex** contains the requirements to be met by conformity assessment bodies wishing to be accredited.

ENTRY INTO FORCE: 4.2.2025.

Managed security services

2023/0108(COD) - 24/04/2024 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 53 votes to 5, with 33 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services.

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

Subject matter

The proposed Regulation aims to enable the adoption of European cybersecurity certification schemes for managed security services. The definition of managed security services under this Regulation includes a non-exhaustive list of managed security services that could qualify for certification schemes, such as incident handling, penetration testing, security audits, and consulting related to technical support.

European certification schemes for managed security services should lead to the uptake of those services and to increased competition between providers offering managed security services. Without prejudice for the objective of ensuring sufficient and appropriate levels of relevant technical knowledge and professional integrity of such providers, certification schemes should, therefore, facilitate market entry and the offering of managed security services, by simplifying, to the extent possible, the potential regulatory, administrative and financial burden that providers, especially microenterprises or small and medium-sized enterprises (SMEs), could encounter when offering managed security services.

Additionally, in order to encourage the uptake of, and stimulate the demand for, managed security services, the schemes should contribute to the accessibility thereof, especially for smaller actors, such as microenterprises and SMEs, as well as local and regional authorities which have limited capacity and resources, but which are more prone to cybersecurity breaches with financial, legal, reputational, and operational implications.

The Union certification scheme for managed security services should contribute to the availability of secure and high-quality services which guarantee a safe digital transition and to the achievement of targets set up in the Digital Decade Policy Programme, especially with regard to the goal that 75% of Union undertakings start using Cloud, AI or Big Data, that more than 90% of microenterprises and SMEs reach at least a basic level of digital intensity and that key public services are offered online.

Preparation, adoption and review of a European cybersecurity certification scheme

Following a request from the Commission, ENISA will prepare a candidate scheme that meets the applicable requirements set out in the Regulation. Following a request from the European Cybersecurity Certification Group (ECCG) may prepare a candidate scheme that meets the applicable requirements. If ENISA rejects such a request, it will have to give reasons for its refusal. Any decision to reject such an application will be taken by the Management Board.

When preparing a candidate scheme, ENISA should consult all relevant stakeholders in a timely manner through a formal, open, transparent and inclusive consultation process. For each candidate scheme, ENISA should set up an ad hoc working group to provide specific advice and expertise. The ad hoc working groups set up for this purpose should include, where appropriate, experts from Member States' public administrations, EU institutions, bodies, offices and agencies and the private sector.

Information and consultation on the European cybersecurity certification schemes

The Commission should make the information on its request to **ENISA** to prepare a candidate scheme. During the preparation of a candidate scheme by ENISA, the European Parliament as well as the Council may request the Commission in its capacity as chair of the European Cybersecurity Certification Group (ECCG) and ENISA to present relevant information on a draft candidate scheme on a quarterly basis. Upon the request of the European Parliament or the Council, ENISA, in agreement with the Commission, may make available to the European Parliament and to the Council relevant parts of a draft candidate scheme in a manner appropriate to the confidentiality level required, and where appropriate in a restricted manner.

In order to enhance the dialogue between the Union institutions and to contribute to a formal, open, transparent and inclusive consultation process, the European Parliament as well as the Council may invite the Commission and ENISA to discuss matters concerning the functioning of European cybersecurity certification schemes for ICT products, ICT services, ICT processes or managed security services.

A **new annex** contains the requirements to be met by conformity assessment bodies wishing to be accredited.

In a **statement**, the Commission recalled that it is recognised that a thorough review of the Cybersecurity Regulation is of the utmost importance, including the evaluation of the procedures leading to the development, adoption and review of European cybersecurity certification schemes.

This review should be based on a deep analysis and broad consultation on the impact, effectiveness and efficiency of the functioning of the European cybersecurity certification framework. The analysis carried out as part of the evaluation established in Article 67 of the Cybersecurity Act should include on-going scheme development activities, such as the one concerning European cybersecurity certification scheme for cloud services (EUCS) as well as those of adopted schemes such as the one concerning the European Common Criteria-based cybersecurity certification scheme (EUCC).

Accordingly, the Commission, which is responsible for the review of the Cybersecurity Act, should ensure that the review takes into account as appropriate the necessary elements mentioned in light of Article 67 when presenting the review to the co-legislators.

Managed security services

2023/0108(COD) - 18/04/2023 - Legislative proposal

PURPOSE: to create European cybersecurity certification schemes for managed security services.

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: Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification sets up a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

Managed security services, which are services consisting of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management, have gained increasing importance in the prevention and mitigation of cybersecurity incidents. Accordingly, the providers of those services are considered as essential or important entities belonging to a sector of high criticality pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union.

Managed security service providers in areas such as incident response, penetration testing, security audits and consultancy, play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. They have however also themselves been the target of **cyberattacks** and pose a particular risk because of their close integration in the operations of their customers.

Some Member States have already begun adopting certification schemes for managed security services. There is therefore a growing risk of **fragmentation** of the internal market for managed security services owing to inconsistencies in cybersecurity certification schemes across the Union. This proposal aims to prevent such fragmentation.

CONTENT: the proposed targeted amendment to amend the scope of the European cybersecurity certification framework in the Cybersecurity Act aims to enable, by means of Commission implementing acts, the adoption of **European cybersecurity certification schemes for 'managed security services'**, in addition to information and technology (ICT) products, ICT services and ICT processes, which are already covered under the Cybersecurity Act.

The proposal also introduces a definition of those services, which is very closely aligned to the definition of 'managed security services providers' under the NIS 2 Directive (Article 2 of the Cybersecurity Act). It also adds new provisions on the security objectives of European cybersecurity certification adapted to 'managed security services'.

Lastly, a number of technical amendments are made to ensure that the relevant articles apply also to 'managed security services'.

Managed security services

2023/0108(COD) - 26/10/2023 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Industry, Research and Energy adopted the report by Josianne CUTAJAR (S&D, MT) on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services.

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:

Changes to the definition of managed security service

The report stated that managed security services, which are services consisting of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management, including detection, response to or recovery from incidents, have gained increasing importance in the prevention and mitigation of cybersecurity incidents. The activities of the providers of managed security services consist of services relating to prevention, identification, protection, detection, analysis, containment, response and recovery, including, but not limited to, cyber threat intelligence provision, real time threat monitoring through proactive techniques, including security-by-design, risk assessment, extended detection, remediation and response.

The Union rolling work programme for European cybersecurity certification

According to Members, the Union rolling work programme should include a list of ICT products, ICT services and ICT processes or categories thereof, and managed security services, that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme. In that context, the Commission should include an in-depth assessment of existing training paths to bridge identified skills gaps and a list of proposals for addressing the needs for skilled employees and types of skills.

SMEs

Members considered that the Commission should ensure appropriate financial support in the regulatory framework of existing Union programmes, in particular in order to ease the financial burden on microenterprises and SMEs, including start-ups acting in the field of managed security services.

Evaluation and review

By 28 June 2024, and every three years thereafter, the Commission should assess the impact, effectiveness and efficiency of ENISA and of its working practices, the possible need to modify ENISA's mandate and the financial implications of any such modification. The evaluation should assess: (i) the efficiency and effectiveness of the procedures leading to consultation, preparation and adoption of European cybersecurity certification schemes, as

well as ways to improve and accelerate those procedures; (ii) whether essential cybersecurity requirements for access to the internal market are necessary in order to prevent ICT products, ICT services, ICT processes and managed security services which do not meet basic cybersecurity requirements from entering the Union market.