European Parliament
2019-2024

Committee on Civil Liberties, Justice and Home Affairs

2022/0085(COD)

1.3.2023

OPINION

of the Committee on Civil Liberties, Justice and Home Affairs

for the Committee on Industry, Research and Energy

on the proposal for a regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Rapporteur for opinion (*): Tomas Tobé

(*) Associated committee – Rule 57 of the Rules of Procedures

PA_Legam

AMENDMENTS

The Committee on Civil Liberties, Justice and Home Affairs calls on the Committee on Industry, Research and Energy, as the committee responsible, to take into account the following amendments:

Amendment 1

Proposal for a regulation
Recital 4

Text proposed by the Commission	*Amendment*
(4) The Union institutions, bodies and agencies are attractive targets who face highly skilled and well-resourced threat actors as well as other threats. At the same time, the level and maturity of cyber resilience and the ability to detect and respond to malicious cyber activities varies significantly across those entities. It is thus necessary for the functioning of the European administration that the institutions, bodies and agencies of the Union achieve a high common level of cybersecurity through a cybersecurity baseline (a set of minimum cybersecurity rules with which network and information systems and their operators and users have to be compliant to minimise cybersecurity risks), information exchange and collaboration.	(4) The Union institutions, bodies and agencies ***have been and*** are attractive targets who face highly skilled and well-resourced threat actors as well as other threats. At the same time, the level and maturity of cyber resilience and the ability to detect and respond to malicious cyber activities varies significantly across those entities. It is thus necessary for the functioning of the European administration that the institutions, bodies and agencies of the Union achieve a high common level of cybersecurity through a cybersecurity baseline (a set of minimum cybersecurity rules with which network and information systems and their operators and users have to be compliant to minimise cybersecurity risks), information exchange and collaboration.

Amendment 2

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) The Directive [proposal NIS 2] on measures for a high common level of cybersecurity across the Union aims to further improve the cybersecurity resilience and incident response capacities of public and private entities, national	(5) The Directive [proposal NIS 2] on measures for a high common level of cybersecurity across the Union aims to further improve the cybersecurity resilience and incident response capacities of public and private entities, national

competent authorities and bodies as well as the Union as a whole. It is therefore necessary that Union institutions, bodies and agencies follow suit by ensuring rules that are consistent with the Directive [proposal NIS 2] and mirror its level of ambition.	competent authorities and bodies as well as the Union as a whole. It is therefore necessary that Union institutions, bodies and agencies follow suit by ensuring rules that are consistent with the Directive [proposal NIS 2] and mirror its level of ambition. ***Security requirements should be at least equal to, or higher than, the minimum security requirements of the entities covered by Directive (EU) 2022/2555.***

Amendment 3

Proposal for a regulation
Recital 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) The Union institutions, bodies, offices and agencies should be provided with adequate means and tools by means of which to strengthen their cyber resilience. It is essential, therefore, to ensure that appropriate coordination mechanisms are in place for decision-making to be done in an efficient and effective manner.

Amendment 4

Proposal for a regulation
Recital 22

Text proposed by the Commission	*Amendment*
(22) All personal data processed under this Regulation should be processed in accordance with data protection legislation including Regulation (EU) 2018/1725 of the European Parliament and of the Council***.***[7]	(22) All personal data processed under this Regulation should be processed in accordance with ***Union*** data protection legislation including Regulation (EU) 2018/1725 of the European Parliament and of the Council[7]***. This Regulation should not affect the application of Union law governing the processing of personal data, including the tasks conferred on and powers of the EDPS. CERT-EU and the***

	IICB should work in close cooperation with the EPDS and staff specialised in data protection in Union institutions, bodies, offices and agencies to ensure full compliance with Union data protection law.
[7] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).	[7] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

Amendment 5

Proposal for a regulation
Recital 22 a (new)

Text proposed by the Commission	*Amendment*
	(22a) Cybersecurity systems and services involved in the prevention, detection and response to cyber threats should comply with data protection and privacy law and should take relevant technical and organisational safeguarding measures to ensure that such compliance is achieved in an accountable way.

Amendment 6

Proposal for a regulation
Recital 23

Text proposed by the Commission	*Amendment*
(23) The handling of information by CERT-EU and the Union institutions, bodies and agencies should be in line with ***the*** rules laid down in Regulation	(23) The handling of information by CERT-EU and the Union institutions, bodies and agencies should be in line with ***Union*** rules ***on information security, in***

[proposed Regulation on information security]. To ensure coordination on security matters, any contacts with CERT-EU initiated or sought by national security and intelligence services should be communicated to the Commission's Security Directorate and the chair of the IICB without undue delay.	***particular those*** laid down in Regulation [proposed Regulation on information security]. To ensure coordination on security matters, any contacts with CERT-EU initiated or sought by national security and intelligence services should be communicated to the Commission's Security Directorate and the chair of the IICB without undue delay.

Amendment 7

Proposal for a regulation
Recital 25 a (new)

Text proposed by the Commission	*Amendment*
	(25a) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 17 May 2022,

Amendment 8

Proposal for a regulation
Article 4 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Each Union institution, body and agency shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity.	5. Each Union institution, body and agency shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity. ***The Local Cybersecurity Officer shall cooperate with the data protection officer designated in accordance with Article 43 of Regulation (EU) 2018/1725 when dealing with overlapping activities, such as applying data protection by design and by default to cybersecurity measures and selecting cybersecurity measures that involve protection of personal data, integrated risk management and integrated security incident handling.***

Amendment 9

Proposal for a regulation
Article 9 – paragraph 3 – subparagraph 1 – point k a (new)

Text proposed by the Commission	*Amendment*
	(ka) the European Data Protection Supervisor;

Amendment 10

Proposal for a regulation
Article 9 – paragraph 3 – subparagraph 1 – point k b (new)

Text proposed by the Commission	*Amendment*
	(kb) the European Union Agency for Law Enforcement Cooperation.

Amendment 11

Proposal for a regulation
Article 12 – paragraph 2 – point e a (new)

Text proposed by the Commission	*Amendment*
	(ea) inform the European Data Protection Supervisor of any indication of an infringement by an Union institution, body, office or agency of the obligations laid down in this Regulation which comprises an unlawful processing of personal data;

Amendment 12

Proposal for a regulation
Article 12 – paragraph 2 – point e b (new)

Text proposed by the Commission	*Amendment*
	(eb) work in close cooperation with the

	European Data Protection Supervisor in the resolution of incidents resulting in personal data breaches or in breaches of the confidentiality of electronic communication.

Amendment 13

Proposal for a regulation
Article 12 – paragraph 7 a (new)

Text proposed by the Commission	*Amendment*
	7a. CERT-EU shall inform the European Data Protection Supervisor when addressing significant vulnerabilities, significant incidents or major attacks that have the potential to result in personal data breaches or in breaches of the confidentiality of electronic communication.

Amendment 14

Proposal for a regulation
Article 18 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The provisions of Regulation (EC) No 1049/2001 of the European Parliament and the Council[9] shall apply with regard to requests for public access to documents held by CERT-EU, including the obligation under that Regulation to consult other Union institutions, bodies and agencies whenever a request concerns their documents.	2. The provisions of Regulation (EC) No 1049/2001 of the European Parliament and the Council[9] shall apply with regard to requests for public access to documents held by CERT-EU, including the obligation under that Regulation to consult other Union institutions, bodies and agencies***, or, where relevant, Member States,*** whenever a request concerns their documents.
[9] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145,	[9] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145,

31.5.2001, p. 43).	31.5.2001, p. 43).

Amendment 15

Proposal for a regulation
Article 18 – paragraph 3 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	Any processing, exchange, collection or retention of personal data by CERT-EU, the IICB and Union institutions, bodies, offices and agencies shall be limited to processing, exchange, collection or retention that is strictly necessary and shall be carried out for the sole purpose of fulfilling their respective obligations under this Regulation.

Amendment 16

Proposal for a regulation
Article 18 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. The Commission shall, by ... [1 year after the date of entry into force of this Regulation], adopt a delegated act to specify which personal data processing activities are permitted under this Regulation, including the purpose of the processing, the categories of personal data, the categories of data subjects, the conditions for data processing, maximum retention periods, the definition of the data controllers and processors, and recipients in the case of transmission.
	The delegated act referred to in the first subparagraph shall limit processing activities to those that are strictly necessary and shall require that such processing activities be as targeted as possible and do not include the indiscriminate retention of traffic or

	content data.
	The Commission shall amend the delegated act referred to in the first subparagraph where it identifies significant changes with regard to the necessity or specific purposes, or to the entities involved in, the processing personal data for the purposes of this Regulation.

Amendment 17

Proposal for a regulation
Article 18 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The handling of information by CERT-EU and its Union institutions, bodies and agencies shall be in line with ***the*** rules laid down in [proposed Regulation on information security].	4. The handling of information by CERT-EU and its Union institutions, bodies and agencies shall be in line with ***Union*** rules ***on information security, in particular those*** laid down in [proposed Regulation on information security].

Amendment 18

Proposal for a regulation
Article 18 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Any contacts with CERT-EU initiated or sought by national security and intelligence services shall be communicated to the Commission's Security Directorate and the chair of the IICB without undue delay.	5. Any contacts with CERT-EU initiated or sought by national security and intelligence services shall be communicated to the Commission's Security Directorate***, Europol*** and the chair of the IICB without undue delay.

Amendment 19

Proposal for a regulation
Article 19 – title

Text proposed by the Commission	*Amendment*
Sharing ***obligations***	***Information*** Sharing

Amendment 20

Proposal for a regulation
Article 19 – paragraph 1

Text proposed by the Commission	*Amendment*
1. ***To enable CERT-EU*** to coordinate vulnerability management and incident response, ***it may request*** Union institutions, bodies ***and*** agencies ***to*** provide ***it*** with information from their respective ***IT*** system inventories that is relevant for the CERT-EU support. The requested ***institution, body or agency*** shall transmit the requested information, and any subsequent updates thereto, without undue delay.	1. ***In order for CERT-EU to carry out the tasks set out in Article 12, in particular in order*** to coordinate vulnerability management and incident response, Union institutions, bodies ***or*** agencies ***shall, upon a request by CERT-EU,*** provide ***CERT-EU*** with information from their respective ***ICT*** system inventories that is relevant for the CERT-EU support***, including any changes to their IT environment***. The requested ***entity*** shall transmit the requested information, and any subsequent updates thereto, without undue delay. ***Without prejudice to Regulation (EU) 2018/1725, any sharing of data between CERT-EU and Union institutions, bodies, offices or agencies shall be carried out in line with the principles of clear safeguards for specific use-cases and shall use mutual legal assistance treaties and other agreements, in order to ensure a high level of protection for rights when processing requests for cross-border access to data.***

Amendment 21

Proposal for a regulation
Article 19 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. Union institutions, bodies, offices

	and agencies may voluntarily provide CERT-EU with information on cyber threats and incidents, near misses and vulnerabilities affecting them. They may also request CERT-EU for further technical assistance and advice to combat cybersecurity incidents and major attacks. CERT-EU may prioritise the processing of mandatory notifications over voluntary notifications, save in the case of duly substantiated and urgent voluntary requests by Union institutions, bodies, offices and agencies.

Amendment 22

Proposal for a regulation
Article 19 – paragraph 3

Text proposed by the Commission	*Amendment*
3. CERT-EU may only exchange incident-specific information which reveals the identity of the Union institution, body or agency affected by the incident with the ***consent*** of that entity. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the ***consent*** of the entity affected by the incident.	3. CERT-EU may only exchange incident-specific information which reveals the identity of the Union institution, body or agency affected by the incident with the ***authorisation*** of that entity. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the ***authorization*** of the entity affected by the incident. ***Where necessary for the carrying out of its tasks, CERT-EU may exchange incident-specific information, including in the absence of authorisation on the part of the Union institution, body, office or agency affected by the incident. The Union institution, body, office or agency shall be notified of any such exchange of information in advance.***

Amendment 23

Proposal for a regulation
Article 19 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The sharing obligations shall not extend to EU Classified Information (EUCI) and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency ***under the explicit condition that it will not*** be shared with CERT-EU.	4. The sharing obligations shall not extend to EU Classified Information (EUCI) and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency***, unless the Member State Security or Intelligence Service or law enforcement agency concerned allow that information to*** be shared with CERT-EU.

Amendment 24

Proposal for a regulation
Article 20 – paragraph 3

Text proposed by the Commission	*Amendment*
3. CERT-EU shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on significant cyber threats, significant vulnerabilities and significant incidents notified in accordance with paragraph 1.	3. CERT-EU shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on significant cyber threats, significant vulnerabilities and significant incidents notified in accordance with paragraph 1. ***That report shall be made public, subject to the relevant Union rules on information security, in particular those laid down in [proposed Regulation on information security].***

Amendment 25

Proposal for a regulation
Article 20 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The notification obligations shall not extend to EUCI and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency ***under the explicit condition that it***	5. The notification obligations shall not extend to EUCI and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency***, unless the Member State Security***

will not be shared with ***CERT-EU***.	***or Intelligence Service or law enforcement agency concerned allow that information to*** be shared with ***CERT-EU***.

Amendment 26

Proposal for a regulation
Article 21 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The IICB shall issue guidance on incident response coordination and cooperation for significant incidents. Where the criminal nature of an incident is suspected, CERT-EU shall ***advise on how to*** report the incident to law enforcement authorities.	4. The IICB shall issue guidance on incident response coordination and cooperation for significant incidents. Where the criminal nature of an incident is suspected, CERT-EU ***or the IICB*** shall report the incident to law enforcement authorities ***without undue delay***.

Amendment 27

Proposal for a regulation
Article 24 a (new)

Text proposed by the Commission	*Amendment*
	Article 24a
	Exercise of the delegation
	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
	2. The power to adopt delegated acts referred to in Article 18(3a) shall be conferred on the Commission for an indeterminate period of time from ... [one day after the date of entry into force of this Regulation].
	3. The delegation of power referred to in Article 18(3a) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the

European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 18(3a) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Amendment 28

Proposal for a regulation
Annex II – paragraph 1 – point 2 a (new)

Text proposed by the Commission	*Amendment*
	(2a) the use of encryption at rest, encryption in transit and end-to-end encryption where possible;

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
References	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Committee responsible Date announced in plenary	ITRE 4.4.2022
Opinion by Date announced in plenary	LIBE 4.4.2022
Associated committees - date announced in plenary	15.9.2022
Rapporteur for the opinion Date appointed	Tomas Tobé 12.12.2022
Discussed in committee	31.1.2023
Date adopted	1.3.2023
Result of final vote	+: 62 –: 0 0: 1
Members present for the final vote	Magdalena Adamowicz, Abir Al-Sahlani, Malik Azmani, Katarina Barley, Pietro Bartolo, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Karolin Braunsberger-Reinhold, Patrick Breyer, Saskia Bricmont, Patricia Chagnon, Caterina Chinnici, Clare Daly, Lena Düpont, Lucia Ďuriš Nicholsonová, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Erik Marquardt, Nuno Melo, Maite Pagazaurtundúa, Karlo Ressler, Diana Riba i Giner, Birgit Sippel, Sara Skyttedal, Vincenzo Sofo, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Yana Toom, Milan Uhrík, Tom Vandendriessche, Jadwiga Wiśniewska
Substitutes present for the final vote	Susanna Ceccardi, Gwendoline Delbos-Corfield, Loucas Fourlas, Beata Kempa, Philippe Olivier, Dragoş Tudorache, Petar Vitanov, Tomáš Zdechovský
Substitutes under Rule 209(7) present for the final vote	Gheorghe Falcă, Jean-François Jalkh, Petra Kammerevert, Marisa Matias, Martina Michels, Ljudmila Novak, Stanislav Polčák, Mick Wallace, Bernhard Zimniok

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

62	+
ECR	Patryk Jaki, Assita Kanko, Beata Kempa, Vincenzo Sofo, Jadwiga Wiśniewska
ID	Susanna Ceccardi, Patricia Chagnon, Jean-François Jalkh, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche, Bernhard Zimniok
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Karolin Braunsberger-Reinhold, Lena Düpont, Gheorghe Falcă, Loucas Fourlas, Andrzej Halicki, Jeroen Lenaers, Nuno Melo, Ljudmila Novak, Stanislav Polčák, Karlo Ressler, Sara Skyttedal, Tomas Tobé, Tomáš Zdechovský
Renew	Abir Al-Sahlani, Malik Azmani, Lucia Ďuriš Nicholsonová, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Ramona Strugariu, Yana Toom, Dragoş Tudorache
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Petra Kammerevert, Łukasz Kohut, Juan Fernando López Aguilar, Birgit Sippel, Petar Vitanov
The Left	Clare Daly, Marisa Matias, Martina Michels, Mick Wallace
Verts/ALE	Patrick Breyer, Saskia Bricmont, Gwendoline Delbos-Corfield, Alice Kuhnke, Erik Marquardt, Diana Riba i Giner, Tineke Strik

0	-

1	0
NI	Milan Uhrík

Key to symbols:
+ : in favour
- : against
0 : abstention