European Parliament
2019-2024

Committee on Industry, Research and Energy

2020/0359(COD)

3.6.2021

AMENDMENTS
363 - 600

Draft report
Bart Groothuis
(PE692.602v01-00)

Measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

Proposal for a directive
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Amendment 363
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 15 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. ENISA shall issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union. The report shall in particular include an assessment of the following:	1. ENISA shall issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union. The report shall ***be delivered in machine-readable format and shall*** in particular include an assessment of the following:

Or. en

Justification

Ensuring digital accessibility

Amendment 364
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 15 – paragraph 1 – point a a (new)

Text proposed by the Commission	*Amendment*
	(aa) the general level of cybersecurity awareness amongst citizens and consumers, the security of consumer-facing connected devices, and the security of digital public services and the respective digital infrastructures through which such services are offered to citizens;

Or. en

Justification

ENISA's report on the state of cybersecurity in the Union is an appropriate platform to assess the level of cybersecurity awareness of consumers and citizens, and the security levels of

consumer-facing connected devices and digital public services, and the respective infrastructures, offered to citizens.

Amendment 365
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 15 – paragraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) the technical, financial and human resources available to competent authorities and cybersecurity policies***, and the implementation of supervisory measures and enforcement actions in light of the outcomes of peer reviews referred to in Article 16***;	(b) the technical, financial and human resources available to competent authorities and cybersecurity policies;

Or. en

Amendment 366
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 15 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) a cybersecurity index providing for an aggregated assessment of the maturity level of cybersecurity capabilities.	(c) a cybersecurity index providing for an aggregated assessment of the maturity level of ***Union's*** cybersecurity capabilities.

Or. en

Justification

The index should be for the Union as a whole, and not Member State by Member State.

Amendment 367
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 15 – paragraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) an overview of the general level of cybersecurity awareness and use amongst citizens as well as on the general level of security of consumer-oriented connected devices put on the market in the Union.

Or. en

Justification

It is imperative to cover all risks and vulnerabilities.

Amendment 368
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 15 – paragraph 1 – point c b (new)

Text proposed by the Commission	*Amendment*
	(cb) the alignment of Member States' national cybersecurity strategies referred to in Article 5, including the level of convergence of key performance indicators for the assessment of the strategies.

Or. en

Justification

ENISA's report on the state of cybersecurity in the Union should also assess the level of convergence among Member States' national cybersecurity strategies to evaluate the overall alignment of strategic objectives identified at the national level, and the resulting policies adopted by Member States.

Amendment 369
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand,

Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 15 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The report shall include particular policy recommendations for increasing the level of cybersecurity across the Union and a summary of the findings for the particular period from the Agency's EU Cybersecurity Technical Situation Reports issued by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.	2. The report shall include ***the obstacles identified at the national level,*** particular policy recommendations for increasing the level of cybersecurity across the Union**,** and a summary of the findings for the particular period from the Agency's EU Cybersecurity Technical Situation Reports issued by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.

Or. en

Justification

ENISA's report on the state of cybersecurity in the Union can enable the identification of obstacles at the national level, enabling a better understanding of the gaps identified at the national level and focusing the resulting policy recommendations to targeted areas.

Amendment 370
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 15 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. ENISA, in cooperation with the Commission and with guidance from the Cooperation Group and the CSIRTs network, shall prepare the methodological specifications, including the relevant variables underpinning the scoring and validation of the cybersecurity index referred to in paragraph 1(e).

Or. en

Justification

A methodological specification is necessary to underpin the construction of the cybersecurity index to assess the level of maturity of cybersecurity capabilities.

Amendment 371
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 16

Text proposed by the Commission	*Amendment*
[...]	***deleted***

Or. en

Amendment 372
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 16 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. The Commission shall establish, after consulting the Cooperation Group and ENISA, and at the latest by 18 months following the entry into force of this Directive, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The reviews shall be conducted by cybersecurity technical experts drawn from Member States different than the one reviewed and shall cover at least the following:	1. The Commission shall establish, after consulting the Cooperation Group and ENISA, and at the latest by 18 months following the entry into force of this Directive, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. ***ENISA shall develop templates for the self-assessment of the reviewed aspects, which Member States being reviewed shall complete and provide to designated experts prior to the commencement of the peer-review process.*** The reviews shall be conducted by cybersecurity technical experts drawn from ***ENISA and at least two*** Member States different than the one reviewed and shall cover at least the following:

Or. en

Justification

A self-assessment process prior to the commencement of the peer-review process will provide more agency to the Member State under review, and enable the Member State under review and the designated experts from the Member States and ENISA performing the peer-review to compare findings and improve Member States' evaluation processes.

Amendment 373
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 16 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. The Commission shall establish, after consulting the Cooperation Group and ENISA, and at the latest by 18 months following the entry into force of this Directive, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The reviews shall be conducted by cybersecurity technical experts drawn from Member States different than the one reviewed and shall cover at least the following:	1. The Commission shall establish, after consulting the Cooperation Group and ENISA, and at the latest by 18 months following the entry into force of this Directive, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The reviews shall be conducted by cybersecurity technical experts drawn from Member States different than the one reviewed***, in consultation with ENISA,*** and shall cover at least the following:

Or. en

Amendment 374
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 16 – paragraph 1 – point iii

Text proposed by the Commission	*Amendment*
(iii) the ***operational*** capabilities and effectiveness of CSIRTs;	(iii) the ***technical*** capabilities and effectiveness of CSIRTs ***in executing their***

tasks;

Or. en

Amendment 375
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 16 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The methodology shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States shall designate experts eligible to carry out the peer reviews. ENISA and the Commission shall designate experts to participate as observers in the peer-reviews. The Commission, supported by ENISA, shall establish within the methodology as referred to in paragraph 1 an objective, non-discriminatory, fair and transparent system for the selection and the random allocation of experts for each peer review.	2. The methodology shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States shall designate experts eligible to carry out the peer reviews***. The Commission, supported by ENISA, shall develop appropriate codes of conduct underpinning the work methods of designated experts participating in peer-reviews to safeguard the confidentiality of information obtained through the peer-review process, and the non-disclosure of such information to any third parties***. ENISA and the Commission shall designate experts to participate as observers in the peer-reviews. The Commission, supported by ENISA, shall establish within the methodology as referred to in paragraph 1 an objective, non-discriminatory, fair and transparent system for the selection and the random allocation of experts for each peer review.

Or. en

Justification

Appropriate codes of conduct are necessary to pre-emptively safeguard the confidentiality of the information obtained through the peer-review process.

Amendment 376

Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 16 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Peer reviews shall entail actual or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, the Member States being reviewed shall provide the designated experts with the requested information necessary for the assessment of the reviewed aspects. Any information obtained through the peer review process shall be used solely for that purpose. ***The experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that review to any third parties.***	4. Peer reviews shall entail actual or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, ***the designated experts tasked with carrying out the peer-review shall communicate the aspects under review as referred to in paragraph 1, including any additional targeted issues specific to the Member State or sectors referred to in paragraph 3, and request a corresponding self-assessment report from the Member States being reviewed.*** The Member States being reviewed shall provide the designated experts with the requested information necessary for the assessment of the reviewed aspects. Any information obtained through the peer review process shall be used solely for that purpose.

Or. en

Justification

In line with the principle of good cooperation, the Member State under review should receive a communication laying out the items to be reviewed by the designated experts.

Amendment 377
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 16 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Once reviewed in a Member State, the same aspects shall not be subject to further peer review within that Member State during the two years following the	5. Once reviewed in a Member State, the same aspects shall not be subject to further peer review within that Member State during the two years following the

conclusion of a peer review, unless otherwise decided by the ***Commission,*** upon consultation with ***ENISA and the Cooperation Group***.	conclusion of a peer review, unless otherwise decided by the ***Cooperation Group*** upon consultation with ***the Commission and ENISA***.

Or. en

Amendment 378
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 16 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Member ***State*** shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Member States, the Commission and ENISA ***without undue delay***.	6. Member ***States*** shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Member States, the Commission and ENISA***, before the designation of experts referred to in paragraphs 1 and 2***.

Or. en

Justification

Any conflicts of interest must be resolved before the designation of experts participating in the peer-review process.

Amendment 379
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 16 – paragraph 7

Text proposed by the Commission	*Amendment*
7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. The reports shall be submitted to the Commission, the	7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews***. The reports shall include recommendations to***

Cooperation Group, the CSIRTs network and ENISA. The reports shall be discussed in the Cooperation Group and the CSIRTs network. The reports may be published on the dedicated website of the Cooperation Group.	***enable improvement on the aspects covered by the peer-review process, including recommendations on the transfer of technologies, tools, measures, and processes from Member States carrying out the peer-review to the Member State being reviewed***. The reports shall be submitted to the Commission, the Cooperation Group, the CSIRTs network and ENISA. The reports shall be discussed in the Cooperation Group and the CSIRTs network. The reports may be published on the dedicated website of the Cooperation Group.

Or. en

Justification

Peer-review reports should include specific recommendations on the transfer of technologies and related policies and practices from the designated experts carrying out the peer-review process in order to enable Member States being reviewed to take advantage of innovations and solutions employed by more mature competent authorities or CSIRTs.

Amendment 380
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 16 – paragraph 7

Text proposed by the Commission	*Amendment*
7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. The reports shall be submitted to the Commission, the Cooperation Group, the CSIRTs network and ENISA. The reports shall be discussed in the Cooperation Group and the CSIRTs network. ***The reports may be published on the dedicated website of the Cooperation Group.***	7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. The reports shall be submitted to the Commission, the Cooperation Group, the CSIRTs network and ENISA. The reports shall be discussed in the Cooperation Group and the CSIRTs network.

Or. en

Amendment 381
Eva Maydell, Massimiliano Salini

Proposal for a directive
Article 16 – paragraph 7 a (new)

Text proposed by the Commission	*Amendment*
	7a. The Commission will review the peer-review system taking into account the implementation in Member States. In case of misalignment of the implementations at national level, intervention plans that address existing differences are needed.

Or. en

Amendment 382
Tsvetelina Penkova

Proposal for a directive
Article 17 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.	1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article. ***Those measures shall non-exhaustively include an appropriate deployment of state-of-the-art products, services and processes for the resilience of the entity's network and information systems.***

Or. en

Amendment 383
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand,

Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 17 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.	2. Member States shall ensure that members of the management body ***of essential and important entities*** follow specific trainings***, and shall encourage essential and important entities to offer similar trainings to all employees***, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.

Or. en

Justification

Cybersecurity trainings should be offered to all relevant employees within an entity, and not only to the management body, in order to build a more comprehensive culture of cybersecurity.

Amendment 384
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 17 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the ***operations of*** the entity.	2. Member States shall ensure that members of the management body ***of essential and important entities*** follow specific trainings, ***where possible*** on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the ***services provided by*** the entity.

Or. en

Amendment 385
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 18 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.	1. Member States shall ensure that essential and important entities***, including ICT suppliers providing products and services for critical functions performed by essential or important entities,*** shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented. ***ICT suppliers shall bear sole liability for non-compliance by providers of essential or important functions with the obligations under this article unless such non-compliance was known to and disregarded by the commissioning authority concerned.***

Or. fr

Amendment 386
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 18 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and	1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and

information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.	information systems which those entities use in the provision of their services ***and to prevent or minimise the impact of incidents on recipients of their services and on other services***. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented***, and differentiate between the essential and important entities and between the sectors and subsectors with higher or lower level of criticality referred to in Annexes I and II***.

Or. en

Amendment 387
Eva Maydell, Massimiliano Salini

Proposal for a directive
Article 18 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.	1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. ***The corrective measures should be appropriate and proportionate in terms of time and effort, according to risk analysis.*** Having regard to the state of the art ***and to international standards (such as ISO31000 and ISA/IEC 27005)***, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.

Or. en

Amendment 388
François-Xavier Bellamy

Proposal for a directive
Article 18 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.	1. Member States shall ensure that essential and important entities***, including manufacturers and providers of ICT products,*** shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.

Or. en

Amendment 389
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 18 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities ***shall*** take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use ***in*** the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.	1. Member States shall ensure that essential and important entities take appropriate and proportionate technical***, operational*** and organisational measures to manage the risks posed to the security of network and information systems which those entities use ***for their operations or for*** the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.

Or. en

Justification

Cybersecurity risk management measures to be applicable not only to provision of entities' services but also for their operations overall.

Amendment 390
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 18 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) risk analysis and information system security policies;	(a) risk analysis and information system security policies ***in connection with critical network and information system functions***;

Or. fr

Amendment 391
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 18 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) incident handling (prevention, detection, ***and*** response to incidents);	(b) incident handling (prevention, detection, ***mitigation,*** response to***, recovery from, and attribution of*** incidents);

Or. en

Amendment 392
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 18 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) incident handling (prevention, detection, ***and*** response to incidents);	(b) incident handling (prevention, detection, ***containment,*** response to***, and mitigation of*** incidents);

Or. en

Amendment 393
Evžen Tošenovský

Proposal for a directive
Article 18 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) incident ***handling (***prevention, detection, and response to incidents);	(b) incident ***management (including*** prevention, detection, and response to incidents);

Or. en

Amendment 394
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 18 – paragraph 2 – point c

Text proposed by the Commission	*Amendment*
(c) business continuity and crisis management;	(c) business continuity***, disaster recovery*** and crisis management;

Or. en

Justification

Business continuity focuses on keeping business operational during a disaster, while disaster recovery focuses on restoring data access and IT infrastructure after a disaster.

Amendment 395

Christophe Grudler, Klemen Grošelj, Nathalie Loiseau, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

Proposal for a directive
Article 18 – paragraph 2 – point c

Text proposed by the Commission	*Amendment*
(c) business continuity and crisis management;	(c) ***backup management,*** business continuity and crisis management;

Or. en

Justification

Entities should have a solid system of backup management in order to have business continuity.

Amendment 396
Tsvetelina Penkova

Proposal for a directive
Article 18 – paragraph 2 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) where relevant, multi-factor authentication and/or continuous authentication solutions;

Or. en

Amendment 397
Christophe Grudler, Klemen Grošelj, Valérie Hayer

Proposal for a directive
Article 18 – paragraph 2 – point d

Text proposed by the Commission	*Amendment*
(d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers ***such as providers of data storage and processing***	(d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers;

services or managed security services;

Or. en

Justification

It is inopportune to mention here a specific category of providers, as it could be too limitative.

Amendment 398
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 18 – paragraph 2 – point f

Text proposed by the Commission	*Amendment*
(f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;	(f) policies and procedures (***training,*** testing and auditing) to assess the effectiveness of cybersecurity risk management measures;

Or. en

Amendment 399
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 18 – paragraph 2 – point f a (new)

Text proposed by the Commission	*Amendment*
	(fa) deployment of secured voice, video and text communications, and of secured emergency communications systems within the entity;

Or. en

Justification

Secured communications systems improves the level of robustness and increases the resilience of entities falling in scope of this Directive.

Amendment 400
Tsvetelina Penkova

Proposal for a directive
Article 18 – paragraph 2 – point f b (new)

Text proposed by the Commission	*Amendment*
	(fb) periodic compromise assessments of the entity's network, infrastructure and devices;

Or. en

Amendment 401
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 18 – paragraph 2 – point g

Text proposed by the Commission	*Amendment*
(g) the use of cryptography and encryption.	(g) ***support*** the use of cryptography and encryption***, where appropriate***.

Or. en

Amendment 402
Evžen Tošenovský

Proposal for a directive
Article 18 – paragraph 2 – point g

Text proposed by the Commission	*Amendment*
(g) the use of cryptography and encryption.	(g) the use of cryptography and encryption ***where appropriate***.

Or. en

Amendment 403

Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 18 – paragraph 2 – point g

Text proposed by the Commission	*Amendment*
(g) the use of cryptography and encryption.	(g) the use***, where appropriate,*** of cryptography and encryption.

Or. fr

Amendment 404
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 18 – paragraph 2 – point g

Text proposed by the Commission	*Amendment*
(g) the use of cryptography and encryption.	(g) the use of cryptography and ***strong*** encryption.

Or. en

Justification

We need to support investment in state of the art technology

Amendment 405
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 18 – paragraph 2 – point g a (new)

Text proposed by the Commission	*Amendment*
	(ga) wide adoption of basic computer hygiene practices such as software updates, device configuration, network segmentation, identity and access management or user awareness and training regarding corporate email cyber threats, phishing or social engineering

techniques.

Or. en

Amendment 406
Tsvetelina Penkova

Proposal for a directive
Article 18 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the ***vulnerabilities specific to each supplier and service provider and the*** overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.

Or. en

Justification

Mandating large-scale vulnerability assessments of all suppliers and service providers could increase the risk exposure as such information should be disclosed on a need-to-know basis and after the identified vulnerabilities have been patched/ corrected. Widespread disclosure of such vulnerabilities would equal to handling the guidebook on how to exploit them.

Amendment 407
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 18 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and	3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each ***first-level***

service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	supplier and service provider and the overall quality of products and cybersecurity practices of their ***first-level*** suppliers and service providers, including their secure development procedures.

Or. en

Justification

As part of their cybersecurity risk management measures entities should focus on the first-level suppliers; for the second-, third-, n-level the entities should use contractual means to ensure that suppliers are accountable and responsible for breaching commitments including security of products.

Amendment 408
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 18 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall***, without undue delay,*** take all necessary corrective measures to bring the service concerned into compliance.	4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall take all necessary corrective measures to bring the service concerned into compliance ***within a reasonable period and in line with their own interests***.

Or. fr

Amendment 409
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 18 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. In order to promote the convergent implementation of paragraph 1 and 2, Member States shall be in accordance

with Article 12(4) assisted by the Cooperation Group, and shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

Or. en

Amendment 410
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 18 – paragraph 4 b (new)

Text proposed by the Commission	*Amendment*
	4b. ENISA, in collaboration with Member States and industry, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraphs 1 and 2 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.

Or. en

Amendment 411
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 18 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in	***deleted***

accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.

Or. en

Amendment 412
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera, Markus Pieper

Proposal for a directive
Article 18 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow***, to the greatest extent possible,*** international ***and European*** standards, as well as relevant technical specifications.	5. ***ENISA, in collaboration with Member States shall draw up advice and guidelines regarding the technical and methodological specifications areas to be considered in relation to paragraph 2.*** The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow ***European and*** international standards, as well as relevant technical specifications. ***In developing implementing acts, the Commission shall also consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process.***

Or. en

Amendment 413
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 18 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission may adopt ***implementing*** acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the ***examination procedure referred to in*** Article ***37(2)*** and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.	5. The Commission may adopt ***delegated*** acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the Article ***36*** and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.

Or. en

Amendment 414
Tsvetelina Penkova

Proposal for a directive
Article 18 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission may adopt ***implementing*** acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.	5. The Commission may adopt ***delegated*** acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.

Or. en

Justification

A delegated act procedure will add further transparency as the European Parliament will be consulted for the approval process.

Amendment 415
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 18 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission may adopt ***implementing*** acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.	5. The Commission may adopt ***delegated*** acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.

Or. fr

Amendment 416
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 18 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.	***deleted***

Or. en

Amendment 417
Eva Maydell, Massimiliano Salini

Proposal for a directive
Article 18 – paragraph 6 a (new)

Text proposed by the Commission	*Amendment*

6a. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, they will always seek harmonisation at EU level.

Or. en

Amendment 418
Tsvetelina Penkova

Proposal for a directive
Article 18 a (new)

Text proposed by the Commission	*Amendment*
	Article 18a
	Cybersecurity risk management capabilities
	Member States shall ensure that entities referred to in Annex I and Annex II have the capabilities to implement the requirements of Article 18 by:
	1. Prepare and identify pursuant to Article 18(2)(a):
	(a) maintain records of essential or important functions and network and information systems supporting them, including their interdependencies within an entity and into the supply chain. Have a process in place to regularly review and update;
	(b) have a process in place to regularly perform or commission a comprehensive risk or compromise assessment and to identify risk and assess cyber threats and vulnerabilities on networks and information systems.
	2. Protect, detect and defend pursuant to Article 18(2)(b):
	(a) use appropriate tools to real-time monitor networks and information systems to effectively detect malfunctions and cyber threats and mitigate their

impact;

(b) ensure resilience, continuity, confidentiality, integrity, availability and authenticity of network and information systems and associated access rights, including where appropriate, by protecting data from exfiltration or other forms of interference both at rest and in transit using appropriate technical and organizational controls and risk assessment procedures;

(c) have the processes and capabilities in place to dynamically adjust the risk mitigation measures and efforts to the cyber threats and incidents as they occur;

(d) have mechanisms in place that enable different layers of technical and organizational controls and criteria that activate actions pursuant to Article18(2)(b) of this Directive taking into account the risk.

3. Recover pursuant to Article 18(2)(c):

(a) have processes and tools in place to enable timely processing and resolution of incidents while prioritizing and mitigating risks;

(b) have processes and tools in place to enable dedicated plans to contain, recover from cyber threats and accidental incidents and ensure service continuity;

(c) test regularly the efficacy of the measures foreseen pursuant to Article 18(2)(c);

(d) maintain a record of all incidents having a significant impact on the provision of the service, and proper procedures for timely notifying the management body of the entity of such incidents.

To the extent relevant, the processes described in this article may be constituted by processes established pursuant to Article 28, 30 and 32 of

Regulation (EU) 2016/679.

Or. en

Amendment 419
Christophe Grudler, Klemen Grošelj, Nathalie Loiseau, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

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

Text proposed by the Commission	*Amendment*
	1a. To identify the specific critical ICT services, systems or products supply chains that are subject to a coordinated risk assessment, the following criteria shall be taken into account:
	(a) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products;
	(b) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data;
	(c) the availability of alternative ICT services, systems or products;
	(d) the resilience of the overall supply chain of ICT services, systems or products against disruptive events; and
	(e) the potential significance to entities' activities of emerging ICT services, systems or products.

Or. en

Justification

Moved from Recital 47

Amendment 420
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 19 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission, after consulting with the Cooperation Group ***and*** ENISA, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.	2. The Commission, after consulting with the Cooperation Group***,*** ENISA ***and the industry***, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.

Or. en

Amendment 421
Eva Maydell, Massimiliano Salini

Proposal for a directive
Article 19 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission, after consulting with the Cooperation Group and ENISA, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.	2. The Commission, after consulting with the Cooperation Group and ENISA, shall identify the specific critical ICT ***and ICS*** services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.

Or. en

Amendment 422
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 19 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria shall be taken into account:
	(a) the extent to which essential and important entities use and rely on specific

critical ICT services, systems or products;

(b) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data;

(c) the availability of alternative ICT services, systems or products;

(d) the resilience of the overall supply chain of ICT services, systems or products against disruptive events;

(e) for emerging ICT services, systems or products, their potential future significance for the entities' activities.

Or. en

Amendment 423
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 19 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. The Stakeholder Cybersecurity Certification Group as per pursuant to Article 22 of Regulation (EU) 2019/881 shall issue an opinion on security risk assessments of specific critical ICT services, systems or products supply chains and the opinion shall be taken into account by the Cooperation Group and ENISA when it develops and executes an EU coordinated risk assessment of critical supply chain.

Or. en

Amendment 424
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs ***3 and 4*** of any incident having a significant impact ***on the provision of their*** services***. Where appropriate***, those entities shall notify***, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that*** service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.	1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs ***2 and 3*** of any incident having a significant impact***. Where the incident concerns the provisions of entities'*** services, those entities shall notify ***affected users about the unavailability or underlying risks of use of the*** service ***in order to mitigate the adverse effects of the incident. Essential and important entities may deviate from notifying affected users in case of overriding reasons inducing, but not limited to, that notification worsening the impact of an ongoing incident***. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident. ***The notification shall not make the notifying entity subject to increased liability.***

Or. en

Justification

The default rule should be that affected users should be notified immediately about the reason behind the unavailability of their services. Such notification should include information that would allow them to mitigate the adverse effects of the cyberattack.

Amendment 425
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that	1. Member States shall ensure that

essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. ***Where appropriate,*** those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.	essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service ***and provide information that would enable them to mitigate the adverse effects of the cyberattacks. By exception, where public disclosure could trigger further cyberattacks, essential and important entities, could delay the notification***. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.

Or. en

Justification

Change of logic, from a subjective assessment to disclosure as rule, with limited exception.

Amendment 426
Christophe Grudler, Klemen Grošelj, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact ***on the provision of their services***. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that	1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that

service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.	those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident. ***Where the competent authorities or the CSIRT consider that it is necessary, essential and important entities may notify other essential and important entities of any significant incident occurring in their sector.***

Or. en

Justification

Informing entities of the same sector in case of a major event could help them to better prepare themselves if the incident is ultimately broader than envisaged initially.

Amendment 427
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities notify**,** ***without undue delay,*** the competent authorities ***or*** the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.	1. Member States shall ensure that essential and important entities notify the ***relevant*** competent authorities ***and*** the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services ***('significant incident')***. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.

Or. en

Amendment 428
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents ***that are likely to adversely affect the provision of that service***. Member States shall ensure that those entities report, among others, ***any*** information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.	1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents ***with a confirmed substantial impact***. Member States shall ensure that those entities report, among others, ***the relevant*** information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.

Or. fr

Amendment 429
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident. ***Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of***	***deleted***

any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.

Or. en

Amendment 430
Eva Maydell, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 2 – subparagraph 1

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.	***deleted***

Or. en

Amendment 431
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 2 – subparagraph 1

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.	***deleted***

Or. en

Amendment 432
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 20 – paragraph 2 – subparagraph 1

Text proposed by the Commission	*Amendment*
Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that ***those entities identify that could have potentially*** resulted in a significant incident.	Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that***, if steps to mitigate the risk had not been taken or are not taken in the future, would have*** resulted ***or are likely in the future to result*** in a significant incident.

Or. en

Justification

The use of potentiality as a criteria was a potential loophole that needs fixing.

Amendment 433
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 2 – subparagraph 2

Text proposed by the Commission	*Amendment*
Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not	***deleted***

make the notifying entity subject to increased liability.

Or. en

Amendment 434
Eva Maydell, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 2 – subparagraph 2

Text proposed by the Commission	*Amendment*
Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.	***deleted***

Or. en

Amendment 435
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 20 – paragraph 2 – subparagraph 2

Text proposed by the Commission	*Amendment*
Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying	Those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. ***By exception, where public disclosure could trigger further attacks***

entity subject to increased liability.	***against information systems, essential and important entities, could delay the notification.*** The notification shall not make the notifying entity subject to increased liability.

Or. en

Justification

Change of logic, from a subjective assessment to disclosure as rule, with limited exception.

Amendment 436
Tsvetelina Penkova

Proposal for a directive
Article 20 – paragraph 2 – subparagraph 2

Text proposed by the Commission	*Amendment*
Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability**.**	Where applicable ***and in respect to their contractual arrangements***, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability

Or. en

Amendment 437
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 3

Text proposed by the Commission	*Amendment*
3. An incident shall be considered significant if:	***deleted***

(a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned;

(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.

Or. en

Amendment 438
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 20 – paragraph 3 – point b

Text proposed by the Commission	*Amendment*
(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.	(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses. ***Non-material losses shall include:***

Or. fr

Amendment 439
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 20 – paragraph 3 – point b – point i (new)

Text proposed by the Commission	*Amendment*
	(i) a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or of the related services offered by an essential or important entity or accessible via a network and an information system;

Or. fr

Amendment 440
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 20 – paragraph 3 – point b – point ii (new)

Text proposed by the Commission	*Amendment*
	(ii) a risk to public safety and security or loss of life.

Or. fr

Amendment 441
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. Member States shall ensure that in order to determine the significance of the individual incident, where available, the following parameters shall, in particular, be taken into account:
	(a) the number of the recipients of the services affected by the incident;
	(b) the duration of the incident;
	(c) the geographical spread of the area affected by the incident;
	(d) the extent to which the functioning and continuity of the service is affected;
	(e) the extent of impact, including financial, on economic and societal activities of the entity directly concerned, of other entities or on national security.

Or. en

Amendment 442
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 3 b (new)

Text proposed by the Commission	*Amendment*
	3b. Member States shall establish a single entry point for notifications required from essential and important entities under paragraph 1, and where relevant also for other notifications under this Directive and under other relevant Union law, and decide on which authorities shall receive the notifications and the scope of the information provided for each authority, including for the purpose of information sharing pursuant to paragraphs 7a, 8a and 8b of this Article.

Or. en

Amendment 443
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – introductory part

Text proposed by the Commission	*Amendment*
4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to ***the*** competent ***authorities*** or the CSIRT:	4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to ***a*** competent ***authority*** or the CSIRT:

Or. fr

Amendment 444
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – introductory part

Text proposed by the Commission	*Amendment*
4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities ***or*** the CSIRT:	4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities ***and*** the CSIRT:

Or. en

Amendment 445
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point -a (new)

Text proposed by the Commission	*Amendment*
	(-a) an early warning within 24 hours after having become aware of an incident, without any obligations on the entity concerned to disclose additional information regarding the incident;

Or. en

Amendment 446
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) without undue delay and in any event within ***24*** hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;	(a) without undue delay and in any event within ***72*** hours after having become aware ***of the confirmed impact*** of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;

Or. fr

Amendment 447
Eva Maydell, Markus Pieper, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) without undue delay and in any event ***within 24*** hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;	(a) without undue delay and in any event ***no later than 72*** hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;

Or. en

Amendment 448
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) without undue delay and in any event within ***24*** hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;	(a) without undue delay and in any event within ***72*** hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;

Or. en

Justification

Aligning the notification timeline with the timeline provided in Regulation (EU) 2016/679 can harmonise the notification process and avoid double reporting in cases where the incident involves personal data. Moreover, a 72-hour notification timeline allows entities to invest resources in dealing with the incident and gain a better understanding of the incident in order to provide more detailed information to the competent authority of CSIRT.

Amendment 449
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) without undue delay ***and in any event within 24 hours*** after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;	(a) without undue delay after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;

Or. en

Amendment 450
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) upon the request of a competent authority or a CSIRT, an intermediate ***report*** on relevant status updates;	(b) upon the request of a competent authority or a CSIRT, ***without undue delay*** an intermediate ***information*** on relevant status updates;

Or. en

Amendment 451
Eva Maydell, Markus Pieper, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point c – introductory part

Text proposed by the Commission	*Amendment*
(c) a ***final*** report not later than ***one month*** after the submission of the ***report***	(c) a ***status*** report not later than ***three months for an essential entity and no later***

under point (a), including at least the following:	***than four months for an important entity*** after the submission of the ***initial notification*** under point (a), including at least the following:

Or. en

Amendment 452
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point c – introductory part

Text proposed by the Commission	*Amendment*
(c) a ***final*** report not later than one month after the submission of the report under point (a), including at least the following:	(c) a ***detailed incident*** report not later than one month after the submission of the report under point (a), including at least the following:

Or. en

Amendment 453
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point c – introductory part

Text proposed by the Commission	*Amendment*
(c) a ***final*** report not later than one month after the submission of the report under point (a), including at least the following:	(c) a ***comprehensive*** report not later than one month after the submission of the report under point(a), including at least the following:

Or. en

Justification

Cybersecurity incidents may last for a longer period. Hence, a comprehensive report is more fitting than a final one given that certain incidents may require considerable more time to be fully handled, for the report thereof to be considered final.

Amendment 454
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point c – introductory part

Text proposed by the Commission	*Amendment*
(c) ***a final*** report ***not later than one month*** after the submission of the report under point (a), including at least the following:	(c) ***an exhaustive*** report after the submission of the report under point (a), including at least the following:

Or. fr

Amendment 455
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point c – point i

Text proposed by the Commission	*Amendment*
(i) a detailed description of the incident, its severity and impact;	(i) a detailed description of the ***confirmed*** incident, its severity and impact;

Or. fr

Amendment 456
Eva Maydell, Markus Pieper, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) a final report should be drawn up one month after the incident had been mitigated.

Or. en

Justification

It provides flexibility for both essential and important entities for incidents that take longer time to be handled.

Amendment 457
Eva Maydell, Markus Pieper, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	Member States may establish a single entry point for all notifications required under this Directive, the Regulation (EU) 2016/679, Directive2002/58/EC and sector specific legislation.

Or. en

Amendment 458
Eva Maydell, Markus Pieper, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 b (new)

Text proposed by the Commission	*Amendment*
	ENISA, in cooperation with the Cooperation Group, should develop common notification templates by means of guidelines to streamline the reporting information requested by this Directive and decrease the burdens for reporting entities.

Or. en

Amendment 459
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 1 c (new)

Text proposed by the Commission	*Amendment*
	Member States shall ensure confidentiality and appropriate protections around sensitive information about incidents shared with competent authorities, and enact parameters around how incident information is further shared and reused.

Or. en

Amendment 460
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 20 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. When processing notifications, the competent authorities and the CSIRT shall, taking into account their available capacity, prioritise the processing of notifications from essential entities over those from important entities and processing of mandatory notifications from essential and important entities over the voluntary notifications pursuant to Article 27.

Or. en

Amendment 461
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 5

Text proposed by the Commission	*Amendment*

5. The competent national authorities or the CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures. Where the CSIRT did not receive the notification referred to in paragraph 1 , the guidance shall be provided by the competent authority in collaboration with the CSIRT. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.	5. The competent national authorities or the CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance ***and actionable advice*** on the implementation of possible mitigation measures. Where the CSIRT did not receive the notification referred to in paragraph 1, the guidance ***and actionable advice*** shall be provided by the competent authority in collaboration with the CSIRT. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.

Or. en

Amendment 462
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 5

Text proposed by the Commission	*Amendment*
5. ***The competent national authorities or*** the CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures***. Where the CSIRT did not receive the notification referred to in paragraph 1, the guidance shall be provided by the competent authority in collaboration with the CSIRT***. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the	5. The CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident***, particularly whether they deem it significant,*** and, upon request of the entity, guidance on the implementation of possible mitigation measures. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement

incident is suspected to be of criminal nature, the competent ***national*** authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.	authorities. ***Where the incident is suspected to be of nature breaching the national security, the competent authorities or the CSIRT shall without undue delay inform relevant national authorities.***

Or. en

Amendment 463
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The competent national authorities or the CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point ***(a)*** of paragraph ***4***, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures. Where the CSIRT did not receive the notification referred to in paragraph 1 , the guidance shall be provided by the competent authority in collaboration with the CSIRT. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.	5. The competent national authorities or the CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point ***(b)*** of paragraph ***3***, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures. Where the CSIRT did not receive the notification referred to in paragraph 1, the guidance shall be provided by the competent authority in collaboration with the CSIRT. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.

Or. en

Justification

Consistency with changes introduced to the text of the Directive.

Amendment 464
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Nicola Danti, Christophe Grudler

Proposal for a directive
Article 20 – paragraph 5 a (new)

Text proposed by the Commission	*Amendment*
	5a. Member States shall establish a single entry point for all notifications required under this Directive.

Or. en

Justification

From recital 56.

Amendment 465
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Nicola Danti, Christophe Grudler, Martina Dlabajová

Proposal for a directive
Article 20 – paragraph 5 b (new)

Text proposed by the Commission	*Amendment*
	5b. ENISA, in cooperation with the Cooperation Group, shall develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law.

Or. en

Justification

From recital 56; to decrease the administrative burdens for companies.

Amendment 466
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.	6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform ***without undue delay*** the other affected Member States and ENISA of the incident. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

Or. en

Amendment 467
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 7

Text proposed by the Commission	*Amendment*
7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may***, after consulting*** the entity ***concerned,*** inform the public about the incident ***or require the entity to do so***.	7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may ***require*** the entity ***to*** inform the public about the incident.

Or. en

Amendment 468
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive

Article 20 – paragraph 7

Text proposed by the Commission	*Amendment*
7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.	7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public ***on a mutual basis*** about the incident or require the entity to do so.

Or. fr

Amendment 469
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 20 – paragraph 7

Text proposed by the Commission	*Amendment*
7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned ***may***, after consulting the entity concerned, inform the public about the incident or require the entity to do so.	7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned ***shall***, after consulting the entity concerned, inform the public about the incident or require the entity to do so.

Or. en

Justification

Where public awareness is necessary the MS cannot have the option to not inform the public. The assessment is done when one qualifies the public awareness as "necessary".

Amendment 470
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 20 – paragraph 7 a (new)

Text proposed by the Commission	*Amendment*
	7a. Competent authorities or the CSIRTs shall provide without undue delay to the single point of contact information on significant incidents notified in accordance with paragraph 1.

Or. en

Amendment 471
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 8

Text proposed by the Commission	*Amendment*
8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to ***paragraphs 1 and 2*** to the single points of contact of other affected Member States.	8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to ***paragraph 1*** to the single points of contact of other affected Member States. ***In compliance with Union law, or in accordance with Member State legislation compliant with Union law, the single point of contact shall preserve the security and commercial interests of the essential or important entity reporting the incident, including the confidentiality of the information provided by the reporting entity in the notification of the incident, when forwarding the notification to the single points of contact of other affected Member States.***

Or. en

Amendment 472
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 20 – paragraph 8

Text proposed by the Commission	*Amendment*
8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to ***paragraphs 1 and 2*** to the single points of contact of other affected Member States.	8. At the request of the competent authority or the CSIRT, the single point of contact shall forward ***without undue delay*** notifications received pursuant to ***paragraph 1*** to the single points of contact of other affected Member States.

Or. en

Amendment 473
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 8

Text proposed by the Commission	*Amendment*
8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to ***paragraphs 1 and 2*** to the single points of contact of other affected Member States.	8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to ***paragraph 1*** to the single points of contact of other affected Member States.

Or. en

Amendment 474
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 20 – paragraph 9

Text proposed by the Commission	*Amendment*
9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and	9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and

aggregated data on incidents, significant cyber threats and near misses notified in accordance with ***paragraphs 1 and 2*** and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.	aggregated data on ***significant*** incidents, significant cyber threats and ***significant*** near misses notified in accordance with ***paragraph 1*** and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.

Or. en

Amendment 475
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 9

Text proposed by the Commission	*Amendment*
9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with ***paragraphs 1 and 2 and in accordance with*** Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.	9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with ***paragraph 1 of this Article, and*** Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.

Or. en

Justification

Consistency with changes introduced to the text of the Directive.

Amendment 476
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 9

Text proposed by the Commission	*Amendment*
9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with ***paragraphs 1 and 2 and*** in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.	9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with ***paragraph 1*** in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.

Or. en

Amendment 477
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 20 – paragraph 10

Text proposed by the Commission	*Amendment*
10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents ***and cyber threats*** notified in accordance with paragraphs 1 ***and 2*** by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].	10. Competent authorities ***or the CSIRTs*** shall provide ***without undue delay*** to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on ***significant*** incidents***,*** notified in accordance with paragraphs 1 by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]***, as well as on the measures taken by competent authorities or CSIRTs in response to those incidents***.

Or. en

Amendment 478
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand,

Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 10

Text proposed by the Commission	*Amendment*
10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with ***paragraphs 1 and 2*** by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].	10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with ***paragraph 1*** by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].

Or. en

Amendment 479
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 10

Text proposed by the Commission	*Amendment*
10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with ***paragraphs 1 and 2*** by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].	10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with ***paragraph 1*** by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].

Or. en

Amendment 480
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 20 – paragraph 10 a (new)

Text proposed by the Commission	*Amendment*
	10a. Competent authorities or the CSIRTs shall provide without undue delay to the national regulatory authorities or other competent authorities responsible for public electronic communications networks or for publicly available electronic communications services pursuant to Directive (EU) 2018/1972, information on significant incidents notified in accordance with paragraph 1 by providers of public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I, as well as on the measures taken by competent authorities or CSIRTs in response to those incidents.

Or. en

Amendment 481
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 10 a (new)

Text proposed by the Commission	*Amendment*
	10a. ENISA, in cooperation with the Cooperation Group, shall develop common incident notification templates by [date of transposition deadline of the Directive], to streamline the reporting obligations of essential and important entities, and simplify the sharing of relevant information referred to in point (b) of paragraph 1 of this Article.

Or. en

Justification

Common incident templates can simplify the incident reporting process, provide clarity to reporting entities and harmonise the information disclosed by entities reporting entities. ENISA is best placed to carry out this task.

Amendment 482
Eva Maydell, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 20 – paragraph 11

Text proposed by the Commission	*Amendment*
11. ***The Commission, may adopt implementing acts*** further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 ***and 2***. ***The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).***	11. ***ENISA shall develop a common EU-wide template*** further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1.

Or. en

Amendment 483
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 20 – paragraph 11

Text proposed by the Commission	*Amendment*
11. The Commission***, may*** adopt ***implementing*** acts further specifying ***the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify*** the cases in which	11. The Commission ***shall be empowered to*** adopt ***delegated*** acts further specifying the cases in which an incident shall be considered significant as referred to in paragraph ***2, and*** in accordance with the ***exercise of delegation power*** referred to in Article ***36***.

an incident shall be considered significant as referred to in paragraph ***3. Those implementing acts shall be adopted*** in accordance with the ***examination procedure*** referred to in Article ***37(2)***.

Or. en

Justification

Deletion in line with proposed changes to Article 20. Delegated acts are the preferred instrument to further specify the cases in which an incident is considered significant.

Amendment 484
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 20 – paragraph 11

Text proposed by the Commission	*Amendment*
11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to ***paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident*** shall be ***considered significant as referred to in paragraph 3***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).	11. The Commission***, after it has consulted the industry and taking utmost account of ENISA's opinion***, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to ***paragraph 1. They*** shall be ***based on European and international standards to the greatest extent possible***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Or. en

Amendment 485
Tsvetelina Penkova

Proposal for a directive
Article 20 – paragraph 11

Text proposed by the Commission	*Amendment*
11. The Commission, may adopt	11. The Commission, may adopt

implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).	***delegated*** acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Or. en

Justification

A delegated act procedure will add further transparency as the European Parliament will be consulted for the approval process.

Amendment 486
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 21 – title

Text proposed by the Commission	*Amendment*
Use of European cybersecurity certification schemes	Use of European cybersecurity certification schemes ***and standardisation***

Or. en

Amendment 487
Tsvetelina Penkova

Proposal for a directive
Article 21 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to ***demonstrate compliance with certain requirements of*** Article ***18, Member States may require*** essential and important entities to certify certain ICT products, ICT services and ICT	1. In order to ***elevate the overall level of cybersecurity resilience, the Commission may issue a legislative proposal under*** Article ***114 TFEU requiring certain*** essential and important

processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.	entities to certify certain ICT products, ICT services and ICT processes under ***existing*** specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties. ***Such certification requirements shall foresee a transition period that allows providers and end users to get into conformity, and they shall be developed in a way that avoids market distortion.***

Or. en

Justification

The competence to the issue of mandatory certification requirements should lie exclusively with the Commission as it would guarantee a horizontal application of the rules, also aligning with the objectives of the EU Cybersecurity Act (Regulation (EU) 2019/881). If mandatory certification is considered, it should be introduced in conjunction with the provisions laid down under Article 56 para 2 and Article 56 para 3 of the EU Cybersecurity Act, also being accompanied by a timeframe that allows both suppliers and customers to implement these requirements and fully integrate these new products into their operations. Finally, it is necessary to guarantee that the mandatory regime will not lead to a market distortion by creating favourable conditions for specific players (i.e. largest operators that could better recoup their investment through customer base and available resources, or approval of certificates based on the applicant's origin.)

Amendment 488
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Lina Gálvez Muñoz

Proposal for a directive
Article 21 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to demonstrate compliance with certain requirements of Article 18, Member States ***may require*** essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to	1. In order to demonstrate compliance with certain requirements of Article 18, ***and following guidance from ENISA, the Commission, and the Cooperation Group,*** Member States ***shall encourage*** essential and important entities to certify certain ICT products, ICT services and ICT processes**,**

Article 49 of Regulation (EU) 2019/881**.** ***The products, services and processes subject to*** certification ***may be developed by an essential or important entity or procured from third parties***.	***developed either by the essential and important entities or procured from third parties,*** under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881***, or under equivalent and internationally accepted*** certification ***schemes***.

Or. en

Justification

Certification schemes should follow the process laid out by the Cybersecurity Act. Mandatory certification at the national level may incur fragmentation risks to the single market.

Amendment 489
Christophe Grudler, Klemen Grošelj, Nathalie Loiseau, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

Proposal for a directive
Article 21 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to ***certify*** certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881**.** ***The products, services and processes subject to*** certification ***may be developed by an essential or important entity or procured from third parties***.	1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to ***use*** certain ***certified*** ICT products, ICT services and ICT processes***, whether procured from third parties or developed by the essential or important entity, certified*** under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881***, or, in the absence of such a scheme, under equivalent internationally recognised*** certification ***schemes***.

Or. en

Justification

It is not essential and important entities that should be required to certify their products if the Member States require it. Instead, entities should either obtain certified products, services or processes from third parties, or they should certify the products, services or processes that

they developed themselves. Moreover, as the European certification schemes are not yet fully in place, entities should be able to use products, services or processes certified by existing equivalent internationally schemes.

Amendment 490
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 21 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to ***demonstrate compliance with certain requirements of Article 18***, Member States may ***require*** essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881***. The products, services and processes subject to*** certification ***may be developed by an*** essential ***or*** important ***entity or procured from third parties***.	1. In order to ***increase the level of cybersecurity***, Member States may ***recommend*** essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 ***or other international cybersecurity*** certification ***schemes. Member States shall also encourage*** essential ***and*** important ***entities to comply with European and internationally accepted standards***.

Or. en

Amendment 491
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 21 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential ***and*** important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. ***The products, services and processes***	1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require ***ICT suppliers providing products and services for critical functions performed by*** essential ***or*** important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to

subject to certification may be developed by an essential or important entity or procured from third parties.	Article 49 of Regulation (EU) 2019/881.

Or. fr

Amendment 492
Eva Maydell, Franc Bogovič, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 21 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to demonstrate compliance with certain requirements of Article 18, Member States ***may require*** essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.	1. In order to demonstrate compliance with certain requirements of Article 18, Member States ***shall encourage*** essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.

Or. en

Amendment 493
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 21 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in	***deleted***

accordance with Article 36.

Or. en

Amendment 494
Tsvetelina Penkova

Proposal for a directive
Article 21 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.	***deleted***

Or. en

Amendment 495
Eva Maydell, Markus Pieper, Franc Bogovič, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 21 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.	***deleted***

Or. en

Amendment 496
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 21 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ***The Commission shall be empowered to*** adopt delegated acts specifying ***which categories of*** essential entities shall be required to obtain a certificate and ***under which*** specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.	2. ***Taking account of ENISA's opinion, the Commission may*** adopt delegated acts specifying ***that ICT suppliers providing products and services for critical functions performed by*** essential ***or important*** entities shall be required to obtain a certificate and ***identifying the relevant*** specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.

Or. fr

Amendment 497
Christophe Grudler, Klemen Grošelj, Nathalie Loiseau, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

Proposal for a directive
Article 21 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. In order to demonstrate compliance with certain requirements of Article 18 of this Directive, Member States may require essential and important entities to use qualified trust services pursuant to Regulation (EU) No 910/2014.

Or. en

Justification

The use of qualified trust services under the eIDAS Regulation should be encouraged when appropriate.

Amendment 498
Christophe Grudler, Klemen Grošelj, Nathalie Loiseau, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

Proposal for a directive
Article 21 – paragraph 2 b (new)

Text proposed by the Commission	*Amendment*
	2b. Member States may rely on certified cybersecurity services providers, which could be certified under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881, to enforce the supervision activities provided for in Articles 29 and 30 of this Directive.

Or. en

Justification

With the increased number of entities to be regulated, Member States should have the possibility to rely on certified cybersecurity services providers: providers that would have been certified according to a European certification scheme.

Amendment 499
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 21 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission may request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.	***deleted***

Or. en

Amendment 500
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 21 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission may request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 ***in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available***.	3. The Commission***, after consulting the Cooperation Group and the European Cybersecurity Certification Group,*** may request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881.

Or. en

Amendment 501
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 23

Text proposed by the Commission	*Amendment*
Article 23	***deleted***
Databases of domain names and registration data	
1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.	
2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain	

names and the points of contact administering the domain names under the TLDs.

3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.

4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.

5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Or. en

Justification

Although these entities do play a role in ensuring a high level of cybersecurity, regulating their core activity is better suited in a sector specific legislation.

Amendment 502
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 23 – paragraph 1

Text proposed by the Commission	*Amendment*
1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and ***the*** entities providing domain name registration services ***for the TLD*** shall collect and maintain accurate and complete domain name registration data in a dedicated database ***facility with due diligence subject to Union data protection law as regards data which are personal data***.	1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and entities providing domain name registration services shall collect and maintain accurate and complete domain name registration data in a dedicated database.

Or. en

Justification

Consistency with amended text to widen the scope of DNS entities and not only those providing such services for the TLD. Due diligence to Union data protection law covered by the proposed amendment to Article 2 with reference to the legal basis under Article 6.1 (c) of Regulation (EU) 2016/679.

Amendment 503
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 23 – paragraph 1

Text proposed by the Commission	*Amendment*
1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and ***the entities providing domain name registration services for the TLD*** shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.	1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and ***registrars*** shall collect and maintain accurate***, verified*** and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.

Or. en

Amendment 504
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 23 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ensure that the TLD registries and the ***entities providing domain name registration services for the TLD*** have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.	3. Member States shall ensure that the TLD registries and the ***registrars*** have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.

Or. en

Amendment 505
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 23 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall ensure that ***the*** TLD registries and ***the*** entities providing domain name registration services ***for the TLD publish, without undue delay*** after the registration of a domain name, domain registration data ***which are not personal data***.	4. Member States shall ensure that TLD registries and entities providing domain name registration services ***make publicly available, within 72 hours*** after the registration of a domain name, domain registration data ***of legal persons as registrants***.

Or. en

Amendment 506

Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 23 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall ensure that the TLD registries and the ***entities providing domain name registration services for the TLD*** publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.	4. Member States shall ensure that the TLD registries and the ***and the registrars*** publish, without undue delay ***but no later than 24 hours*** after the registration of a domain name, ***fees,*** domain registration data***,*** which are not personal data.

Or. en

Amendment 507
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 23 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Member States shall ensure that ***the*** TLD registries and ***the*** entities providing domain name registration services ***for the TLD*** provide access to specific domain name registration data upon ***lawful and*** duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and ***the*** entities providing domain name registration services ***for the TLD*** reply ***without undue delay*** to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.	5. Member States shall ensure that TLD registries and entities providing domain name registration services provide access to specific domain name registration data***, including personal data,*** upon duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and entities providing domain name registration services reply ***within 72 hours*** to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available. ***The Commission may adopt implementing acts laying out the requirements to be demonstrated by legitimate access seekers to TLD registries and entities providing domain name registration services before access to***

specific domain name registration data is granted. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Or. en

Justification

Consistency with amended text to widen the scope of DNS entities and not only those providing such services for the TLD. TLD registries and the entities providing domain name registration services should reply to duly justified requests of legitimate access seekers within 72 hours, and the Commission may adopt implementing acts laying out the conclusive requirements to be demonstrated by legitimate access seekers for access to domain name registration data.

Amendment 508
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 23 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Member States shall ensure that the TLD registries and the ***entities providing domain name registration services for the TLD*** provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the ***entities providing domain name registration services for the TLD*** reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.	5. Member States shall ensure that the TLD registries and the ***registrars*** provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the ***registrars*** reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Or. en

Amendment 509
Evžen Tošenovský

Proposal for a directive
Article 24 – paragraph 1

Text proposed by the Commission	*Amendment*
1. DNS service providers, TLD name registries, cloud computing service providers, data centre service providers ***and*** content delivery network providers referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.	1. DNS service providers, TLD name registries, cloud computing service providers, data centre service providers***,*** content delivery network providers ***and providers of number-independent interpersonal communications services*** referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.

Or. en

Amendment 510
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 24 – paragraph 1

Text proposed by the Commission	*Amendment*
1. ***DNS service providers, TLD name registries,*** cloud computing service providers, data centre service providers and content delivery network providers referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.	1. Cloud computing service providers, data centre service providers and content delivery network providers referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.

Or. en

Justification

Adjustment of scope in line with other proposed changes

Amendment 511
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 24 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. All essential and important entities referred to in Annexes I and II, with the exception of entities referred to in paragraph 1 of this Article, shall fall under the jurisdiction of the Member State where they provide their services. If the entity provides services in more than one Member State, it shall fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States shall cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions.

Or. en

Amendment 512
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 24 – paragraph 2

Text proposed by the Commission	*Amendment*
2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the ***highest number of employees in the Union***.	2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the ***operational and management capacities to implement***

cybersecurity measures.

Or. fr

Amendment 513
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 24 – paragraph 2

Text proposed by the Commission	*Amendment*
2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment ***with the highest number of employees*** in the Union.	2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment ***responsible for the implementation of the main cybersecurity risk management measures*** in the Union.

Or. en

Amendment 514
Tsvetelina Penkova

Proposal for a directive
Article 24 – paragraph 2

Text proposed by the Commission	*Amendment*
2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the	2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken***, or where cybersecurity operations are carried out***. If such decisions are not taken in any establishment in the Union, the main

Member State where the entities have the establishment with the highest number of employees in the Union.	establishment shall be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the Union.

Or. en

Amendment 515
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 24 – paragraph 2

Text proposed by the Commission	*Amendment*
2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be ***deemed to be in the Member State where the entities have the establishment with the highest number of employees*** in the Union.	2. For the purposes of this Directive, entities ***providing activities*** referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be ***the place of its central administration*** in the Union.

Or. en

Amendment 516
Eva Maydell, Markus Pieper, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 24 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. Essential and important entities should be subject to this Directive only in those Member States where they perform activities relevant to their designation as essential or important entities.

Amendment 517
Evžen Tošenovský

Proposal for a directive
Article 25

Text proposed by the Commission	*Amendment*
Article 25	***deleted***
Registry for essential and important entities	
1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1). The entities shall submit the following information to ENISA by [12 months after entering into force of the Directive at the latest]:	
(a) the name of the entity;	
(b) the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 24(3);	
(c) up-to-date contact details, including email addresses and telephone numbers of the entities.	
2. The entities referred to in paragraph 1 shall notify ENISA about any changes to the details they submitted under paragraph 1 without delay, and in any event, within three months from the date on which the change took effect.	
3. Upon receipt of the information under paragraph 1, ENISA shall forward it to the single points of contact depending on the indicated location of each entity's main establishment or, if it is not established in the Union, of its designated representative. Where an entity referred to in paragraph 1 has besides its main	

establishment in the Union further establishments in other Member States, ENISA shall also inform the single points of contact of those Member States.

4. Where an entity fails to register its activity or to provide the relevant information within the deadline set out in paragraph 1, any Member State where the entity provides services shall be competent to ensure that entity's compliance with the obligations laid down in this Directive.

Or. en

Amendment 518
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 25 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1). The entities shall submit the following information to ENISA by [12 months after entering into force of the Directive at the latest]:	1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1)***. ENISA shall establish appropriate information classification and management protocols to ensure the security and confidentiality of disclosed information, and restrict the access, storage, and transmission of such information to intended users***. The entities shall submit the following information to ENISA by [12 months after entering into force of the Directive at the latest]:

Or. en

Justification

Proper management protocols should be set for the information provided by entities falling in scope of this Directive.

Amendment 519

Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 25 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1)***. The entities shall submit*** the following information ***to ENISA by [12 months after entering into force of the Directive at the latest]***:	1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1)***, including*** the following information:

Or. en

Amendment 520
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 25 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1). The entities shall submit the following information to ENISA by [12 months after entering into force of the Directive at the latest]:	1. ENISA shall create and maintain a ***secure*** registry for essential and important entities referred to in Article 24(1). The entities shall submit the following information to ENISA by [12 months after entering into force of the Directive at the latest]:

Or. en

Justification

As a single point of failure, a registry containing entities designated under a non-public procedure should be properly secured.

Amendment 521
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 25 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Upon receipt of the information under paragraph 1, ENISA shall forward it to the single points of contact depending on the indicated location of each entity's main establishment or, if it is not established in the Union, of its designated representative. Where an entity referred to in paragraph 1 has besides its main establishment in the Union further establishments in other Member States, ENISA shall also inform the single points of contact of those Member States.	***deleted***

Or. en

Justification

Taking into account that the current instrument is a Directive, the proposed procedure needs to be refined, as Member States have to transpose the provisions into their national laws, requiring the entities to register in ENISA's register, so ENISA can forward back to the same Member State that the entities are registered.

Amendment 522
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 26 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. Without prejudice to Regulation (EU) 2016/679, Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing:	1. Without prejudice to Regulation (EU) 2016/679, Member States shall ensure that essential and important entities ***and other relevant entities not covered by the scope of this Directive*** may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing:

Or. en

Amendment 523
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 26 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. ***Without prejudice to Regulation (EU) 2016/679,*** Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing:	1. Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, ***near misses,*** vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing:

Or. en

Justification

Deletion covered by changes to text of the Directive regarding the legal basis introduced in Article 2.

Amendment 524
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 26 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. ***Without prejudice to Regulation (EU) 2016/679,*** Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration	1. Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, ***industrial espionage*** tactics, techniques and procedures, cybersecurity alerts***,*** ***metadata*** and configuration tools, where

tools, where such information sharing:	such information sharing:

Or. en

Amendment 525
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 26 – paragraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques, mitigation strategies, or response and recovery stages.	(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection***, containment and prevention*** techniques, mitigation strategies, or response and recovery stages***, facilitating collaboration in cyber threat research among public entities, private entities and research bodies***.

Or. en

Amendment 526
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 26 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that the exchange of information takes place within trusted communities of essential and important entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared ***and in compliance with the rules of Union law referred to in paragraph 1***.	2. Member States shall ensure that the exchange of information takes place within trusted communities of essential and important entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared.

Or. en

Amendment 527
Evžen Tošenovský

Proposal for a directive
Article 26 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ***ensure that*** the exchange of information takes place within trusted communities of essential and important entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared and in compliance with the rules of Union law referred to in paragraph 1.	2. Member States shall ***facilitate*** the exchange of information takes place within trusted communities of essential and important ***entities and other relevant*** entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared and in compliance with the rules of Union law referred to in paragraph 1.

Or. en

Amendment 528
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 26 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ***ensure that*** the exchange of information ***takes place within*** trusted communities of essential and important entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared ***and in compliance with the rules of Union law referred to in paragraph 1***.	2. Member States shall ***facilitate*** the exchange of information ***by enabling the establishment of*** trusted communities of essential and important entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared.

Or. en

Justification

Deletion covered by changes to text of the Directive regarding the legal basis introduced in Article 2.

Amendment 529
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 26 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ***set out rules specifying the procedure,*** operational elements (including the use of dedicated ICT platforms), content ***and conditions*** of the information sharing arrangements referred to in paragraph 2***. Such rules*** shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article ***5(2) (g)***.	3. Member States shall ***facilitate information sharing by making*** operational elements (including the use of dedicated ICT platforms), ***and*** content ***available*** of the information sharing arrangements referred to in paragraph 2***, and may impose certain conditions on the information made available by competent authorities or CSIRTs. Member States*** shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article ***5(2)(l)***.

Or. en

Amendment 530
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 26 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall set out rules specifying the procedure, operational	3. Member States***, pursuant to paragraph 5,*** shall set out rules specifying

elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such rules shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).	the procedure, operational elements (including the use of dedicated ICT platforms ***and tools***), content and conditions of the information sharing arrangements referred to in paragraph 2. Such rules shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).

Or. en

Amendment 531
Evžen Tošenovský

Proposal for a directive
Article 26 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall set out ***rules*** specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such ***rules*** shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).	3. Member States shall set out ***recommendations*** specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such ***recommendations*** shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).

Or. en

Amendment 532
Evžen Tošenovský

Proposal for a directive
Article 26 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. Provisions of paragraphs 1, 2 and 3 of this Article shall apply mutatis mutandis for the information-sharing with entities under the jurisdiction of other Member State. The competent authorities of Member States concerned shall cooperate to facilitate the information-sharing.

Or. en

Amendment 533
Evžen Tošenovský

Proposal for a directive
Article 26 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Essential and important entities ***shall*** notify the competent authorities of their participation in the information-sharing arrangements referred to in ***paragraph*** 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.	4. Essential and important entities ***may*** notify the competent authorities of their participation in the information-sharing arrangements referred to in ***paragraphs*** 2 ***and 3a***, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.

Or. en

Amendment 534
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 26 – paragraph 5

Text proposed by the Commission	*Amendment*
5. In compliance with Union law, ENISA shall support the establishment of	5. In compliance with Union law, ENISA shall support the establishment of

cybersecurity information-sharing arrangements referred to in ***paragraph*** 2 by providing best practices and guidance.	cybersecurity information-sharing arrangements referred to in ***paragraphs*** 2 ***and 3a*** by providing best practices and guidance.

Or. en

Amendment 535
Evžen Tošenovský

Proposal for a directive
Article 27 – title

Text proposed by the Commission	*Amendment*
Voluntary ***notification of relevant information***	Voluntary ***reporting***

Or. en

Amendment 536
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 27 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall ensure that, without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. ***When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.***	Member States shall ensure that, without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications ***to competent authorities or the CSIRT***, on a voluntary basis, of significant incidents, ***significant*** cyber threats or ***significant*** near misses.

Or. en

Amendment 537
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 27 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall ensure that, without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.	Member States shall ensure that, without prejudice to Article 3, entities ***within the scope and those*** falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.

Or. en

Amendment 538
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 27 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	Member States shall ensure that Article 20 applies mutatis mutandis for the submission and processing of the

voluntary notifications referred to in paragraph 1 and 1a of this Article. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.

Or. en

Amendment 539
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 27 – paragraph 1 b (new)

Text proposed by the Commission	*Amendment*
	Member States shall ensure that Article 20 applies mutatis mutandis for the submission and processing of the voluntary notifications referred to in paragraphs 1 and 1a of this Article. Where applicable, the voluntarily reporting entities shall be encouraged to notify simultaneously the recipients of their services that are potentially affected of any measures or remedies that those recipients can take in response to the threat. The notification shall not make the notifying entity subject to increased liability. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.

Or. en

Amendment 540
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 28 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.	2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches***, without prejudice to the competences, tasks and powers of data protection authorities pursuant to Regulation (EU) 2016/679***.

Or. en

Justification

Clarification needed to ensure that NIS2 does not interfere with GDPR enforcement.

Amendment 541
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 29 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that the measures of supervision or enforcement imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.	1. Member States shall ensure that the measures of supervision or enforcement imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case ***of each individual case as well as the need to promote the exchange of information between competent authorities and essential entities***.

Or. en

Amendment 542
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 29 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) on-site inspections and off-site supervision, including random checks;	(a) on-site inspections and off-site supervision, including random checks***, carried out by certified professionals***;

Or. en

Amendment 543
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 29 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) ***regular*** audits;	(b) ***annual*** audits;

Or. en

Amendment 544
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 29 – paragraph 2 – point b – point i (new)

Text proposed by the Commission	*Amendment*
	(i) an ad hoc audit can be carried out in cases justified on the ground of a significant incident or non-compliance by the essential entity;

Or. en

Amendment 545
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 29 – paragraph 2 – point c

Text proposed by the Commission	*Amendment*
(c) ***targeted*** security audits based on risk assessments or risk-related available information;	(c) security audits based on risk assessments or risk-related available information ***carried out by a qualified independent body or a competent authority or independent experts and make the results thereof available to the competent authority***; ***the cost of the audit shall be paid by the provider;***

Or. en

Justification

Aligning the text with 40 and 41 of Directive (EU) 2018/1972

Amendment 546
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 29 – paragraph 2 – point c

Text proposed by the Commission	*Amendment*
(c) targeted security audits based on risk assessments ***or*** risk-related available information;	(c) targeted security audits based on risk assessments ***performed by the competent authorities, risk assessments performed by the audited entity, or in the absence thereof,*** risk-related available information;

Or. en

Justification

Risk assessments performed by the entity may contribute valuable information to the competent authority supervising their compliance with the provisions laid out in this Directive.

Amendment 547
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 29 – paragraph 2 – point g

Text proposed by the Commission	*Amendment*
(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence**.**	(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence***; the cost of the audit shall be paid by the essential entity;***

Or. en

Amendment 548
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 29 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. where exercising their power under points (a) to (d) in paragraph 2, the competent authorities shall follow a due process in order to minimise the impact on business processes for the entity;

Or. en

Amendment 549
Evžen Tošenovský

Proposal for a directive
Article 29 – paragraph 4 – point a a (new)

Text proposed by the Commission	*Amendment*
	(aa) investigate cases of non-compliance and the effects thereof on the security of the services;

Or. en

Amendment 550
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 29 – paragraph 4 – point b

Text proposed by the Commission	*Amendment*
(b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;	(b) issue binding instructions***, including those regarding the measures required to remedy an incident or prevent one from occurring when a significant threat has been identified, time-limits for implementation and reporting obligations,*** or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;

Or. en

Amendment 551
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 29 – paragraph 4 – point h

Text proposed by the Commission	*Amendment*
(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner;	(h) order***, where necessary for risk management purposes,*** those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner;

Or. en

Amendment 552
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova

Proposal for a directive
Article 29 – paragraph 4 – point i

Text proposed by the Commission	*Amendment*
(i) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;	***deleted***

Or. en

Justification

Far-reaching provision.

Amendment 553
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 29 – paragraph 4 – point i

Text proposed by the Commission	*Amendment*
(i) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;	(i) make a public statement***, where necessary for risk management purposes,*** which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;

Or. en

Amendment 554
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 29 – paragraph 4 – point j

Text proposed by the Commission	*Amendment*
(j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to***, or instead of,*** the measures referred to in	(j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to the measures referred to in points (a) to (i) of

points (a) to (i) of this paragraph, depending on the circumstances of each individual case.

this paragraph, depending on the circumstances of each individual case.

Or. en

Amendment 555
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – introductory part

Text proposed by the Commission	*Amendment*
5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity ***is*** requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the power to:	5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity ***or suppliers of products or services for critical functions performed by essential or important entities are*** requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the power to:

Or. fr

Amendment 556
François-Xavier Bellamy

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – introductory part

Text proposed by the Commission	*Amendment*
5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent	5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent

authorities have the power to establish a deadline within which the essential entity ***is*** requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the power to:	authorities have the power to establish a deadline within which the essential entity ***or manufacturers and providers of ICT products are*** requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the power to:

Or. en

Amendment 557
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;	(a) ***where applicable, temporarily*** suspend or request a certification or authorisation body to ***temporarily*** suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity ***until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied***;

Or. en

Justification

There is a lack of proportionality and territoriality of the application of this provision for an awarded certification internationally accepted to an entity.

Amendment 558
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;	(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity ***or related ICT suppliers providing products and services for critical functions performed by essential or important entities***;

Or. fr

Amendment 559
François-Xavier Bellamy

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;	(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity ***or the related manufacturers and providers of ICT products***;

Or. en

Amendment 560
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) ***suspend or*** request a certification or authorisation body to ***suspend*** a certification or authorisation concerning	(a) request a certification or authorisation body to ***consider suspension of*** a certification or authorisation

part or all ***the*** services or activities provided by an essential entity;	concerning part or all ***relevant*** services or activities provided by an essential entity;

Or. en

Amendment 561
Eva Maydell, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.	***deleted***

Or. en

Amendment 562
Evžen Tošenovský

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.	***deleted***

Or. en

Amendment 563
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and ***of*** any other natural person held responsible for the breach, from exercising managerial functions in that entity.	(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity ***or related ICT suppliers providing products and services for critical functions performed by essential or important entities***, and ***against*** any other natural person held responsible for the breach, from exercising managerial functions in that entity.

Or. fr

Amendment 564
François-Xavier Bellamy

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.	(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity***, or the related manufacturers and providers of ICT products***.

Or. en

Amendment 565
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity***, *and of any other natural person held responsible for the breach,*** from exercising managerial functions in that entity.	(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity from exercising managerial functions in that entity. ***This provision shall not apply to public administration entities as referred to in point (23) of Article 4.***

Or. en

Amendment 566
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 2

Text proposed by the Commission	*Amendment*
These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.	***deleted***

Or. en

Justification

Provision covered with proposed change to Article 29, paragraph 5, point (a).

Amendment 567
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 2

Text proposed by the Commission	*Amendment*
These sanctions shall be applied only until the entity ***takes*** the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.	These sanctions shall be applied only until the entity ***or related ICT suppliers providing products and services for critical functions performed by essential or important entities take*** the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.

Or. fr

Amendment 568
François-Xavier Bellamy

Proposal for a directive
Article 29 – paragraph 5 – subparagraph 2

Text proposed by the Commission	*Amendment*
These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.	These sanctions shall be applied only until the entity***, or the related manufacturers and providers of ICT products,*** takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.

Or. en

Amendment 569

Evžen Tošenovský

Proposal for a directive
Article 29 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive. ***Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.***	6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive.

Or. en

Amendment 570
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 29 – paragraph 7 – point c

Text proposed by the Commission	*Amendment*
(c) the actual damage caused or losses incurred ***or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential*** financial or economic losses, effects on other services, number of users affected ***or potentially affected***;	(c) the actual damage caused or losses incurred ***including*** financial or economic losses, effects on other services, ***and the*** number of users affected;

Or. en

Justification

Enforcement actions or sanctions from competent authorities should apply to actual damages or losses rather than potential damages or potential losses. The same principles should apply to the actual number of users affected rather than the potential number of users affected.

Amendment 571
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 29 – paragraph 7 – point c

Text proposed by the Commission	*Amendment*
(c) the actual damage caused or losses incurred ***or potential damage or losses that could have been triggered, insofar as they can be determined***. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;	(c) the actual damage caused or losses incurred. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;

Or. en

Amendment 572
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 30 – paragraph 2 – point a a (new)

Text proposed by the Commission	*Amendment*
	(aa) investigate cases of non-compliance and the effects thereof on the security of the services;

Or. en

Amendment 573
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 30 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) ***targeted*** security audits based on risk assessments or risk-related available information;	(b) security audits based on risk assessments or risk-related available information ***carried out by a qualified independent body or a competent authority and make the results thereof available to the competent authority***; ***the cost of the audit shall be paid by the provider;***

Or. en

Justification

Aligning the text with art. 40 and 41 of Directive (EU) 2018/1972.

Amendment 574
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 30 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) targeted security audits based on risk assessments ***or*** risk-related available information;	(b) targeted security audits based on risk assessments ***performed by the competent authority, risk assessments performed by the audited entity, or in the absence thereof,*** risk-related available information;

Or. en

Justification

Risk assessments performed by the entity may contribute valuable information to the competent authority supervising their compliance with the provisions laid out in this Directive.

Amendment 575
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 30 – paragraph 2 – point c

Text proposed by the Commission	*Amendment*
(c) security scans based on objective, fair and transparent risk assessment criteria;	(c) security scans based on objective***, non-discriminatory***, fair and transparent risk assessment criteria;

Or. en

Justification

In line with original text in Article 29 for the supervision and enforcement of essential entities.

Amendment 576
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 30 – paragraph 4 – point g

Text proposed by the Commission	*Amendment*
(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;	(g) order***, where necessary for risk management purposes,*** those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;

Or. en

Amendment 577
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova

Proposal for a directive
Article 30 – paragraph 4 – point h

Text proposed by the Commission	*Amendment*
(h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;	***deleted***

Or. en

Justification

Far-reaching provision.

Amendment 578
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 30 – paragraph 4 – point h

Text proposed by the Commission	*Amendment*
(h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;	(h) make a public statement***, where necessary for risk management purposes,*** which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;

Or. en

Amendment 579
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 31 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that the imposition of administrative fines on essential and important entities pursuant to this Article in respect of infringements of the obligations laid down in this Directive are, in each individual case, effective,	1. Member States shall ensure that the imposition of administrative fines on essential and important entities pursuant to this Article in respect of infringements of the obligations laid down in this Directive are, in each individual case, effective,

proportionate and dissuasive**.**	proportionate and dissuasive ***and only imposed if the infringement was intentional, negligent or the entity had had prior notice of the possibility of committing an infringement***.

Or. en

Amendment 580
Evžen Tošenovský, Zdzisław Krasnodębski

Proposal for a directive
Article 31 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Without prejudice to the powers of competent authorities pursuant to Articles 29 and 30, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities referred to in Article 4(23) subject to the obligations provided for by this Directive.	***deleted***

Or. en

Amendment 581
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 32 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities	1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities

competent pursuant to Articles 55 and 56 of that Regulation within ***a reasonable period of time***.	competent pursuant to Articles 55 and 56 of that Regulation within ***72 hours***.

Or. en

Justification

Aligned with Article 33(1) GDPR, where controllers have to notify a personal data breach within 72 hours.

Amendment 582
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 32 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ***within a reasonable period of time***.	1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation(EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ***without undue delay***.

Or. en

Justification

This obligation is without prejudice to the reporting obligation on controllers as defined in Article 33 of Regulation (EU) 2016/679, which must be done "without undue delay". This change is in line with EDPS Opinion 5/2021 on the Cybersecurity Strategy and the NIS2.0 Directive in order to enable data protection authorities to perform their tasks effectively.

Amendment 583
Rasmus Andresen

on behalf of the Greens/EFA Group

Proposal for a directive
Article 32 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority ***may*** inform the supervisory authority established in the same Member State.	3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority ***shall*** inform the supervisory authority established in the same Member State.

Or. en

Justification

In line with the GDPR logic for cross-border cases. They trigger the consistency mechanism under Section 2 of Chapter VII GDPR.

Amendment 584
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 34 a (new)

Text proposed by the Commission	*Amendment*
	Article 34a
	Right to an effective judicial remedy
	Without prejudice to any available administrative or non-judicial remedy, the recipients of services provided by essential and important entities, having incurred damages as a result of the providers' non-compliance with this Directive, shall have the right to an effective judicial remedy.

Or. en

Justification

In a similar manner to Arts. 77 – 79 GDPR, recipients of a service harmed by an essential/important entity who has not complied with the NIS2 rules, they should have adequate remedies. This also incentivise the entities to comply.

Amendment 585
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 35 – paragraph 1

Text proposed by the Commission	*Amendment*
The Commission shall periodically review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The first report shall be submitted by… [***54*** months after the date of entry into force of this Directive].	The Commission shall periodically review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The first report shall be submitted by… [***36*** months after the date of entry into force of this Directive].

Or. en

Justification

Due to the importance of this act and the evolution of the risks faster results are needed.

Amendment 586
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 35 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	As regards Digital Providers referred to in point (6) of Annex II, where platforms operated by such important entities are classified as very large online platforms within the meaning of Article 25 of Regulation (EU) XXXX/XXXX [Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC], or where the providers of core platform services are designated as gatekeepers within the meaning of Article 3 of Regulation (EU) XXXX/XXXX [Contestable and fair markets in the digital sector (Digital Markets Act)], these providers shall be designated as essential entities within the meaning of this Directive to adequately address the functioning of the economy and society in relation to cybersecurity, given the systemic risk stemming from the functioning and use made of their services in the Union, or the important gateway function that their core platform services serve for business users to reach end users.

Or. en

Amendment 587
Evžen Tošenovský, Izabela-Helena Kloc

Proposal for a directive
Article 36

Text proposed by the Commission	*Amendment*
Article 36	***deleted***
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 Articles 18(6) and 21(2) shall be conferred on the Commission for a period of five years from […]

3. The delegation of power referred to in Articles 18(6) and 21(2) 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 the 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. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.

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

6. A delegated act adopted pursuant to Articles 18(6) and 21(2) 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 to 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.

Or. en

Amendment 588
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Christophe Grudler

Proposal for a directive
Article 37 – paragraph 3 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	Where no opinion is delivered, the draft implementing act may not be adopted.

Or. en

Justification

As described in Article 5, (4.b) of Regulation (EU) No 182/2011.

Amendment 589
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 38 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall adopt and publish, by … [***18*** months after the date of entry into force of this Directive], the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].	1. Member States shall adopt and publish, by … [***24*** months after the date of entry into force of this Directive], the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].

Or. en

Amendment 590
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 38 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall adopt and publish, by … [***18*** months after the date of	1. Member States shall adopt and publish, by … [***24*** months after the date of

entry into force of this Directive], the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].	entry into force of this Directive], the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].

Or. en

Amendment 591
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Christophe Grudler, Martina Dlabajová

Proposal for a directive
Article 39

Text proposed by the Commission	*Amendment*
Article 39	***deleted***
Amendment of Regulation (EU) No 910/2014	
Article 19 of Regulation (EU) No 910/2014 is deleted.	

Or. en

Justification

Article 19 Regulation (EU) No 910/2014 (eIDAS) forms the basis of security conditions for qualified trust service providers. A deletion of an article in the eIDAS Regulation should be done through the review of the eIDAS Regulation.

Amendment 592
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 39 – paragraph 1

Text proposed by the Commission	*Amendment*
Article 19 of Regulation (EU) No 910/2014 is deleted.	Article 19 of Regulation (EU) No 910/2014 is deleted ***with effect from [date of transposition deadline of the Directive].***

Or. en

Amendment 593
Evžen Tošenovský

Proposal for a directive
Article 40 – paragraph 1

Text proposed by the Commission	*Amendment*
Articles 40 and 41 of Directive (EU) 2018/1972 ***are*** deleted.	Directive (EU) 2018/1972 ***is amended with effect from [date of transposition deadline of the Directive] as follows:***
	(a) Article 40 is replaced by the following: "Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services comply with Directive (EU) XXXX/XXXX (NIS2)."
	(b) Article 41 is deleted.

Or. en

Amendment 594
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 40 – paragraph 1

Text proposed by the Commission	*Amendment*
Articles 40 and 41 of Directive (EU) 2018/1972 are ***deleted***.	Articles 40 and 41 of Directive (EU) 2018/1972 are ***to be applied insofar as they are not in contradiction with this Directive***.

Or. en

Justification

EECC is a sectorial legislation and some specificities of communication services need to be preserved, without increasing the administrative burden.

Amendment 595
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Christophe Grudler

Proposal for a directive
Article 40 – paragraph 1

Text proposed by the Commission	*Amendment*
Articles 40 and 41 of Directive (EU) 2018/1972 are deleted.	Articles 40 and 41 of Directive (EU) 2018/1972 are deleted ***18 months after the date of entry into force of this Directive***.

Or. en

Amendment 596
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 40 a (new)

Text proposed by the Commission	*Amendment*
	Article 40a
	Amendments to Directive 2020/1828/EC on Representative Actions for the Protection of the Collective Interests of Consumers
	The following is added to Annex I: "(X) Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive(EU) 2016/1148"

Or. en

Justification

Security incidents in the digital domain can have consequences on large number of citizens, sometimes millions, and individual redress could put strain on any redress system. As a solution collective redress would allow a number of consumers to jointly bring a court case when the factual basis is the non-respect of NIS 2 provisions by an entity falling under the scope.

Amendment 597
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

Proposal for a directive
Article 42 – paragraph 1

Text proposed by the Commission	*Amendment*
This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union***, with exception to Article 39 which enters into force on the day following the day when the transposition deadline as laid down in Article 38 expires***.

Or. en

Justification

There is a need of a provision stating that the deletion of the article 19 of the eIDAS enters into force at the day when the NIS2 implementation date expires. This is required to avoid legal loophole during the time for the NIS2 implementation to national legislation, as the eIDAS is a regulation and the NIS2 a directive with a time prescribed for the implantation.

Amendment 598
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Annex I – subheading 1

Text proposed by the Commission	*Amendment*
ESSENTIAL ENTITIES:	***ENTITIES WITH HIGHER LEVEL OF CRITICALITY***:

Or. en

Amendment 599
Evžen Tošenovský

Proposal for a directive
Annex I – table – point 9

Text proposed by the Commission	*Amendment*
9. Public administration	***deleted***
– Public administration entities of central governments	
– Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 [98]	
– Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003	

Or. en

Amendment 600
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Annex II – subheading 1

Text proposed by the Commission	*Amendment*
IMPORTANT ENITIES:	ENITIES ***WITH LOWER LEVEL OF CRITICALITY***:

Or. en