










Procedure file

Basic information	
COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Awaiting Council's 1st reading position
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
	 Industry, Research and Energy		02/05/2023
		 CUTAJAR Josianne	
		Shadow rapporteur	
		 NIEBLER Angelika	
		 GROOTHUIS Bart	
Council of the European Union		 NIINISTÖ Ville	
		 TOŠENOVSKÝ Evžen	
	Committee for opinion	Rapporteur for opinion	Appointed
	 Internal Market and Consumer Protection	Chair on behalf of committee	23/05/2023
		 CAVAZZINI Anna	
	 Civil Liberties, Justice and Home Affairs	The committee decided not to give an opinion.	
European Commission	Commission DG	Commissioner	
	Communications Networks, Content and Technology	BRETON Thierry	
European Economic and Social Committee			

Key events			
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 71)		
09/11/2023	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 71)		
20/03/2024	Approval in committee of the text agreed at 1st reading interinstitutional negotiations	PE760.887 GEDA/A/(2024)001687	
24/04/2024	Decision by Parliament, 1st reading	T9-0354/2024	

Technical information

Procedure reference	2023/0108(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
	Amending Regulation 2019/881 2017/0225(COD)
Legal basis	Treaty on the Functioning of the EU TFEU 114
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/9/11804

Documentation gateway

Legislative proposal		COM(2023)0208	18/04/2023	EC	Summary
Economic and Social Committee: opinion, report		CES2408/2023	13/07/2023	ESC	
Committee draft report		PE752.802	07/09/2023	EP	
Amendments tabled in committee		PE753.562	21/09/2023	EP	
Specific opinion	IMCO	PE749.983	21/09/2023	EP	
Committee report tabled for plenary, 1st reading/single reading		A9-0307/2023	26/10/2023	EP	Summary
Text agreed during interinstitutional negotiations		PE760.887	20/03/2024	EP	
Coreper letter confirming interinstitutional agreement		GEDA/A/(2024)001687	21/03/2024	CSL	
Text adopted by Parliament, 1st		T9-0354/2024	24/04/2024	EP	

reading/single reading					
Additional information					
Research document	Briefing	19/10/2023			

Managed security services

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

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.

Transparency				
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	ESET Slovak
CUTAJAR Josianne	Rapporteur	ITRE	06/07/2023	Red Alert Labs IoT Security
DANTI Nicola	Member	12/10/2023	Leonardo S.p.A.	