Procedure file

Basic information

COD - Ordinary legislative procedure (ex-codecision procedure) Regulation 2017/0225(COD)	Procedure completed
EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act) Repealing Regulation (EU) 526/2013 2010/0275(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 8.40.08 Agencies and bodies of the EU	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
ITRE Industry, Research and Energy	NIEBLER Angelika Shadow rapporteur KOUROUMBASHEV Peter TOŠENOVSKÝ Evžen TELIČKA Pavel DALUNDE Jakop G. TAMBURRANO Dario LETARD-LECHEVALIER Christelle	27/10/2017

Committee for opinion	Rapporteur for opinion	Appointed
AFET Foreign Affairs	The committee decided not to give an opinion.	
BUDG Budgets	GEIER Jens	26/09/2017
IMCO Internal Market and Consumer Protection (Associated committee)	DANTI Nicola	25/09/2017
LIBE Civil Liberties, Justice and Home Affairs		11/03/2019

		FRANZ Romeo	
Council of the European Union	Council configuration	Meeting	Date
	General Affairs	3685	09/04/2019
	General Affairs	3578	20/11/2017
European Commission	Commission DG	Commissioner	
	Communications Networks, Content and Technology	KING Julian	
European Economic and Social Committee			
European Committee of the Regions			

Key events

13/09/2017	Legislative proposal published	COM(2017)0477	Summary
23/10/2017	Committee referral announced in Parliament, 1st reading		
20/11/2017	Resolution/conclusions adopted by Council		
18/01/2018	Referral to associated committees announced in Parliament		
10/07/2018	Vote in committee, 1st reading		
10/07/2018	Committee decision to open interinstitutional negotiations with report adopted in committee		
30/07/2018	Committee report tabled for plenary, 1st reading	A8-0264/2018	
10/09/2018	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 71)		
12/09/2018	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 71)		
14/01/2019	Approval in committee of the text agreed at 1st reading interinstitutional negotiations		
11/03/2019	Debate in Parliament		
12/03/2019	Results of vote in Parliament		
12/03/2019	Decision by Parliament, 1st reading	T8-0151/2019	Summary
09/04/2019	Act adopted by Council after Parliament's 1st reading		
17/04/2019	Final act signed		
17/04/2019	End of procedure in Parliament		
07/06/2019	Final act published in Official Journal		

Technical information

Procedure reference	2017/0225(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
	Repealing Regulation (EU) 526/2013 2010/0275(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 European Committee of the Regions
Stage reached in procedure	Procedure completed
Committee dossier	ITRE/8/11042

Documentation gateway

Legislative proposal		COM(2017)0477	13/09/2017	EC	Summary
Document attached to the procedure		SWD(2017)0500	13/09/2017	EC	
Document attached to the procedure		SWD(2017)0501	13/09/2017	EC	
Document attached to the procedure		SWD(2017)0502	13/09/2017	EC	
Economic and Social Committee: opinion, report		CES4390/2017	14/02/2018	ESC	
Committee opinion	LIBE	PE615.394	16/03/2018	EP	
Committee draft report		PE619.373	27/03/2018	EP	
Committee opinion	BUDG	PE619.094	23/04/2018	EP	
Amendments tabled in committee		PE621.015	30/04/2018	EP	
Amendments tabled in committee		PE621.098	30/04/2018	EP	
Committee opinion	IMCO	PE616.831	22/05/2018	EP	
Committee report tabled for plenary, 1st reading/single reading		A8-0264/2018	30/07/2018	EP	
Text adopted by Parliament, 1st reading/single reading		T8-0151/2019	12/03/2019	EP	Summary
Draft final act		00086/2018/LEX	17/04/2019	CSL	
Commission response to text adopted in plenary		SP(2019)393	30/04/2019	EC	

Final act

Regulation 2019/881
OJ L 151 07.06.2019, p. 0015 Summary

EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act)

PURPOSE: to enhance the organisational aspects of ENISA, the EU Cybersecurity Agency, with a view to ensuring an adequate level of cybersecurity in the Union and repeal Regulation (EU) 526/2013 on Information and Communication Technology cybersecurity certification (Cybersecurity Act).

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: the European Union has taken a number of actions to increase resilience and enhance its cybersecurity preparedness. Since the first EU Cybersecurity Strategy adopted in 2013, important developments have taken place, including the second mandate for the European Union Agency for Network and Information Security (ENISA) and the adoption of the Directive on security of network and information systems (NIS Directive), which form the basis for the present proposal.

In 2016 the European Commission adopted a Communication on Strengthening Europe's Cyber Resilience System, in which further measures were announced to increase the EUs resilience and preparedness.

The Council recalled that the ENISA Regulation is one of the core elements of an EU cyber resilience framework and called upon the Commission to take further steps to address issue of certification at the European level. In 2017, it welcomed the Commission's intention to review the Cybersecurity Strategy in September and to propose further targeted actions before the end of 2017.

IMPACT ASSESSMENT: the impact assessment sought to mitigate problems such as the fragmentation of policies and approaches to cybersecurity across Member States; dispersed resources and fragmentation of approaches to cybersecurity across EU institutions, agencies and bodies; insufficient awareness and information of citizens and companies, coupled with the growing emergence of multiple national and sectoral certification schemes.

The analysis led to the conclusion that a reformed ENISA in combination with an EU general ICT cybersecurity certification framework was the preferred option.

CONTENT: overall, the proposal reviews the current mandate of ENISA and lays down a renewed set of tasks and functions, with a view to effectively and efficiently supporting Member States, EU institutions and other stakeholders' efforts to ensure a secure cyberspace in the European Union.

The new proposed mandate seeks to give the Agency a stronger and more central role, in particular by also supporting Member States in implementing the NIS Directive and to counter particular threats more actively (operational capacity) and by becoming a centre of expertise supporting Member States and the Commission on cybersecurity certification.

Specially, it proposal seeks to establish:

- an EU Cybersecurity Agency, building on the European Agency for Network and Information Security (ENISA), which will improve coordination and cooperation across Member States and EU institutions, agencies and bodies;
- an EU cybersecurity certification framework that will ensure the trustworthiness of the billions of devices (Internet of Things) which drive todays critical infrastructures, such as energy and transport networks, and also new consumer devices, such as connected cars.

An EU Cybersecurity Agency: the Agency will be given a permanent mandate to assist Member States in effectively preventing and responding to cyber-attacks. It will improve the EU's preparedness to react by organising yearly pan-European cybersecurity exercises and by ensuring better sharing of threat intelligence and knowledge through the setting up of Information Sharing and Analyses Centres. It will help implement the Directive on the Security of Network and Information Systems which contains reporting obligations to national authorities in case of serious incidents.

The Cybersecurity Agency would also help put in place and implement the EU-wide certification framework that the Commission is proposing to ensure that products and services are cyber secure. The proposal also includes the provisions facilitating the combating of fraud, corruption and other unlawful activities as well as staffing and budget provisions.

An EU cybersecurity certification framework: at present, a number of different security certification schemes for ICT products exist in the EU. The Cybersecurity Agency, ENISA, will put in place and implement this certification process. The proposed EU-wide certification framework creates a comprehensive set of rules, technical requirements, standards and procedures to agree each scheme. Each scheme will be based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service e.g. smart cards.

The proposal establishes the main legal effects of European cybersecurity certification schemes, namely (i) the obligation to implement the scheme at national level and the voluntary nature of certification; (ii) the invalidating effect of European cybersecurity certification schemes on national schemes for the same products or services. It also lays down the procedure for the adoption of European cybersecurity certification schemes and the respective roles of the Commission, ENISA and the European Cybersecurity Certification Group.

BUDGETARY IMPLICATIONS: the total appropriations for ENISA, including administrative expenditure, from 2019 to 2022 is estimated at EUR 86.038 million.

EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act)

The Committee on Industry, Research and Energy adopted the report by Angelika NIEBLER (EPP, DE) on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

The committee recommended that the position of the European Parliament adopted at first reading following the ordinary legislative procedure amend the Commission proposal as follows:

Mandate and tasks of the Agency: the EU Cybersecurity Agency shall be reinforced for the purpose of: (i) contributing to achieving a

high common level of cybersecurity; (ii) preventing cyber-attacks within the Union; (iii) reducing fragmentation in the internal market and improve its functioning; (iv) ensuring consistency by taking into account the Member States cooperation achievements under the Directive on security of network and information systems (NIS Directive).

The Agency shall respect the competences of Member States regarding cybersecurity, especially those concerning public security, defence, national security and the activities of the state in areas of criminal law.

The main tasks of the Agency shall be, inter alia, to:

- promote cooperation, coordination and information sharing at Union level among Member States, Union institutions, agencies and bodies, and relevant stakeholders, on matters related to cybersecurity;
- support projects contributing to a high level of awareness, cyber hygiene and cyber literacy among citizens and businesses on issues related to the cybersecurity;
- contribute towards raising the awareness of the public, including by promoting education, about cybersecurity risks and provide guidance on good practices for individual users aimed at citizens, organisations and businesses;
- assist Members States and Union institutions in establishing and implementing coordinated vulnerability disclosure policies and government vulnerability disclosure review processes, whose practices and determinations should be transparent and subject to independent oversight;
- facilitate the establishment and launch of a long-term European IT security project to support the development of an independent IT security industry across the Union;
- support operational cooperation among Member States, Union institutions, agencies and bodies, with a view to achieving collaboration, by analysing and assessing existing national schemes, by developing and implementing a plan and by using the appropriate instruments to achieve the highest level of cybersecurity certification in the Union and the Member States;
- contribute to an EU level response in case of large-scale cross-border cybersecurity incidents and crises, mainly by supporting the technical management of incidents or crises with the aid of its independent expertise and its own resources;
- organise at least once a year, cybersecurity exercises across the Union.

Organisation and management: Members suggest that ENISA further strengthens its capabilities and technical expertise to be able to provide adequate support for operational cooperation with Member States. For this purpose the Agency shall progressively reinforce its staff dedicated to this task so as to be able to collect and analyse autonomously different types of a wide range of cybersecurity threats and malware, perform forensic analysis and assist Members States in the response to large scale incidents.

ENISA shall increase its know-how and capacities based on existing resources present in the Member States, notably by seconding national experts to the Agency, creating pools of experts, and staff- exchange programmes.

The Agency shall set up an ENISA Advisory Group composed of recognised security experts representing the relevant stakeholders, such as the ICT industry including SMEs, operators of essential services according to the NIS Directive, providers of electronic communications networks or services available to the public, consumer groups, academic experts in the cybersecurity, European Standards Organisations (ESOs), and EU agencies.

The ENISA Advisory Group shall set out the objectives in its work programme, which shall be published every six months to ensure transparency.

The Agency shall also have a Stakeholders Certification Group as an advisory body, to ensure regular dialogue with the private sector, consumers organisations, academia and other relevant stakeholders.

European cybersecurity certification schemes: Members consider that not only products and services should be covered by the regulation, but also the whole life cycle. Thus, processes have also to be included in the scope of application.

The certification scheme shall ensure:

- the confidentiality, integrity, availability and privacy of services, functions and data;
- that services, functions and data can be accessed and used only by authorised persons and/or authorised systems and programmes;
- that a process is in place to identify and document all dependencies and known vulnerabilities in ICT products, processes and services;
- that ICT products, processes and services are secure by default and by design;
- that other risks linked to cyber-incidents, such as risks to life, health, the environment and other significant legal interests are minimised.

Members suggested greater involvement from Member States and industry in the certification process.

The Agency shall maintain a website with all relevant information on European cybersecurity certification schemes, including with regards to withdrawn and expired certificates and national certifications covered, and ensure that they are made public.

Lastly, to promote the overall acceptance of certificates and conformity assessment results issued by conformity assessment bodies, Members proposed that national certification supervisory authorities operate a rigorous and transparent peer evaluation system and regularly undergo such evaluation.

EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act)

The European Parliament adopted by 586 votes to 44, with 36 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council on ENISA, the European Union Cybersecurity Agency and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

The position of the European Parliament adopted at first reading under the ordinary legislative procedure has amended the Commission proposal as follows:

Enhanced powers for the EU Cybersecurity Agency (ENISA)

In order to ensure the proper functioning of the internal market while seeking to achieve a high level of cybersecurity, the proposed regulation would set out the objectives, tasks and organisational issues concerning ENISA (the European Union Agency for Cybersecurity).

ENISA would carry out its tasks with the aim of achieving a high common level of cybersecurity throughout the Union, including by actively assisting Member States and EU institutions, bodies, offices and agencies to improve cybersecurity. It would serve as a reference point for cybersecurity advice and expertise for EU institutions, bodies, offices and agencies as well as for other relevant EU stakeholders. To this end, it should develop its own resources, including its technical capacities and skills.

ENISA should, among other things:

- assist Member States and EU institutions, bodies, offices and agencies in (i) building capacity and preparedness to prevent, detect and respond to cyber threats and incidents; (ii) developing and promoting cyber security policies to support the overall availability or integrity of the public core of the open Internet; and (iii) implementing, on a voluntary basis, policies on vulnerability disclosure;

- promote information sharing and coordination at EU level, between Member States, EU institutions, bodies, offices and agencies and relevant public and private sector stakeholders on cybersecurity issues;

- promote the use of European cybersecurity certification to avoid fragmentation of the internal market;

- support Member States in the field of cybersecurity awareness and education by promoting closer coordination and the exchange of good practices between Member States. Such support could include the development of a network of national education contact points and a cybersecurity training platform;

- raise public awareness of the risks associated with cybersecurity and provide guidance to citizens, organisations and businesses on good practices for individual users, including IT hygiene and digital skills;

- facilitate the technical management of incidents with significant or substantial impact, in particular by supporting the voluntary sharing of technical solutions between Member States or by producing combined technical information, such as technical solutions voluntarily shared by Member States;

- promote the concepts of security from the design stage and privacy from the design stage at EU level;

- contribute, where appropriate, to cooperation with organisations such as the OECD, OSCE and NATO, for example through joint exercises in the field of cybersecurity.

ENISA should keep the European Parliament regularly informed of its activities.

National Liaison Officer Network

The Management Board should establish, on a proposal from the Executive Director, a network of national liaison officers composed of representatives of all Member States (national liaison officers). This network would facilitate the exchange of information between ENISA and the Member States and would help ENISA to publicise its activities and disseminate the results of its work and recommendations to relevant stakeholders across the Union.

European Cybersecurity Certification Framework

The amended text creates the first European cybersecurity certification scheme to ensure that products, processes and services sold in EU countries comply with cybersecurity standards.

The Commission should publish, no later than one year after the entry into force of the Regulation, a rolling work programme of the Union for European Cybersecurity Certification which identifies strategic priorities for future European cybersecurity certification schemes. It should maintain a dedicated website providing information on European cybersecurity certification schemes, European cybersecurity certificates and EU declarations of conformity.

In order to ensure equivalence of standards across the Union for European cybersecurity certificates and EU declarations of conformity, national cybersecurity certification authorities would be subject to peer review.

EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act)

PURPOSE: reform the current European Network and Information Security Agency (ENISA) to provide the EU with an increased cybersecurity capacity and define a framework for the establishment of a European Cybersecurity Certification Scheme.

LEGISLATIVE ACT: 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 and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

CONTENT: with a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down:

- objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and

- 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.

European Union Cybersecurity Agency (ENISA)

The Regulation strengthens the current European Union Network and Information Security Agency (ENISA) into a permanent body, the EU

Cybersecurity Agency.

ENISA shall carry out its tasks with the aim of achieving a high common level of cybersecurity throughout the Union, including by actively assisting Member States and EU institutions, bodies, offices and agencies to improve cybersecurity. It would serve as a reference point for cybersecurity advice and expertise for EU institutions, bodies, offices and agencies as well as for other relevant EU stakeholders.

ENISAs tasks shall include:

- assist EU institutions, bodies, offices and agencies, as well as Member States, in the development and implementation of EU policies related to cybersecurity and help them to increase the protection of their networks and information systems, improve cyber-resilience and cyber-reaction capacities, and develop skills and competences in the field of cybersecurity;
- support EU policy on cybersecurity certification, for example by playing a central role in the development of certification systems;
- promote the use of the new certification system, for example by creating a website providing information on certificates;
- promote cooperation, including information sharing and coordination at EU level;
- support Member States' actions to prevent and respond to cyber threats, in particular in the event of cross-border incidents;
- promote a high level of awareness among citizens, organisations and businesses of cybersecurity issues, including computer hygiene and digital skills;
- organise regular EU-wide cyber security exercises, including a large-scale global exercise once every two years;
- produce long-term strategic analyses of cyber threats and incidents to identify emerging trends and help prevent incidents.

The mandate also provides for a network of national liaison officers to facilitate the exchange of information between ENISA and the Member States.

An ENISA Advisory Group composed of recognised experts representing relevant stakeholders, as well as a Stakeholder Group for Cybersecurity Certification shall also be established.

European Cybersecurity Certification Framework

The Regulation creates the first European cybersecurity certification scheme to ensure that products, processes and services sold in EU countries comply with cybersecurity standards.

The Commission shall publish, no later than one year after the entry into force of the Regulation, a rolling work programme of the Union for European Cybersecurity Certification which identifies strategic priorities for future European cybersecurity certification schemes. It shall maintain a dedicated website providing information on European cybersecurity certification schemes, European cybersecurity certificates and EU declarations of conformity.

The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law.

The Commission shall regularly monitor the impact of certification systems and assess their level of use by manufacturers and service providers.

There will be three different levels of insurance, depending on the level of risk associated with the intended use of the product, namely "basic", "substantial" or "high". At the most basic level, manufacturers or service providers shall be able to carry out the conformity assessment themselves.

In order to ensure equivalence of standards across the Union for European cybersecurity certificates and EU declarations of conformity, national cybersecurity certification authorities shall be subject to peer review.

ENTRY INTO FORCE: 27.6.2019. Certain provisions shall apply from 28.6.2021.