Council of the European Union

Brussels, 9 January 2025
(OR. en)

5193/25

LIMITE

CYBER 9
JAI 27
DATAPROTECT 5
TELECOM 6
MI 13
CSC 15
CSCI 5
CADREFIN 2
BUDGET 1
IND 7
RELEX 17
CODEC 16

NOTE

From:	Presidency
To:	Delegations
Subject:	Stocktaking exercise on the implementation of EU cybersecurity laws

In line with the estimates of the Presidency, four main EU cybersecurity laws, most of them recently adopted – the NIS2 Directive, the Cyber Resilience Act, the Cyber Solidarity Act and the Cybersecurity Act – provide for over 70 individual tasks and empowerments for the Commission, other EU bodies and the Member States. The Presidency believes there is a need for a simple tool to have an overview of the implementation process. This is an ad hoc process and in no way seeks to replace the Commission's role under the Treaties as regards its oversight regarding the implementation and application of EU law by Member States.

In light of this, the Presidency will be launching a stocktaking exercise on the implementation of these four pieces of legislation, on the basis of the four tables attached as an annex. The tables are meant to be a living instrument, providing up-to date information on the implementation of EU cybersecurity laws, both by the EU institutions and bodies as well as by the Member States.

This process is designed to be collaborative, and the Presidency will ensure that all stakeholders will have the opportunity to contribute at all stages. The steps outlined below provide the roadmap for this process:

Step 1: Initial feedback (end of January)

The Presidency invites Member States and the Commission for feedback on the envisaged process following the presentation of the tables at the HWPCI meeting on 13 January 2025. This will give stakeholders the opportunity to share their thoughts, suggestions, and identify possible missing elements which will help in refining the approach. The discussion on the initial feedback will take place on 27th January.

Step 2: State of play (January - February)

Following the feedback received from all stakeholders, the table might be amended mid February.

The Presidency will then invite the Member States to complete the 'state of play' section **by 17 March**.

In parallel, the Commission, ENISA and other stakeholders mentioned in the table will also be asked to provide relevant information **by 17 March**.

Step 3: Table (March/April)

The Presidency will consolidate the input received and produce a new version of the tables, incorporating all information received by the end of April. The Presidency will ask for feedback from Member States and Commission on the new version by mid – May.

Step 4: Debate(s) and updates (May – June)

The Presidency will:

– propose a debate on challenges and best practices in implementation;
– facilitate regular coordinated updates of the tables, as necessary;
– invite the stakeholders (Member States, EU Institutions, bodies and agencies) to provide information proactively, should they reach new milestones in implementation of specific instruments.

Step 5: Conclusion and sharing of the lessons learned (June)

The possible horizon of this exercise stretches well beyond the Polish Presidency. In light of this, by the end of June, the Presidency will share its lessons learned from the process, in the hope that the exercise will continue under future Presidencies.

The Presidency looks forward to delegations' active participation and engagement throughout this process.

ANNEX

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Instructions

Member States will be asked to provide information referred to in the third table - the content of the table will be based on self-declaration of Member States and is not linked to the assessment by the Commission as to the completeness of the transposition.

Version last updated on 8.01.2025, distributed for the purpose of consultation with Member States and relevant EU institutions / bodies.

Tasks and empowerments of the Commission

Task	Legal basis	Obligatory (y/n)	Deadline	Status	Reference
Guidelines claryfing the application of Article 4(1) and (2) - sector-specific Union legal acts	Article 3(3)	**Yes**	17 July 2023	Completed	Guidelines
Implementing act - technical and methodological requirements of the Cybersecurity risk management measures with regards to DNS service providers, TLD name registries [...]	Article 21(5)	**Yes**	17 October 2024	Completed	Commission Implementing Regulation 2024/2690

Implementing act - specyfing the cases in which an incident shall be considered to be significant with regards to DNS service providers, TLD name registries [...]	Article 23(11)	**Yes**	17 October 2024	Completed	Commission Implementing Regulation 2024/2690
Providing guidelines and templates regarding the obligations laid down in Article 3(4) (notification of entities)	Article 3(4)	**Yes**	without undue delay	Completed	Guidelines
Identification of specific critical ICT services, ICT systems and ICT products that may be subject to the coordinated security risk assessment	Article 22(2)	**Yes**	no deadline		
Review of the functioning of the Directive	Article 40	**Yes**	By 17 October 2027 and every 36 months thereafter		
Implementing act - procedural arrangements necessary for the functioning of the NIS Cooperation Group	Article 14(8)	No	n/a	Completed	Commission Implementing Decision 2017/ 179
Delegated act - specyfing which categories of essential and important entities are required to use certain certified ICT products, ICT services and ICT rpocessess or obtan a certificate under a European cybersecurity certification scheme	Article 24(2)	No	n/a		

Tasks of ENISA, CSIRT network and Cooperation Group

Actor	Task	Legal basis	Deadline	Status	Reference
ENISA	Adoption of report on the state of cybersecurity in the Union and its presentation in the European Parliament	Article 18(1)	biennial	First report published	2024 Report on the State of the Cybersecurity in the Union | ENISA
ENISA	Developing a European vulnerability database	Article 12(2)	no deadline		
ENISA	Drawing up advice and guidelines regarding the technical areas to be considered for standardisation	Article 25(2)	no deadline		
ENISA	Creation of registry of entities providing digital services (DNS service providers, TLD name registries...)	Article 27(1)	no deadline	Completed	Launch date: 9 December 2024
NIS Cooperation Group	Establishment of the methodology and organisational aspects of peer reviews	Article 19(1)	17 January 2025	NIS Coperation Group silent procedure running until 15 January 2025	
CSIRTs network	For the purpose of the review referred to in Article 40, assess the progress made with regard to the operational cooperation and adopt a report	Article 15(4)	By 17 January 2025, and every two years thereafter		

Information from Member States

Member State	Main act transposing NIS2	Competent authority	Cyber crisis management authority
	Reference: Article 41(1)	*Reference: Article 8*	*Reference: Article 9*
Belgium			
Bulgaria			
Czechia			
Denmark			
Germany			
Estonia			
Ireland			
Greece			
Spain			
France			
Croatia			
Italy			
Cyprus			
Latvia			
Lithuania			
Luxembourg			
Hungary			
Malta			
Netherlands			

Austria			
Poland			
Portugal			
Romania			
Slovenia			
Slovakia			
Finland			
Sweden			

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 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)

Instructions

Member States will be asked to provide information referred to in the third table.

Tasks and empowerments of the Commission

Task	Legal basis	Obligatory (y/n)	Deadline	Status	Reference
Report on the evaluation and review of CRA, to be submitted to the EP and to the Council	Article 70(1)	**Yes**	By 11 December 2030 and every four years thereafter		
Report assessing the effectiveness of the single reporting platform and the impact of the application of the cybersecurity-related grounds referred to in Article 16(2) by the CSIRTs, to be submitted to the EP and the Council	Article 70(2)	**Yes**	By 11 September 2028		
Organisation of a cross-sectoral group of notified bodies	Article 51	**Yes**	No deadline		
Request to the European standardisation organisations to draft harmonised standards for essential cybersecurity requirements	Article 27(1)	**Yes**	No deadline		
Organising consultation and information session with stakeholders on the implementation of CRA	Article 9(2)	**Yes**	Once a year		

Organisation of the exchange of experience between the MS's national authorities responsible for notification policy	Article 50	**Yes**	No deadline		
Making publicly available the list of the bodies notified	Article 44(2)	**Yes**	No deadline - after the notification by notifying authorities		
Making publicly available the information of the procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies - as notified by the Member States	Article 38(2)	**Yes**	No deadline - after the notification by the MSs		
Implementing act specyfing the simplified technical documentation form targeted at the needs of SMEs	Article 33(5)	**Yes**	No deadline		
Implementing act specifying the technical description of the categories of products with digital elements	Article 7(4)	**Yes**	11 December 2025		
Guidance to assist economic operators in applying CRA, with a focus on SMEs	Article 26	**Yes**	No deadline		
Encouraging and facilitating the exchange of experience between the designated market surveillance authorities	Article 52(9)	**Yes**	No deadline		
Delegated act specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications by CSIRT	Article 14(9)	**Yes**	11 December 2025		

Advertising available financial support of exsisting Union programmes	Article 33(4)	**Yes**	No deadline		
Implementing acts providing for corrective or restrictive measures at Union level, including requiring products concerned to be withdrawn from the market or recalled	Article 56(5), Article 57(9)	No - only under conditions laid down in article 56 and 57 respectively	n/a		
Implementing act establishing common specifications covering technical requirements	Article 27(2)	No - only under conditions laid down in Article 27(2)	n/a		
Implementing act specifying the format and procedures of the notifications referred to in articles 14, 15 and 16	Article 14(10)	No	n/a		
Implementing act specifying the format and elements of the software bill of materials	Article 13(24)	No	n/a		
Implementing act laying down technical specifications for labels, pictograms or any other marks related to the security of products with dgitail elements, their support period and mechanisms to promote their use and increase public awareness	Article 30(6)	No	n/a		
Delegated acts adding elements to be included in the technical documentation set out in Annex VII to take account of technological developments	Article 31(5)	No	n/a		
Delegated act specyfing whether limitation and exclusion of application of CRA to certain products with digital elements	Article 2(5)	No	n/a		

Delegated act specyfing the European cybersecurity certification schemes that can be used to demonstrate conformity of products with the essential cybersecurity requirements	Article 27(9)	No	n/a		
Delegated act specyfing minimum support period for specific product categories	Article 13(8)	No	n/a		
Delegated act establishing voluntary security attestation programmes allowing the developers or users of products with digital elements qualifying as free and open-source software to assess the conformity of such products with essential requirements or other obligations laid down in CRA	Article 25	No	n/a		
Delegated act determining which products are to be required to obtain a EUropean cybersecrutiy certificate	Article 8(1)	No	n/a		
Delegated act amending Annex IV (Critical products with digital elements)	Article 8(2)	No	n/a		
Delegated act amending Annex III (Important products with digital elements)	Article 7(3)	No	n/a		
Delegated act adding elements to the minimum content of the EU declaration of conformity	Article 28(5)	No	n/a		

Tasks for ENISA

Task	Legal basis	Obligatory (y/n)	Deadline	Status	Reference
Establishment of a single reporting platform	Article 16(1)	Yes	No deadline		

Information from Member States

Member State	**Notifying authority**	**Any laws related to the implementation of the Regulation, including those laying down penalties**	**Actions addressed to the SMEs, if applicable**	**Cyber resilience regulatory sandboxes, if applicable**
	Reference: Article 36(1)	*Reference: Article 52(2)*	*Reference: Article 33(1), Support measures for SMEs*	*Reference: Article 33(2), Support measures for SMEs*
Belgium				
Bulgaria				
Czechia				
Denmark				
Germany				
Estonia				
Ireland				
Greece				
Spain				
France				
Croatia				
Italy				
Cyprus				
Latvia				
Lithuania				
Luxembourg				
Hungary				
Malta				
Netherlands				

Austria				
Poland				
Portugal				
Romania				
Slovenia				
Slovakia				
Finland				
Sweden				

Instructions

Member States will be asked to provide information on their National Cyber Hub and Hosting Consortium, if applicable.

Tasks and empowerments of the Commission

Task	Legal basis	Obligatory (y/n)	Deadline	Status	Reference
Proposal for a Council implementing act authorising the provision EU Cybersecurity Reserve to DEP-associated third country	Article 19(3)	**Yes**, but subject to positive assessment of the information provided by the third country concerned	n/a		
Entrusting the operation of EU Cybersecurity Reserve, in full or in part, to ENISA	Article 14(5)	**Yes**, but subject to contribution agreement as defined in Article 2 point (18) of Financial Regulation	no deadline		
Assessment of information with regards to DEP-associated third countries whose DEP associated agreements provide for participation in EU Cybersecurity Reserve	Article 19(3)	**Yes**, but subject to amendment of DEP association agreements	At least once a year		
Identification of the sectors or sub-sectors for which a call for proposals to award grants may be issued in the framework of Cybersecurity Emergency Mechanism	Article 12(4)	**Yes**	no deadline		
Establishing priorities of the EU Cybersecurity Reserve, and informing the EP and the Council thereof	Article 14(4)	**Yes**	no deadline		

Delegated act specyfing the types and number of response services required for the EU Cybersecurity Reserve	Article 14(7)	No	n/a		
Implementing act specyfing the detailed procedural arrangements for requesting EU Cybersecurity Reserve support services and responding to such requests	Article 15(7)	No	n/a		
Amendment of Digital Europe Programme association agreements	Article 19(1)	No	n/a		

Tasks of ENISA, ECCC and NIS Cooperation Group

Actor	Task	Legal basis	Deadline	Status	Reference
ENISA	**Interoperability guidelines specifying in particular information sharing formats and protocols for Cross-Border Cyber Hubs**	Article 6(4)	Without undue delay and at the latest 12 months after the date of entry into force of CySol		
ENISA	**Mapping of the services needed by the users referred to in Article 3(3)(a) and (b); including the availability of such services**	Article 14(6)	At least every two years		
ENISA	**Developing a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve**	Article 15(6)	no deadline		
ENISA	**Developing a template for agreements between the trusted provider and the user to which the support under the EU Cybersecurity Reserve is provided**	Article 16(6)	no deadline		

ECCC	**Mapping of the tools, infrastructures and services necessary and of adequate quality to establish or enhance National Cyber Hubs and Cross-Border Cyber Hubs, and their availability**	Article 9(4)	At least every two years		
NIS Cooperation Group	**Developing common risk scenarios and methodologies for the coordinated testing exercises under the Cybersecurity Emergency Mechanism**	Article 12(6)	no deadline		

Information from Member States

Member State	**National Cyber Hub, if applicable**	**Hosting Consortium, if applicable**
	Reference: Article 4	*Reference: Article 5*
Belgium		
Bulgaria		
Czechia		
Denmark		
Germany		
Estonia		
Ireland		
Greece		
Spain		
France		
Croatia		
Italy		
Cyprus		

Latvia		
Lithuania		
Luxembourg		
Hungary		
Malta		
Netherlands		
Austria		
Poland		
Portugal		
Romania		
Slovenia		
Slovakia		
Finland		
Sweden		

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 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)

Instructions and information

Member States will be asked to provide information on their national cybersecurity certification authorities.

Tasks and empowerments of the Commission

Task	Legal basis	Obligatory (y/n)	Deadline	Status	Reference
Union rolling work programme for European cybersecurity certification	Article 47	**Yes**	The Union rolling work programme shall be updated at least once every three years	First work programme published in February 2024	Link
Assessment of the efficiency and use of the adopted cybersecurity schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law	Article 56	**Yes**	First assessment shall be carried out by 31 December 2023, and subsequent assessments shall be carried out at least every two years thereafter		
Evaluation and review of ENISA and of the impact, effectiveness and effiiciency of Title III (certification framework)	Article 67(1) and (2)	**Yes**	By 28 June 2024, and every five years thereafter		
Requests for preparation of cybersecurity schemes	Article 48	No	n/a	*See separate table below*	
Adoption of cybersecurity schemes	Article 49(7)	No	n/a	*See separate table below*	

Implementing act establishing a plan for peer review which covers a period of at least five years, laying down the criteria concerning the composition of the peer review team, the methodology to be used in peer review, and the schedule, the frequency and other tasks related to it	Article 59(5)	No	n/a - not mandatory		
Implementing act establishing the circumstances, formats and procedures for notifications of conformity assessment bodies	Article 61(5)	No	n/a - not mandatory	Completed	Implementing Regulation 2024/3143

European cybersecurity certification schemes

Name of the scheme	Status	Reference
European Common Criteria-based cybersecurity certification scheme	Implementing Regulation 2024/482 adopted by the Commission, will be applicable from 27 February 2025 Amended by Implementing Regulation 2024/3144	Implementing Regulation 2024/482
European Cloud Certification Scheme	Request sent to ENISA	
European 5G Certification Scheme	Request sent to ENISA	
European Digital Identity Wallets Scheme	Request sent to ENISA	

Information from Member States

Member State	National cybersecurity certification authority(ies)
Belgium	
Bulgaria	
Czechia	
Denmark	
Germany	
Estonia	

Ireland	
Greece	
Spain	
France	
Croatia	
Italy	
Cyprus	
Latvia	
Lithuania	
Luxembourg	
Hungary	
Malta	
Netherlands	
Austria	
Poland	
Portugal	
Romania	
Slovenia	
Slovakia	
Finland	
Sweden	