European Parliament
2019-2024

Plenary sitting

A9-0313/2021

04.11.2021

***I
REPORT

on the proposal for a 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
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Committee on Industry, Research and Energy

Rapporteur: Bart Groothuis

Rapporteur for the opinion (*):
Lukas Mandl, Committee on Civil Liberties, Justice and Home Affairs

(*) Associated committees – Rule 57 of the Rules of Procedure

Symbols for procedures

*	Consultation procedure
***	Consent procedure
***I	Ordinary legislative procedure (first reading)
***II	Ordinary legislative procedure (second reading)
***III	Ordinary legislative procedure (third reading)

(The type of procedure depends on the legal basis proposed by the draft act.)

Amendments to a draft act

Amendments by Parliament set out in two columns

Deletions are indicated in ***bold italics*** in the left-hand column. Replacements are indicated in ***bold italics*** in both columns. New text is indicated in ***bold italics*** in the right-hand column.

The first and second lines of the header of each amendment identify the relevant part of the draft act under consideration. If an amendment pertains to an existing act that the draft act is seeking to amend, the amendment heading includes a third line identifying the existing act and a fourth line identifying the provision in that act that Parliament wishes to amend.

Amendments by Parliament in the form of a consolidated text

New text is highlighted in ***bold italics***. Deletions are indicated using either the ▌ symbol or strikeout. Replacements are indicated by highlighting the new text in ***bold italics*** and by deleting or striking out the text that has been replaced.
By way of exception, purely technical changes made by the drafting departments in preparing the final text are not highlighted.

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the proposal for a 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
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2020)0823),

– having regard to Article 294(2) and Article 114 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C9-0422/2020),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to the opinion of the of the European Economic and Social Committee of 27 April 2021[1],

– after consulting the Committee of the Regions,

– having regard to Rule 59 of its Rules of Procedure,

– having regard to the opinions of the Committee on Civil Liberties, Justice and Home Affairs, the Committee on Foreign Affairs, the Committee on the Internal Market and Consumer Protection and the Committee on Transport and Tourism,

– having regard to the report of the Committee on Industry, Research and Energy (A9-0313/2021),

1. Adopts its position at first reading hereinafter set out;

2. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

[1] OJ C 286, 16.7.2021, p. 170.

Amendment 1

Proposal for a directive
Title

Text proposed by the Commission	*Amendment*
Proposal for a	Proposal for a
DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	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	on measures for a high common level of cybersecurity across the Union ***(NIS 2 Directive)***, repealing Directive (EU) 2016/1148

Amendment 2

Proposal for a directive
Recital 1

Text proposed by the Commission	*Amendment*
(1) Directive (EU) 2016/1148 of the European Parliament and the Council[11] aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's economy and society ***to function effectively***.	(1) Directive (EU) 2016/1148 of the European Parliament and the Council[11]***, commonly known as the 'NIS directive'*** aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's ***security and to the effective functioning of its*** economy and society.
[11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016 p. 1).	[11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016 p. 1).

Amendment 3

Proposal for a directive
Recital 3

Text proposed by the Commission	*Amendment*
(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence and cause major damage to the Union economy and society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market.	(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence and cause major damage to the Union economy and society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market. ***Moreover, cybersecurity is a key enabler for many critical sectors to successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalisation.***

Amendment 4

Proposal for a directive
Recital 3 a (new)

Text proposed by the Commission	*Amendment*
	(3a) Large-scale cybersecurity incidents and crises at Union level require coordinated action to ensure a rapid and effective response, because of the high degree of interdependence between sectors and countries. The availability of cyber-resilient networks and information systems and the availability, confidentiality and integrity of data are

	vital for the security of the Union within as well as beyond its borders, as cyber threats could originate from outside the Union. The Union's ambition to acquire a more prominent geopolitical role also rests on credible cyber defence and deterrence, including the capacity to identify malicious actions in a timely and effective manner and to respond adequately.

Amendment 5

Proposal for a directive
Recital 5

Text proposed by the Commission	*Amendment*
(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards. This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.	(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards***. Ultimately, those divergences could lead to higher vulnerability of some Member States to cybersecurity threats, with potential spill-over effects across the Union***. This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive ***(NIS 2 Directive)***.

Amendment 6

Proposal for a directive
Recital 6

Text proposed by the Commission	*Amendment*
(6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14], are of relevance.	(6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the ***prevention,*** investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14], are of relevance.
[14] The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).	[14] The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).

Amendment 7

Proposal for a directive
Recital 7

Text proposed by the Commission	*Amendment*
(7) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy in light of the considerations set out in recitals (4) to (6). The sectors covered by Directive (EU) 2016/1148 should therefore be extended to provide a comprehensive coverage of the sectors and services of vital importance for	(7) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy in light of the considerations set out in recitals (4) to (6). The sectors covered by Directive (EU) 2016/1148 should therefore be extended to provide a comprehensive coverage of the sectors and services of vital importance for

key societal and economic activities within the internal market. The ***rules*** should not be different according to whether the entities are operators of essential services or digital service providers. That differentiation has proven obsolete, since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market.

key societal and economic activities within the internal market. The ***risk management requirements and reporting obligations*** should not be different according to whether the entities are operators of essential services or digital service providers. That differentiation has proven obsolete, since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market.

Amendment 8

Proposal for a directive
Recital 8

Text proposed by the Commission	*Amendment*
(8) In accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services ('identification process'). In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[15], that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. ***Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion.***	(8) In accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services ('identification process'). In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[15], that operate within the sectors or provide the type of services covered by this Directive, fall within its scope.
[15] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p.	[15] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p.

36). 36).

Amendment 9

Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. ***Member States should be responsible for establishing a list of such entities, and submit it to the Commission.***	(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive.

Amendment 10

Proposal for a directive
Recital 9 a (new)

Text proposed by the Commission	*Amendment*
	(9a) Member States should establish a list of all essential and important entities. That list should include the entities that meet the generally applicable size-related criteria as well as the small enterprises and microenterprises that fulfil certain criteria that indicate their key role for the economies or societies of Member States. In order for computer security incident response teams (CSIRTs) and competent authorities to provide assistance and to warn entities about cyber incidents that could affect them, it is important that those authorities have the correct contact details of the entities. Essential and important entities should therefore submit at least the following information to the competent authorities: the name of the entity, the address and up-to-date contact details, including email addresses, IP ranges, telephone numbers and relevant sector(s) and subsector(s) referred to in

	Annexes I and II. The entities should notify the competent authorities of any changes to that information. Member States should without undue delay, ensure that that information can be easily provided through a single entry point. To that end, ENISA, in cooperation with the Cooperation Group, should without undue delay issue guidelines and templates regarding the notification obligations. Member States should notify to the Commission and the Cooperation Group of the number of essential and important entities. Member States should also notify the Commission for the purpose of the review referred to in this Directive of the names of the small enterprises and microenterprises identified as essential and important entities, in order to enable the Commission to assess consistency among the Member States' approaches. That information should be handled as strictly confidential.

Amendment 11

Proposal for a directive
Recital 10

Text proposed by the Commission	*Amendment*
(10) The Commission, in cooperation with the Cooperation Group***, may*** issue guidelines on the implementation of the criteria applicable to micro and small enterprises.	(10) The Commission, in cooperation with the Cooperation Group ***and relevant stakeholders, should*** issue guidelines on the implementation of the criteria applicable to ***microenterprises*** and small enterprises. ***The Commission should also ensure that appropriate guidance is given to all micro and small enterprises falling within the scope of this Directive. The Commission should, with the support of the Member States, provide microenterprises and small enterprises with information in that regard.***

Amendment 12

Proposal for a directive
Recital 10 a (new)

Text proposed by the Commission	*Amendment*
	(10a) The Commission should also issue guidelines to support Member States in correctly implementing the provisions on the scope, and to evaluate the proportionality of the obligations set out by this Directive, in particular as regards entities with complex business models or operating environments, whereby an entity may simultaneously fulfil the criteria assigned to both essential and important entities, or may simultaneously conduct activities that are some within and some outside the scope of this Directive.

Amendment 13

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents ***or significant cyber threats*** of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ***may*** issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been	(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. ***Sector-specific Union legal acts that require essential or important entities to adopt cybersecurity risk management measures or to report significant incidents, should, where possible, be consistent with the terminology, and refer to the definitions laid down in this Directive.*** Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents***, and where those requirements are*** of at least an equivalent effect to the obligations laid down in this Directive***, and apply to the entirety of the security aspects of the operations and services provided by essential and important entities***, those sector-specific

conferred to the Commission in a number of sectors, including transport and energy.

provisions, including on supervision and enforcement, should apply. The Commission ***should*** issue ***comprehensive*** guidelines in relation to the implementation of the lex specialis***, taking into account relevant opinions, expertise and best practices of ENISA and the Cooperation Group***. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications ***that duly take into account the need for a comprehensive and consistent cybersecurity framework.*** This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

Amendment 14

Proposal for a directive
Recital 14

Text proposed by the Commission	*Amendment*
(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent ***authority*** under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information, particularly in relation to the identification	(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent ***authorities within and between Member States,*** under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information ***without undue***

of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose.	***delay***, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information ***where possible in real time,*** for this purpose.
[17] [insert the full title and OJ publication reference when known]	[17] [insert the full title and OJ publication reference when known]

Amendment 15

Proposal for a directive
Recital 15

Text proposed by the Commission	*Amendment*
(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to ***all providers of DNS services along the DNS resolution chain, including operators of root name servers,*** top-level-domain (TLD) name servers, authoritative name servers ***for domain names and recursive resolvers***.	(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to top-level-domain (TLD) name servers, ***publicly available recursive domain name resolution services for internet end-users and*** authoritative ***domain name resolution services. This Directive does not apply to root*** name servers.

Amendment 16

Proposal for a directive
Recital 19

Text proposed by the Commission	*Amendment*
(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council[18] , as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services. Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services.	(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council[18], as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services***, while taking into account the degree of their dependence on network and information systems***. Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services.
[18] Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998, p. 14).	[18] Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998, p. 14).

Amendment 17

Proposal for a directive
Recital 20

Text proposed by the Commission	*Amendment*
(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or	(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or

operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic ***has*** shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.

operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The ***intensified attacks against network and information systems during the*** COVID-19 pandemic ***have*** shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.

Amendment 18

Proposal for a directive
Recital 24

Text proposed by the Commission	*Amendment*
(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ensure that they ***have*** well-functioning ***CSIRTs, also known as computer emergency response teams ('CERTs')***, complying with essential requirements in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. In view of enhancing the trust relationship between the entities and the CSIRTs, in cases where a CSIRT is part of the competent authority, Member States should consider functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities.	(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ***designate one or more CSIRTs under this Directive and ensure that they are well-functioning***, complying with essential requirements in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. ***Member States may designate existing computer emergency response teams (CERTs) as CSIRTs.*** In view of enhancing the trust relationship between the entities and the CSIRTs, in cases where a CSIRT is part of the competent authority, Member States should consider functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities.

Amendment 19

Proposal for a directive
Recital 25

Text proposed by the Commission	*Amendment*
(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] as regards personal data, on behalf of and upon request by an entity under this Directive, a proactive scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.	(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] as regards personal data, on behalf of and upon request by an entity under this Directive***, or, in the case of a serious threat to national security***, a proactive scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.
[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).	[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

Amendment 20

Proposal for a directive
Recital 25 a (new)

Text proposed by the Commission	*Amendment*
	(25a) CSIRTs should have the ability to, upon an entity's request, continuously discover, manage and monitor all internet-facing assets, both on premises and off premises, to understand their overall organisational risk to newly discovered supply chain compromises or

critical vulnerabilities. The knowledge whether an entity runs a privileged management interface, affects the speed of undertaking mitigating actions.

Amendment 21

Proposal for a directive
Recital 26

Text proposed by the Commission	*Amendment*
(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive.	(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks***, including with CSIRTs from third countries where information exchange is reciprocal and beneficial to the security of citizens and entities,*** in addition to the CSIRTs network established by this Directive***, in order to contribute to the development of Union standards that can shape the cybersecurity landscape at international level. Member States could also explore the possibility of increasing cooperation with like-minded partner countries and international organisations with the aim to secure multilateral agreements on cyber norms, responsible state and non-state behaviour in cyberspace and effective global digital governance as well as to create an open, free, stable and secure cyberspace based on international law.***

Amendment 22

Proposal for a directive
Recital 26 a (new)

Text proposed by the Commission	*Amendment*
	(26a) Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application

	security, and business or end-user data on which entities rely upon. Cyber hygiene policies comprising a common baseline set of practices including, but not limited to, software and hardware updates, password changes, management of new installs, limitation of administrator-level access accounts, and backing up of data, enable a proactive framework of preparedness and overall safety and security in the event of incidents or threats. ENISA should monitor and assess Member States' cyber hygiene policies, and explore Union wide schemes to enable cross-border checks ensuring equivalence independent of Member State requirements.

Amendment 23

Proposal for a directive
Recital 26 b (new)

Text proposed by the Commission	*Amendment*
	(26b) The use of artificial intelligence (AI) in cybersecurity has the potential of improving the detection and to stop attacks against network and information systems, enabling resources to be diverted towards more sophisticated attacks. Member States should therefore encourage in their national strategies the use of (semi-)automated tools in cybersecurity and the sharing of data needed to train and improve automated tools in cybersecurity. In order to mitigate risks of unduly interference with the rights and freedoms of individuals that AI-enabled systems might pose, the requirements of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679 shall apply. Integrating appropriate safeguards such as pseudonymisation, encryption, data accuracy and data minimisation could furthermore mitigate such risks.

Amendment 24

Proposal for a directive
Recital 26 c (new)

Text proposed by the Commission	*Amendment*
	(26c) Open-source cybersecurity tools and applications can contribute to a higher degree of transparency and can have a positive impact on the efficiency of industrial innovation. Open standards facilitate interoperability between security tools, benefitting the security of industrial stakeholders. Open-source cybersecurity tools and applications can leverage the wider developer community, enabling entities to pursue vendor diversification and open security strategies. Open security can lead to a more transparent verification process of cybersecurity related tools and a community-driven process of discovering vulnerabilities. Member States should therefore promote the adoption of open-source software and open standards by pursuing policies relating to the use of open data and open-source as part of security through transparency. Policies promoting the adoption and sustainable use of open-source cybersecurity tools are of particular importance for small and medium-sized enterprises (SMEs) facing significant costs for implementation, which could be minimised by reducing the need for specific applications or tools.

Amendment 25

Proposal for a directive
Recital 26 d (new)

Text proposed by the Commission	*Amendment*
	(26d) Public-Private Partnerships (PPPs) in the field of cybersecurity can provide the right framework for knowledge exchange, sharing of best practices and the establishment of a

common level of understanding among all stakeholders. Member States should adopt policies underpinning the establishment of cybersecurity-specific PPPs as part of their national cybersecurity strategies. Those policies should clarify, inter alia, the scope and stakeholders involved, the governance model, the available funding options and the interaction among participating stakeholders. PPPs can leverage the expertise of private sector entities to support Member States' competent authorities in developing state-of-the art services and processes including, but not limited to, information exchange, early warnings, cyber threat and incident exercises, crisis management, and resilience planning.

Amendment 26

Proposal for a directive
Recital 27

Text proposed by the Commission	*Amendment*
(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20] , a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.	(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20], a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market ***or posing serious public security and safety risks for entities or citizens in several Member States or the Union as a whole***. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate

the response across the Union.

[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

Amendment 27

Proposal for a directive
Recital 27 a (new)

Text proposed by the Commission	*Amendment*
	(27a) Member States should, in their national cybersecurity strategies, address specific cybersecurity needs of SMEs. SMEs represent, in the Union context, a large percentage of the industrial and business market and they are often struggling to adapt to new business practices in a more connected world, navigating the digital environment, with employees working from home and business increasingly being conducted online. Some SMEs face specific cybersecurity challenges such as low cyber-awareness, a lack of remote IT security, the high cost of cybersecurity solutions and an increased level of threat, such as ransomware, for which they should receive guidance and support. Member States should have a cybersecurity single point of contact for SMEs, which either provides guidance and support to SMEs or directs them to the appropriate bodies for guidance and support on cybersecurity related issues. Member States are encouraged to also offer services such as website configuration and logging enabling to small enterprises and microenterprises that lack those capabilities.

Amendment 28

Proposal for a directive
Recital 27 b (new)

Text proposed by the Commission	*Amendment*
	(27b) Member States should adopt policies on the promotion of active cyber defence as part of their national cybersecurity strategies. Active cyber defence is the proactive prevention, detection, monitoring, analysis and mitigation of network security breaches, combined with the use of capabilities deployed within and outside the victim network. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enabling a unity of effort in successfully detecting, preventing and addressing attacks against network and information systems. Active cyber defence is based on a defensive strategy that excludes offensive measures against critical civilian infrastructure.

Amendment 29

Proposal for a directive
Recital 28

Text proposed by the Commission	*Amendment*
(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third	(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third

parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC 29417 provide guidance on vulnerability handling and vulnerability disclosure respectively. ***As regards vulnerability disclosure,*** coordination between reporting entities and manufacturers or providers of ICT products or services is particularly important. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also comprise coordination between the reporting entity and the organisation as regards the timing of remediation and publication of vulnerabilities.

parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC 29417 provide guidance on vulnerability handling and vulnerability disclosure respectively. ***Strengthening the*** coordination between reporting entities and manufacturers or providers of ICT products or services is particularly important ***to facilitate the voluntary framework of vulnerability disclosure***. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also comprise coordination between the reporting entity and the organisation as regards the timing of remediation and publication of vulnerabilities.

Amendment 30

Proposal for a directive
Recital 28 a (new)

Text proposed by the Commission	*Amendment*
	(28a) The Commission, ENISA and the Member States should continue to foster international alignment with standards and existing industry best practices in the area of risk management, for example in the areas of supply chain security assessments, information sharing and vulnerability disclosure.

Amendment 31

Proposal for a directive
Recital 29

Text proposed by the Commission	*Amendment*
(29) Member States should therefore take measures to facilitate coordinated	(29) Member States***, in cooperation with ENISA,*** should therefore take

vulnerability disclosure by establishing a relevant national policy. In ***this regard***, Member States should ***designate a CSIRT to take the role of 'coordinator', acting as an intermediary between the reporting*** entities and ***the manufacturers or providers of ICT products or services where necessary. The tasks of the CSIRT coordinator should in particular include identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure timelines, and managing*** vulnerabilities ***that affect multiple organisations (multi-party vulnerability disclosure). Where vulnerabilities affect multiple manufacturers or providers of ICT products or services established in more than one*** Member ***State, the designated CSIRTs from each of the affected*** Member States ***should cooperate within the CSIRTs Network***.

measures to facilitate coordinated vulnerability disclosure by establishing a relevant national policy. In ***that national policy***, Member States should ***address problems encountered by vulnerability researchers.*** Entities and ***natural persons researching*** vulnerabilities ***may in some*** Member ***States be exposed to criminal and civil liability.*** Member States ***are therefore encouraged to issue guidelines as regards the non-prosecution of information security research and an exemption from civil liability for those activities.***

Amendment 32

Proposal for a directive
Recital 29 a (new)

Text proposed by the Commission	*Amendment*
	(29a) Member States should designate a CSIRT to take the role of 'coordinator', acting as an intermediary between the reporting entities and the manufacturers or providers of ICT products or services, which are likely to be affected by the vulnerability, where necessary. The tasks of the CSIRT coordinator should in particular include identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure timelines, and managing vulnerabilities that affect multiple organisations (multi-party vulnerability disclosure). Where vulnerabilities affect multiple manufacturers or providers of ICT products or services established in more than one Member State, the designated CSIRTs from each of the affected

Member States should cooperate within the CSIRTs Network.

Amendment 33

Proposal for a directive
Recital 30

Text proposed by the Commission	*Amendment*
(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. ***In that regard,*** sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability ***registry*** where, essential and important entities and their suppliers, as well as entities which do not fall ***in*** the scope of application of this Directive may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures.	(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. Sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also ***for*** national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability ***database*** where, essential and important entities and their suppliers, as well as entities which do not fall ***within*** the scope of application of this Directive may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures. ***The aim of that database is to address the unique challenges posed by cybersecurity risks to European entities. Furthermore, ENISA should establish a responsible procedure regarding the publication process, in order to give entities the time to take mitigating measures as regards their vulnerabilities, and employ state of the art cybersecurity measures, as well as machine-readable datasets and corresponding interfaces (API). To encourage a culture of disclosure of vulnerabilities a disclosure should be without detriment of the reporting entity.***

Amendment 34

Proposal for a directive
Recital 31

Text proposed by the Commission	*Amendment*
(31) ***Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A*** European vulnerability ***registry*** maintained by ENISA ***would provide improved transparency regarding the publication process before the vulnerability is officially disclosed***, ***and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible***, ENISA should explore the possibility ***of entering*** into structured cooperation agreements with similar registries ***in*** third country jurisdictions.	(31) ***The*** European vulnerability ***database*** maintained by ENISA ***should leverage the Common Vulnerabilities and Exposures (CVE) registry, through the use of its framework for identification***, ***tracking and scoring of vulnerabilities. Furthermore***, ENISA should explore the possibility ***to enter*** into structured cooperation agreements with ***other*** similar registries ***or databases under the*** third country jurisdictions***, to avoid duplications of efforts and to seek complementarity***.

Amendment 35

Proposal for a directive
Recital 33

Text proposed by the Commission	*Amendment*
(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of existing rules.	(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations***, in particular as regards facilitating the alignment in the transposition of this Directive among Member States,*** to be addressed through better implementation of existing rules. ***The Cooperation Group should also map the national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across the Union. This is particularly relevant for the sectors that have an international and cross-border nature.***

Amendment 36

Proposal for a directive
Recital 34

Text proposed by the Commission	*Amendment*
(34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should consider inviting Union bodies and agencies involved in cybersecurity policy, such as ***the European Cybercrime Centre (EC3)***, the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.	(34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should consider inviting ***relevant*** Union bodies and agencies involved in cybersecurity policy, such as ***Europol***, the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.

Amendment 37

Proposal for a directive
Recital 35

Text proposed by the Commission	*Amendment*
(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes for officials from other Member States in order to improve cooperation. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the activities of the host competent authority.	(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes for officials from other Member States***, within structured rules and mechanisms underpinning the scope and, where applicable, the required security clearance of officials participating in such exchange schemes,*** in order to improve cooperation ***and strengthen trust among Member States***. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the activities of the host competent authority ***or CSIRT***.

Amendment 38

Proposal for a directive
Recital 36

Text proposed by the Commission	*Amendment*
(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. Such agreements should ensure adequate protection of data.	(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. Such agreements should ensure ***Union's interests and*** adequate protection of data. ***This shall not preclude the right of Member States to cooperate with likeminded third countries on management of vulnerabilities and cyber security risk management, facilitating reporting and general information sharing in accordance with Union law.***

Amendment 39

Proposal for a directive
Recital 38

Text proposed by the Commission	*Amendment*
(38) For the purposes of this Directive, the term 'risk' should refer to the potential for loss or disruption caused by a cybersecurity incident and should be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of said incident.	***deleted***

Amendment 40

Proposal for a directive
Recital 39

Text proposed by the Commission	*Amendment*
(39) For the purposes of this Directive,	***deleted***

the term 'near misses' should refer to an event which could potentially have caused harm, but was successfully prevented from fully transpiring.

Amendment 41

Proposal for a directive
Recital 40

Text proposed by the Commission	*Amendment*
(40) Risk-management measures should include measures to identify any risks of incidents, to prevent, detect ***and handle*** incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data.	(40) Risk-management measures should include measures to identify any risks of incidents, to prevent, detect***, respond to and recover from*** incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data. ***Those systems should provide for systemic analysis, breaking down the various processes and the interactions between subsystems and taking into account the human factor, in order to have a complete picture of the security of the information system.***

Amendment 42

Proposal for a directive
Recital 41

Text proposed by the Commission	*Amendment*
(41) In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the cybersecurity risk management requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures.	(41) In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the cybersecurity risk management requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures ***and European or international standards, such as ISO31000 and ISA/IEC 27005***.

Amendment 43

Proposal for a directive
Recital 43

Text proposed by the Commission	*Amendment*
(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to ***cyber-attacks*** and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers***, such as providers of data storage and processing services or managed security services,*** is particularly important given the prevalence of incidents where entities have fallen victim to ***attacks against network and information systems*** and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality ***and resilience*** of products ***and services, the cybersecurity measures embedded in them, and the*** cybersecurity practices of their suppliers and service providers, including their secure development procedures. ***Entities should in particular be encouraged to incorporate cybersecurity measures into contractual arrangements with their first-level suppliers and service providers. Entities could consider cybersecurity risks stemming from other levels of suppliers and service providers.***

Amendment 44

Proposal for a directive
Recital 44

Text proposed by the Commission	*Amendment*
(44) Among service providers, managed security services providers (MSSPs) in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to detect ***and*** respond to incidents. Those MSSPs have however also been the targets of	(44) Among service providers, managed security services providers (MSSPs) in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to ***prevent,*** detect***,*** respond to ***or recover from*** incidents. Those MSSPs have however also

cyberattacks themselves and through their close integration in the operations of operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP.	been the targets of cyberattacks themselves and through their close integration in the operations of operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP.

Amendment 45

Proposal for a directive
Recital 45

Text proposed by the Commission	*Amendment*
(45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of the entities, when relying on data transformation and data analytics services from third parties, the entities should take all appropriate cybersecurity measures.	(45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem***, including to counter industrial espionage and to protect trade secrets***. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of the entities, when relying on data transformation and data analytics services from third parties, the entities should take all appropriate cybersecurity measures.

Amendment 46

Proposal for a directive
Recital 45 a (new)

Text proposed by the Commission	*Amendment*
	(45a) Entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust architecture, software updates, device configuration, network segmentation, identity and access management or user awareness, and

organise training for their staff regarding corporate email cyber threats, phishing or social engineering techniques. Furthermore, entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies driven by artificial intelligence or machine learning systems to automate their capabilities and the protection of network architectures.

Amendment 47

Proposal for a directive
Recital 46

Text proposed by the Commission	*Amendment*
(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated ***sectoral*** supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21] , with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.	(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21] , with the aim of identifying per sector which are the critical ICT ***and ICS*** services, systems or products, relevant threats and vulnerabilities. ***Such risk assessments should identify measures, mitigation plans and best practices against critical dependencies, potential single points of failure, threats, vulnerabilities and other risks associated with the supply chain and should explore ways to further encourage their wider adoption by entities. Potential non-technical risk factors, such as undue influence by a third country on suppliers and service providers, in particular in the case of alternative models of governance, include concealed vulnerabilities or backdoors and potential systemic supply disruptions, in particular in case of***

technological lock-in or provider dependency.

[21] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

[21] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

Amendment 48

Proposal for a directive
Recital 47

Text proposed by the Commission	*Amendment*
(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities.	(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products ***throughout their entire lifecycle*** against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities. ***Furthermore, particular emphasis should be placed on ICT services, systems or products that are subject to specific requirements stemming from third***

countries.

Amendment 49

Proposal for a directive
Recital 47 a (new)

Text proposed by the Commission	*Amendment*
	(47a) The Stakeholder Cybersecurity Certification Group established pursuant to Article 22 of Regulation (EU) 2019/881 of the European Parliament and of the Council[1a] should issue an opinion on security risk assessments of specific critical ICT and ICS services, systems or products supply chains. The Cooperation Group and ENISA should take into account that opinion.
	[1a] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)(OJ L 151, 7.6.2019, p.15).

Amendment 50

Proposal for a directive
Recital 50

Text proposed by the Commission	*Amendment*
(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security of network and information systems appropriate to the risk posed. Given that	(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security of network and information systems appropriate to the risk posed. Given that

providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission.	providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk ***to network security*** for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission. ***However, as the attack surface continues to expand, number-independent interpersonal communications services including, but not limited to, social media messengers, are becoming popular attack vectors. Malicious actors use platforms to communicate and attract victims to open compromised web pages, therefore increasing the likelihood of incidents involving the exploitation of personal data, and by extension, the security of information systems.***

Amendment 51

Proposal for a directive
Recital 51

Text proposed by the Commission	*Amendment*
(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto.	(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that ***all*** public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report ***significant*** incidents in relation thereto. ***Member States should ensure that the integrity and availability of those public electronic***

	communications networks are maintained and should consider their protection from sabotage and espionage of vital security interest. Information about incidents, for example on submarine communication cables should be shared actively between Member States.

Amendment 52

Proposal for a directive
Recital 52

Text proposed by the Commission	*Amendment*
(52) Where appropriate, entities should inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. ***The requirement to inform those recipients of such threats*** should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge.	(52) Where appropriate, entities should inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. ***This*** should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge ***and drafted in an easily comprehensible language***.

Amendment 53

Proposal for a directive
Recital 53

Text proposed by the Commission	*Amendment*
(53) ***In particular,*** providers of public electronic communications networks or publicly available electronic communications services, should inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their communications, for instance by using specific types of software or ***encryption*** technologies.	(53) Providers of public electronic communications networks or publicly available electronic communications services, should ***implement security by design and by default, and*** inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their ***devices and*** communications, for instance by using specific types of ***encryption*** software or ***other data-centric security***

technologies.

Amendment 54

Proposal for a directive
Recital 54

Text proposed by the Commission	*Amendment*
(54) In order to safeguard the security of electronic communications networks and services, the use of encryption***, and in particular end-to-end encryption***, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. ***Solutions for lawful access to information in*** end-to-end ***encrypted communications should maintain the effectiveness of*** encryption ***in protecting privacy and security of communications, while providing an*** effective ***response to crime***.	(54) In order to safeguard the security of electronic communications networks and services, the use of encryption ***and other data-centric security technologies, such as, tokenisation, segmentation, throttle access, marking, tagging, strong identity and access management, and automated access decisions***, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. ***However, this should not lead to any efforts to weaken*** end-to-end encryption***, which is a critical technology for*** effective ***data protection and privacy***.

Amendment 55

Proposal for a directive
Recital 54 a (new)

Text proposed by the Commission	*Amendment*
	(54a) In order to safeguard the security and to prevent abuse and manipulation of electronic communications networks and services, the use of interoperable secure routing standards should be promoted to ensure the integrity and robustness of routing functions across the ecosystem of internet carriers.

Amendment 56

Proposal for a directive
Recital 54 b (new)

Text proposed by the Commission	*Amendment*
	(54b) In order to safeguard the functionality and integrity of the internet and to reduce security issues relating to DNS, relevant stakeholders including Union businesses, internet service providers and browser vendors should be couraged to adopt a DNS resolution diversification strategy. Furthermore, Member States should encourage the development and use of a public and secure European DNS resolver service.

Amendment 57

Proposal for a directive
Recital 55

Text proposed by the Commission	*Amendment*
(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification ***within 24 hours,*** followed by a ***final*** report not later than one month after***.*** The initial notification ***should only include the information strictly necessary to make the competent authorities aware of the*** incident ***and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member***	(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification followed by a ***comprehensive*** report not later than one month after ***the submission of*** the initial notification***. The initial*** incident notification ***timeline should not preclude entities from*** reporting ***incidents earlier, therefore allowing them to seek support from CSIRTs swiftly enabling the mitigation and the potential spread of the reported*** incident***. CSIRTs can request an intermediate report on***

States should ensure that the requirement to submit this initial notification ***does not divert the*** reporting ***entity's resources from activities related to incident handling that should be prioritised. To further prevent that*** incident ***reporting obligations either divert resources from*** incident response ***handling or may otherwise compromise the entities*** efforts ***in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the*** entity ***concerned can deviate from the deadlines of 24 hours for the initial notification and one month for the final report***.

relevant status updates, while taking into account the incident response ***and remediation*** efforts ***of the reporting*** entity.

Amendment 58

Proposal for a directive
Recital 55 a (new)

Text proposed by the Commission	*Amendment*
	(55a) A significant incident may have an impact on the confidentiality, integrity or availability of the service. Essential and important entities should notify CSIRTs about significant incidents that have an impact on the availability of their service within 24 hours of becoming aware of the incident. They should notify CIRTs about significant incidents that breach the confidentiality and integrity of their services within 72 hours of becoming aware of the incident. The distinction between the types of incidents is not based on the seriousness of the incident, but on the difficulty for the reporting entity to assess the incident, its significance and the ability to report information that can be of use for the CSIRT. The initial notification should include the information necessary to make the CSIRT aware of the incident and allow the entity to seek assistance, if required. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources

from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the CSIRT, the entity concerned can deviate from the deadlines for the initial notification and for the comprehensive report.

Amendment 59

Proposal for a directive
Recital 59

Text proposed by the Commission	*Amendment*
(59) Maintaining accurate and complete databases of domain names ***and*** registration data (so called 'WHOIS data') ***and providing lawful access to such data*** is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.	(59) Maintaining accurate***, verified*** and complete databases of domain names registration data (so called 'WHOIS data') is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union***, and for tackling illegal activities***. ***TLD registries and entities providing domain name registration services should therefore be required to collect domain name registration data, which should include at least the registrants' name, their physical and email address as well as their telephone number. In practice, the collected data may not always be thoroughly accurate, however TLD registries and entities providing domain name registration services should adopt and implement proportionate processes to verify that natural or legal persons requesting or owning a domain name have provided contact details on which they can be reached and are expected to reply. Using a 'best efforts' approach, those verification processes should reflect the current best practices used within the industry. Those best practices in the verification process should reflect the***

advances being made in the electronic identification process. The TLD registries and entities providing domain name registration services should make publicly available their policies and procedures to ensure the integrity and availability of the domain name registration data. Where processing includes personal data such processing shall comply with Union data protection law.

Amendment 60

Proposal for a directive
Recital 60

Text proposed by the Commission	*Amendment*
(60) The availability and timely accessibility of ***these data to public authorities, including*** competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs***, (***CSIRTs***, and as regards the data of their clients to providers of electronic communications networks and services and providers of cybersecurity technologies and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents. Such access should comply with Union data protection law insofar as it is related to personal data.***	(60) The availability and timely accessibility of ***the domain name registration data to legitimate access seekers is essential for cybersecurity purposes and tackling illegal activities in the online ecosystem. TLD registries and entities providing domain name registration services should therefore be required to enable lawful access to specific domain name registration data, including personal data, to legitimate access seekers, in accordance with Union data protection law. Legitimate access seekers should make a duly justified request to access domain name registration data on the basis of Union or national law, and could include*** competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, ***and national*** CERTs ***or*** CSIRTs***. Member States should ensure that TLD registries and entities providing domain name registration services should respond without undue delay and in any event within 72 hours to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and entities providing domain name registration services should establish policies and procedures for the publication and disclosure of registration***

	data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tools to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board.

Amendment 61

Proposal for a directive
Recital 61

Text proposed by the Commission	*Amendment*
(61) In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the entities providing domain name registration services for the TLD (so-called registrars) should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules.	***deleted***

Amendment 62

Proposal for a directive
Recital 62

Text proposed by the Commission	*Amendment*
(62) TLD registries and ***the*** entities	(62) TLD registries and entities

providing domain name registration services ***for them*** should ***make publically*** available domain name registration data that ***fall outside the scope of Union data protection rules, such as data that concern*** legal persons[25] . TLD registries and ***the*** entities ***providing domain name registration services for the TLD*** should ***also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States*** should ***ensure that TLD registries and the entities providing domain name registration services for them*** should ***respond without undue delay to requests from legitimate access seekers for the disclosure of domain name registration data.*** TLD registries and ***the*** entities providing domain name registration services ***for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board.***

providing domain name registration services should ***be required to make publicly*** available domain name registration data that ***does not contain personal data. A distinction should be made between natural and*** legal persons[25]. ***For legal persons,*** TLD registries and entities should ***make publicly available at least the registrants' name, their physical and email address as well as their telephone number. The legal person*** should ***be required to either provide a generic email address that can be made publicly available or give consent to the publication of a personal email address. The legal person*** should ***be able to demonstrate such consent at the request of*** TLD registries and entities providing domain name registration services***.***

---

[25] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL recital (14) whereby "this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person".

[25] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL recital (14) whereby "this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person".

Amendment 63

Proposal for a directive
Recital 63

Text proposed by the Commission	*Amendment*
(63) All essential and important entities under this Directive should 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 should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions.	(63) All essential and important entities under this Directive should fall under the jurisdiction of the Member State where they provide their services ***or carry out their activities***. If the entity provides services in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions.

Amendment 64

Proposal for a directive
Recital 64

Text proposed by the Commission	*Amendment*
(64) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located	(64) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located

in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.

in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where ***either*** the entity has an establishment with the highest number of employees in the Union ***or the establishment where cybersecurity operations are carried out***. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.

Amendment 65

Proposal for a directive
Recital 65 a (new)

Text proposed by the Commission	*Amendment*
	(65a) ENISA should create and maintain a registry containing information about essential and important entities that comprise DNS service providers, TLD name registries and providers of cloud computing services, data centre services, content delivery networks, online marketplaces, online search engines and social networking platforms. Those essential and important entities should submit to ENISA their names, addresses and up-to-date contact details. They should notify ENISA about any changes to those details without delay and, in any event, within two weeks from the date on which the change took effect. ENISA should forward the information to the relevant single point of contact. The

essential and important entities submitting their information to ENISA are therefore not required to separately inform the competent authority within the Member State. ENISA should develop a simple publicly available application programme that those entities could use to update their information. Furthermore, ENISA should 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.

Amendment 66

Proposal for a directive
Recital 66

Text proposed by the Commission	*Amendment*
(66) Where information considered classified ***according to*** national or Union law is exchanged, reported or otherwise shared under the provisions of this Directive, the corresponding specific rules on the handling of classified information should be applied.	(66) Where information considered classified ***in accordance with*** national or Union law is exchanged, reported or otherwise shared under the provisions of this Directive, the corresponding specific rules on the handling of classified information should be applied. ***In addition, ENISA should have the infrastructure, procedures and rules in place to handle sensitive and classified information in compliance with the applicable security rules for protecting EU classified information.***

Amendment 67

Proposal for a directive
Recital 68

Text proposed by the Commission	*Amendment*
(68) Entities should be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels	(68) Entities should be encouraged ***and supported by Member States*** to collectively leverage their individual knowledge and practical experience at

with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules.

strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive***, such as entities focusing on cybersecurity services and research,*** to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules.

Amendment 68

Proposal for a directive
Recital 69

Text proposed by the Commission	*Amendment*
(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, ***public authorities, CERTs,*** CSIRTs***,*** and providers of security technologies and services ***should constitute a*** legitimate ***interest*** of the ***data controller concerned,*** as referred to in Regulation (EU) 2016/679. ***That should include*** measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools***. Such measures may*** require the processing of ***the following types*** of	(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by ***essential and important*** entities, CSIRTs and providers of security technologies and services***, is necessary for compliance with their legal obligations provided for in this Directive. Such processing of personal data might also be necessary for the purposes of the*** legitimate ***interests pursued by essential and important entities. Where this Directive requires the processing of personal data for the purpose of cybersecurity and network and information security in accordance with the provisions set out in Article 18, 20 and 23*** of the ***Directive, that processing is considered to be necessary for compliance with a legal obligation*** as referred to in ***Article 6(1), point (c) of*** Regulation (EU) 2016/679. ***For the purpose of Article 26 and 27 of this Directive, processing, as referred to in Article 6(1), point (f) of***

personal data*:* IP addresses, uniform resources locators (URLs), domain names, ***and*** email addresses.

Regulation (EU) 2016/679, is considered to be necessary for the purposes of the legitimate interests pursued by the essential and important entities. Measures related to the prevention, detection***, identification, containment***, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools require the processing of ***certain categories*** of personal data***, such as*** IP addresses, uniform resources locators (URLs), domain names, email addresses***, time stamps, Operation System- or browser-related information, cookies or other information indicating the modus operandi***.

Amendment 69

Proposal for a directive
Recital 71

Text proposed by the Commission	*Amendment*
(71) In order to make enforcement effective, a minimum list of administrative ***sanctions*** for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such ***sanctions*** across the Union. Due regard should be given to the nature, gravity and duration of the infringement, the ***actual*** damage caused or losses incurred ***or potential damage or losses that could have been triggered***, the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority	(71) In order to make enforcement effective, a minimum list of administrative ***penalties*** for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such ***penalties*** across the Union. Due regard should be given to the nature, gravity and duration of the infringement, the damage caused or losses incurred, the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The penalties***,*** including

and any other aggravating or mitigating factor. The ***imposition of*** penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection ***and*** due process.	administrative fines***, should be proportionate and their imposition*** should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union ***(the 'Charter')***, including effective judicial protection***,*** due process***, the presumption of innocence and the rights of defence***.

Amendment 70

Proposal for a directive
Recital 72

Text proposed by the Commission	*Amendment*
(72) In order to ensure effective enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of administrative fines.	(72) In order to ensure effective enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of administrative fines ***if the infringement was intentional, negligent or the entity concerned had received notice of the entity's non-compliance***.

Amendment 71

Proposal for a directive
Recital 76

Text proposed by the Commission	*Amendment*
(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply ***sanctions consisting of the*** suspension of a certification or authorisation concerning part or all ***the*** services provided by an essential entity and the ***imposition of*** a temporary ban from the exercise of managerial functions by a natural person. Given their severity and impact on the entities' activities and ultimately on their consumers, such ***sanctions*** should only be	(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply ***a temporary*** suspension of a certification or authorisation concerning part or all ***relevant*** services provided by an essential entity and the ***request to impose*** a temporary ban from the exercise of managerial functions by a natural person ***at chief executive officer or legal representative level***. ***Member States should develop specific procedures and***

applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such ***sanctions*** should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such ***sanctions*** were applied. The imposition of such ***sanctions*** shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter ***of Fundamental Rights of the European Union,*** including effective judicial protection, due process, presumption of innocence and right of defence.

rules concerning the temporary ban from the exercise of managerial functions by a natural person at chief executive officer or legal representative level in public administration entities. In the process of developing such procedures and rules, Member States should take into account the particularities of their respective levels and systems of governance within their public administrations. Given their severity and impact on the entities' activities and ultimately on their consumers, such ***temporary suspensions or bans*** should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such ***temporary suspensions or bans*** should only be applied as ultima ratio, meaning only after the other ***relevant enforcement*** actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such ***temporary suspensions or bans*** were applied. The imposition of such ***temporary suspensions or bans*** shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection, due process, presumption of innocence and right of defence.

Amendment 72

Proposal for a directive
Recital 79

Text proposed by the Commission	*Amendment*
(79) A peer-review mechanism should be introduced, allowing the assessment by experts designated by the Member States	(79) A peer-review mechanism should be introduced, allowing the assessment by ***independent*** experts designated by the

of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources.	Member States**,** of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources. ***Peer-reviews can lead to valuable insights and recommendations strengthening the overall cybersecurity capabilities. In particular, they can contribute in facilitating the transfer of technologies, tools, measures and processes among the Member States involved in the peer-review, creating a functional path for the sharing of best practices across Member States with different levels of maturity in cybersecurity, and enabling the establishment of a high, common level of cybersecurity across the Union. The peer-review should be preceded by a self-assessment by the Member State under review, covering the reviewed aspects and any additional targeted issues communicated by the designated experts to the Member State under peer-review prior to the commencement of the process. The Commission, in cooperation with ENISA and the Cooperation Group, should develop templates for the self-assessment of the reviewed aspects in order to streamline the process and avoid procedural inconsistencies and delays, which Member States under peer-review should complete and provide to the designated experts carrying out the peer-review prior to the commencement of the peer-review process.***

Amendment 73

Proposal for a directive
Recital 80

Text proposed by the Commission	*Amendment*
(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk	(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to

management measures required by this Directive. The Commission should also be empowered to adopt delegated acts establishing which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making***[26]*** . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

cybersecurity risk management measures ***and reporting obligations*** required by this Directive. The Commission should also be empowered to adopt delegated acts establishing which categories of essential ***and important*** entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

---

[26] OJ L 123, 12.5.2016, p. 1.

Amendment 74

Proposal for a directive
Recital 81

Text proposed by the Commission	*Amendment*
(81) In order to ensure uniform conditions for the implementation of the relevant provisions of this Directive concerning the procedural arrangements necessary for the functioning of the Cooperation Group***, the technical elements related to risk management measures or the type of information, the format*** and the procedure of incident notifications, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European	(81) In order to ensure uniform conditions for the implementation of the relevant provisions of this Directive concerning the procedural arrangements necessary for the functioning of the Cooperation Group and the procedure of incident notifications, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.[27]

Parliament and of the Council.[27]

[27] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

[27] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

Amendment 75

Proposal for a directive
Recital 82

Text proposed by the Commission	*Amendment*
(82) The Commission should periodically review this Directive, in consultation with interested parties, in particular with a view to determining ***the need for modification*** in the light of changes to societal, political, technological or market conditions.	(82) The Commission should periodically review this Directive, in consultation with interested parties, in particular with a view to determining ***whether it is appropriate to propose amendments*** in the light of changes to societal, political, technological or market conditions. ***As part of those reviews, the Commission should assess the relevance of the sectors, subsectors and types of entities referred to in the annexes for the functioning of the economy and society in relation to cybersecurity. The Commission should assess, inter alia, whether digital providers that 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) or as gatekeepers as defined in Article 2, point 1 of Regulation (EU) XXXX/XXXX [Contestable and fair markets in the digital sector (Digital Markets Act)], should be designated as essential entities under this Directive. Furthermore, the Commission should assess whether it is appropriate to amend Annex I to the Directive 2020/1828 of the European Parliament and of the Council[1a] by***

adding a reference to this Directive.

[1a] Directive 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p.1).

Amendment 76
Proposal for a directive
Recital 82 a (new)

Text proposed by the Commission	*Amendment*
	(82a) This Directive lays down cybersecurity requirements for Member States as well as essential and important entities established in the Union. Those cybersecurity requirements should also be applied by the Union institutions, bodies, offices and agencies on the basis of a Union legislative act.

Amendment 77

Proposal for a directive
Recital 82 b (new)

Text proposed by the Commission	*Amendment*
	(82b) This Directive creates new tasks for ENISA, thereby enhancing its role, and could also result in ENISA being required to carry out its existing tasks under Regulation (EU) 2019/881 to a higher standard than before. In order to ensure that ENISA has the necessary financial and human resources to carry out existing and new activities under its tasks, as well as to satisfy any higher standard resulting from its enhanced role, its budget should be increased accordingly. In addition, in order to ensure the efficient use of resources,

	ENISA should be given greater flexibility in the way that it is permitted to allocate resources internally, so as to enable it to carry out its tasks, and to satisfy expectations, effectively.

Amendment 78

Proposal for a directive
Recital 84

Text proposed by the Commission	*Amendment*
(84) This Directive respects the fundamental rights, and observes the principles, recognised by the ***Charter of Fundamental Rights of the European Union***, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles**,**	(84) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This ***includes the right to an effective remedy before a court for the recipients of services provided by essential and important entities. This*** Directive should be implemented in accordance with those rights and principles**.**

Amendment 79

Proposal for a directive
Article 1 – paragraph 2 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) lays down supervision and enforcement obligations on Member States.

Amendment 80

Proposal for a directive
Article 2 – paragraph 1

Text proposed by the Commission	*Amendment*
1. This Directive applies to public and private entities of a type referred to as	1. This Directive applies to public and private ***essential and important*** entities of

essential entities in Annex I and as important entities in Annex II. This Directive does not apply to ***entities that qualify as micro and*** small enterprises within the meaning of Commission Recommendation 2003/361/EC.[28]	a type referred to as essential entities in Annex I and as important entities in Annex II ***that provide their services or carry out their activities within the Union***. This Directive does not apply to small enterprises ***or microenterprises*** within the meaning of ***Article 2(2) and (3) of the Annex to*** Commission Recommendation 2003/361/EC[28]. ***Article 3(4) of the Annex of that Recommendation is not applicable.***
[28] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	[28] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Amendment 81

Proposal for a directive
Article 2 – paragraph 2 – subparagraph 1 – introductory part

Text proposed by the Commission	*Amendment*
However, regardless of their size, this Directive also applies to entities ***referred to in Annexes I and II***, where:	Regardless of their size, this Directive also applies to ***essential and important*** entities, where:

Amendment 82

Proposal for a directive
Article 2 – paragraph 2 – subparagraph 1 – point d

Text proposed by the Commission	*Amendment*
(d) a ***potential*** disruption of the service provided by the entity could have an impact on public safety, public security or public health;	(d) a disruption of the service provided by the entity could have an impact on public safety, public security or public health;

Amendment 83

Proposal for a directive
Article 2 – paragraph 2 - subparagraph 1 – point e

Text proposed by the Commission	*Amendment*
(e) a ***potential*** disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;	(e) a disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;

Amendment 84

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

Text proposed by the Commission	*Amendment*
Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.	***deleted***

Amendment 85

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

Text proposed by the Commission	*Amendment*
	2a. By ... [6 months after the transposition deadline], Member States shall establish a list of essential and important entities, including the entities referred to in paragraph 1 and the entities identified pursuant to paragraph 2, points (b) to (f) and Article 24 (1). Member States shall review and, where appropriate update, that list, on a regular basis, and at least every two years thereafter.

Amendment 86

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

Text proposed by the Commission	*Amendment*
	2b. Member States shall ensure that essential and important entities submit at least the following information to competent authorities:
	(a) the name of the entity;
	(b) address and up-to-date contact details, including email addresses, IP ranges, telephone numbers; and
	(c) the relevant sector(s) and subsector(s) referred to in Annexes I and II.
	The essential and important entities shall notify any changes to the details submitted pursuant to the first subparagraph without delay, and, in any event, within two weeks from the date on which the change takes effect. To that end, the Commission, with the assistance of ENISA, shall without undue delay issue guidelines and templates regarding the obligations set out in this paragraph.

Amendment 87

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

Text proposed by the Commission	*Amendment*
	2c. By …[6 months after the transposition deadline] and every two years thereafter, Member States shall notify:
	(a) the Commission and the Cooperation Group of the number of all essential and important entities identified for each sector and subsector referred to in Annexes I and II, and
	(b) the Commission, of the names of the entities identified pursuant to paragraph 2, points (b) to (f).

Amendment 88

Proposal for a directive
Article 2 – paragraph 4

Text proposed by the Commission	*Amendment*
4. This Directive applies without prejudice to Council Directive 2008/114/EC[30] and Directives 2011/93/EU[31] ***and*** 2013/40/EU[32] of the European Parliament and of the Council.	4. This Directive applies without prejudice to Council Directive 2008/114/EC[30] and Directives 2011/93/EU[31]***,*** 2013/40/EU[32] ***and 2002/58/EC[32a]*** of the European Parliament and of the Council.
[30] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).	[30] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).
[31] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).	[31] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).
[32] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).	[32] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).
	[32a] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

Amendment 89

Proposal for a directive
Article 2 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Where provisions of sector–specific acts of Union law require essential or important entities ***either*** to adopt cybersecurity risk management measures or to notify incidents ***or significant cyber threats***, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.	6. Where provisions of sector–specific acts of Union law require essential or important entities to adopt cybersecurity risk management measures or to notify incidents, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply. ***The Commission shall, without undue delay, issue guidelines in relation to the implementation of the sector–specific acts of Union law in order to ensure that cybersecurity requirements established by this Directive are fulfilled by those acts and that there is no overlap or legal uncertainty. When preparing those guidelines, the Commission shall take into account the best practices and expertise of ENISA and the Cooperation Group.***

Amendment 90

Proposal for a directive
Article 2 – paragraph 6 a (new)

Text proposed by the Commission	*Amendment*
	6a. Essential and important entities, CSIRTs and providers of security technologies and services, shall process personal data, to the extent strictly necessary and proportionate for the purposes of cybersecurity and network and information security, to meet the obligations set out in this Directive. That processing of personal data under this Directive shall be carried out in compliance with Regulation (EU) 2016/679, in particular Article 6 thereof.

Amendment 91

Proposal for a directive
Article 2 – paragraph 6 b (new)

Text proposed by the Commission	*Amendment*
	6b. The processing of personal data pursuant to this Directive, providers of public electronic communications networks or providers of publicly available electronic communications referred to in Annex I, point 8, shall be carried out in accordance with Directive 2002/58/EC.

Amendment 92

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

Text proposed by the Commission	*Amendment*
	(4a) 'near miss' means an event which could have compromised the availability, authenticity, integrity or confidentiality of data, or could have caused harm, but was successfully prevented from producing their negative impact;

Amendment 93

Proposal for a directive
Article 4 – paragraph 1 – point 6

Text proposed by the Commission	*Amendment*
(6) 'incident handling' means all actions and procedures aiming at detection, analysis and containment of and a response to an incident;	(6) 'incident handling' means all actions and procedures aiming at ***prevention,*** detection, analysis***,*** and containment of and a response to an incident;

Amendment 94

Proposal for a directive
Article 4 – paragraph 1 – point 7a (new)

Text proposed by the Commission	*Amendment*
	(7a) 'risk' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident;

Amendment 95

Proposal for a directive
Article 4 – paragraph 1 – point 11

Text proposed by the Commission	*Amendment*
(11) 'technical specification' means a technical specification ***within the meaning of*** Article ***2(4)*** of Regulation (EU) ***No 1025/2012***;	(11) 'technical specification' means a technical specification ***as defined in*** Article ***2, point (20)*** of Regulation (EU) ***No 2019/881***;

Amendment 96

Proposal for a directive
Article 4 – paragraph 1 – point 13

Text proposed by the Commission	*Amendment*
(13) 'domain name system (DNS)' means a hierarchical distributed naming system which ***allows end-users to reach*** services and resources ***on the*** internet;	(13) 'domain name system (DNS)' means a hierarchical distributed naming system which ***enables the identification of internet*** services and resources***, allowing end-user devices to utilise*** internet ***routing and connectivity services, to reach those services and resources***;

Amendment 97

Proposal for a directive
Article 4 – paragraph 1 – point 14

Text proposed by the Commission	*Amendment*
(14) 'DNS service provider' means an entity that provides ***recursive or authoritative domain name resolution services to internet end-users and other***	(14) 'DNS service provider' means an entity that provides***:***

DNS service providers;

Amendment 98

Proposal for a directive
Article 4 – paragraph 1 – point 14 – point a (new)

Text proposed by the Commission	*Amendment*
	(a) open and public recursive domain name resolution services to internet end-users; or

Amendment 99

Proposal for a directive
Article 4 – paragraph 1 – point 14 – point b (new)

Text proposed by the Commission	*Amendment*
	(b) authoritative domain name resolution services as a service procurable by third-party entities;

Amendment 100

Proposal for a directive
Article 4 – paragraph 1 – point 15

Text proposed by the Commission	*Amendment*
(15) 'top–level domain name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers;	(15) 'top–level domain name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers***, irrespective of whether any of those operations are being performed by the entity or are outsourced***;

Amendment 101

Proposal for a directive
Article 4 – paragraph 1 – point 15 a (new)

Text proposed by the Commission	*Amendment*
	(15a) 'domain name registration services' means services provided by domain name registries and registrars, privacy or proxy registration service providers, domain brokers or resellers, and any other services which are related to the registration of domain names;

Amendment 102

Proposal for a directive
Article 4 – paragraph 1 – point 23 a (new)

Text proposed by the Commission	*Amendment*
	(23a) 'public electronic communications network' means a public electronic communications network as defined in Article 2, point (8) of Directive (EU) 2018/1972;

Amendment 103

Proposal for a directive
Article 4 – paragraph 1 – point 23 b (new)

Text proposed by the Commission	*Amendment*
	(23b) 'electronic communications service' means a electronic communications service as defined in Article 2, point (4) of Directive (EU) 2018/1972;

Amendment 104

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

Text proposed by the Commission	*Amendment*
1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives ***and*** appropriate policy and regulatory measures, with a view to	1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives***, the required technical, organisational and financial***

achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:

resources to achieve those objectives, as well as the appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:

Amendment 105

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

Text proposed by the Commission	*Amendment*
(a) a definition of objectives and priorities of the Member ***States'*** strategy on cybersecurity;	(a) a definition of objectives and priorities of the Member ***State's*** strategy on cybersecurity;

Amendment 106

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

Text proposed by the Commission	*Amendment*
(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 ***and the roles and responsibilities of public bodies and entities as well as other relevant actors***;	(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2;

Amendment 107

Proposal for a directive
Article 5 – paragraph 1 – point b a (new)

Text proposed by the Commission	*Amendment*
	(ba) a framework allocating the roles and responsibilities of public bodies and entities as well as other relevant actors, underpinning the cooperation and coordination, at the national level, between the competent authorities designated pursuant to Articles 7(1) and Article 8(1), the single point of contact

	designated pursuant to Article 8(3), and the CSIRTs designated pursuant to Article 9;

Amendment 108

Proposal for a directive
Article 5 – paragraph 1 – point e

Text proposed by the Commission	*Amendment*
(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;	(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy***, including a cybersecurity single point of contact for SMEs that provides support for implementing the specific cybersecurity measures***;

Amendment 109

Proposal for a directive
Article 5 – paragraph 1 – point f

Text proposed by the Commission	*Amendment*
(f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[38] [Resilience of Critical Entities Directive] for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks.	(f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[38] [Resilience of Critical Entities Directive]***, both within and between Member States,*** for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks.
[38] [insert the full title and OJ publication reference when known]	[38] [insert the full title and OJ publication reference when known]

Amendment 110

Proposal for a directive
Article 5 – paragraph 1 – point f a (new)

Text proposed by the Commission	*Amendment*
	(fa) an assessment of the general level of cybersecurity awareness among citizens.

Amendment 111

Proposal for a directive
Article 5 – paragraph 2 – point -a (new)

Text proposed by the Commission	*Amendment*
	(-a) a policy addressing cybersecurity for each sector covered by this Directive;

Amendment 112

Proposal for a directive
Article 5 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement;	(b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement***, including encryption requirements and the use of open-source cybersecurity products***;

Amendment 113

Proposal for a directive
Article 5 – paragraph 2 – point d

Text proposed by the Commission	*Amendment*
(d) a policy related to sustaining the general availability and integrity of the public core of the open internet;	(d) a policy related to sustaining the general availability and integrity of the public core of the open internet***, including cybersecurity of undersea communications cables***;

Amendment 114

Proposal for a directive
Article 5 – paragraph 2 – point d a (new)

Text proposed by the Commission	*Amendment*
	(da) a policy to promote and support the development and integration of emerging technologies, such as artificial intelligence, in cybersecurity-enhancing tools and applications;

Amendment 115

Proposal for a directive
Article 5 – paragraph 2 – point d b (new)

Text proposed by the Commission	*Amendment*
	(db) a policy to promote the integration of open-source tools and applications;

Amendment 116

Proposal for a directive
Article 5 – paragraph 2 – point f

Text proposed by the Commission	*Amendment*
(f) a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure;	(f) a policy on supporting academic and research institutions to develop***, enhance and deploy*** cybersecurity tools and secure network infrastructure;

Amendment 117

Proposal for a directive
Article 5 – paragraph 2 – point h

Text proposed by the Commission	*Amendment*
(h) a policy ***addressing specific needs of*** SMEs, ***in particular*** those excluded from the scope of this Directive, ***in relation to*** guidance and support ***in improving their resilience to cybersecurity threats.***	(h) a policy ***promoting cybersecurity for*** SMEs, ***including*** those excluded from the scope of this Directive, ***addressing their specific needs and providing easily accessed*** guidance and support***, including guidelines addressing supply chain challenges faced;***

Amendment 118

Proposal for a directive
Article 5 – paragraph 2 – point h a (new)

Text proposed by the Commission	*Amendment*
	(ha) a policy to promote cyber hygiene comprising a baseline set of practices sand controls and raising the general cybersecurity awareness among citizens of cybersecurity threats and best practices;

Amendment 119

Proposal for a directive
Article 5 – paragraph 2 – point h b (new)

Text proposed by the Commission	*Amendment*
	(hb) a policy on promoting active cyber defence;

Amendment 120

Proposal for a directive
Article 5 – paragraph 2 – point h c (new)

Text proposed by the Commission	*Amendment*
	(hc) a policy to help authorities develop competences and understanding of the security considerations needed to design, build and manage connected places;

Amendment 121

Proposal for a directive
Article 5 – paragraph 2 – point h d (new)

Text proposed by the Commission	*Amendment*
	(hd) a policy specifically addressing the ransomware threat and disrupting the ransomware business model;

Amendment 122

Proposal for a directive
Article 5 – paragraph 2 – point h e (new)

Text proposed by the Commission	*Amendment*
	(he) a policy, including relevant procedures and governance frameworks, to support and promote the establishment of cybersecurity PPPs.

Amendment 123

Proposal for a directive
Article 5 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. Member States may exclude specific information from the notification where and to the extent that it is ***strictly*** necessary to preserve national security.	3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. Member States may exclude specific information from the notification where and to the extent that it is necessary to preserve national security.

Amendment 124

Proposal for a directive
Article 5 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon request, in the development of a national strategy and of key performance indicators for the assessment of the strategy.	4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon request, in the development of a national strategy and of key performance indicators for the assessment of the strategy. ***ENISA shall provide guidance to Member States in order to align their already formulated national cybersecurity strategies with the requirements and obligations set out in this Directive.***

Amendment 125

Proposal for a directive
Article 6 – title

Text proposed by the Commission	*Amendment*
Coordinated vulnerability disclosure and a European vulnerability ***registry***	Coordinated vulnerability disclosure and a European vulnerability ***database***

Amendment 126

Proposal for a directive
Article 6 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, ***where necessary***, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.	1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, ***upon the request of the reporting entity***, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.

Amendment 127

Proposal for a directive
Article 6 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ENISA shall develop and maintain a European vulnerability ***registry***. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of	2. ENISA shall develop and maintain a European vulnerability ***database leveraging the global Common Vulnerabilities and Exposures (CVE)***. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures***, and shall***

network and information systems to disclose and register vulnerabilities present in ICT products or ICT services***, as well as to provide*** access to the information on vulnerabilities contained in the ***registry to all interested parties. The registry*** shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches ***and, in the*** absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.

adopt the necessary technical and organisational measures to ensure the security and integrity of the database, with a view in particular to enabling important and essential entities and their suppliers of network and information systems***, as well as entities which do not fall within the scope of this Directive, and their suppliers,*** to disclose and register vulnerabilities present in ICT products or ICT services***. All interested parties shall be provided*** access to the information on ***the*** vulnerabilities contained in the ***database that have patches or mitigation measures available. The database*** shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches***. In*** absence of available patches, guidance addressed to users of vulnerable ***ICT*** products and ***ICT*** services as to how the risks resulting from disclosed vulnerabilities may be mitigated ***shall be included in the database***.

Amendment 128

Proposal for a directive
Article 7 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. Where a Member State designates more than one competent authority referred to in paragraph 1, it shall clearly indicate which of those competent authorities is to serve as the coordinator for the management of large-scale incidents and crises.

Amendment 129

Proposal for a directive
Article 7 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Each Member State shall identify capabilities, assets and procedures that can be deployed in case of a crisis for the purposes of this Directive.	2. Each Member State shall identify capabilities, assets and procedures that can be deployed in ***the*** case of a crisis for the purposes of this Directive.

Amendment 130

Proposal for a directive
Article 7 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall communicate to the Commission the designation of their competent authorities referred to in paragraph 1 and submit their national cybersecurity incident and crisis response plans as referred to in paragraph 3 within three months from that designation and the adoption of those plans. Member States may exclude specific information from the plan where and to the extent that it is strictly necessary for their national security.	4. Member States shall communicate to the Commission the designation of their competent authorities referred to in paragraph 1 and submit ***to the EU-CyCLONe*** their national cybersecurity incident and crisis response plans as referred to in paragraph 3 within three months from that designation and the adoption of those plans. Member States may exclude specific information from the plan where and to the extent that it is strictly necessary for their national security.

Amendment 131

Proposal for a directive
Article 8 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Each Member State shall designate one national single point of contact on cybersecurity (‘single point of contact’). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State.	3. Each Member State shall designate one ***of the competent authorities referred to in paragraph 1 as a*** national single point of contact on cybersecurity (‘single point of contact’). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State.

Amendment 132

Proposal for a directive
Article 8 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Each single point of contact shall exercise a liaison function to ensure cross–border cooperation of its Member State's authorities with the relevant authorities in other Member States, as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.	4. Each single point of contact shall exercise a liaison function to ensure cross–border cooperation of its Member State's authorities with the relevant authorities in other Member States, ***the Commission and ENISA,*** as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.

Amendment 133

Proposal for a directive
Article 9 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that each CSIRT has adequate resources to carry out effectively their tasks as set out in Article 10(2).	2. Member States shall ensure that each CSIRT has adequate resources ***and the technical capabilities necessary*** to carry out effectively their tasks as set out in Article 10(2).

Amendment 134

Proposal for a directive
Article 9 – paragraph 6 a (new)

Text proposed by the Commission	*Amendment*
	6a. Member States shall ensure the possibility of effective, efficient and secure information exchange on all classification levels between their own CSIRTs and CSIRTs from third countries on the same classification level.

Amendment 135

Proposal for a directive
Article 9 – paragraph 6 b (new)

Text proposed by the Commission	*Amendment*
	6b. CSIRTs shall, without prejudice to Union law, in particular Regulation (EU) 2016/679, cooperate with CSIRTs or equivalent bodies in candidate countries and in other third countries in the Western Balkans and the Eastern Partnership and, where possible, provide them with cybersecurity assistance.

Amendment 136

Proposal for a directive
Article 9 – paragraph 7

Text proposed by the Commission	*Amendment*
7. Member States shall communicate to the Commission without undue delay the CSIRTs designated in accordance with paragraph 1***,*** the CSIRT coordinator designated in accordance with Article 6(1) ***and*** their respective tasks provided in relation to the entities ***referred to in Annexes I and II***.	7. Member States shall communicate to the Commission without undue delay the CSIRTs designated in accordance with paragraph 1 ***and*** the CSIRT coordinator designated in accordance with Article 6(1)***, including*** their respective tasks provided in relation to the ***essential and important*** entities.

Amendment 137

Proposal for a directive
Article 10 – title

Text proposed by the Commission	*Amendment*
Requirements and tasks of CSIRTs	Requirements***, technical capabilities*** and tasks of CSIRTs

Amendment 138

Proposal for a directive
Article 10 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) CSIRTs shall be equipped with an appropriate system for ***managing and*** routing requests, in particular, to facilitate	(c) CSIRTs shall be equipped with an appropriate system for ***classifying,*** routing ***and tracking*** requests, in particular, to

effective and efficient handovers;	facilitate effective and efficient handovers;

Amendment 139

Proposal for a directive
Article 10 – paragraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) CSIRTs shall have appropriate codes of conduct in place to ensure the confidentiality and trustworthiness of their operations;

Amendment 140

Proposal for a directive
Article 10 – paragraph 1 – point d

Text proposed by the Commission	*Amendment*
(d) CSIRTs shall be adequately staffed to ensure availability at all times;	(d) CSIRTs shall be adequately staffed to ensure availability at all times ***and ensure appropriate training frameworks of their staff***;

Amendment 141

Proposal for a directive
Article 10 – paragraph 1 – point e

Text proposed by the Commission	*Amendment*
(e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services;	(e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services***, including broad connectivity across networks, information systems, services and devices***;

Amendment 142

Proposal for a directive
Article 10 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. CSIRTs shall develop at least the

	following technical capabilities:
	(a) the ability to conduct real-time or near-real-time monitoring of networks and information systems, and anomaly detection;
	(b) the ability to support intrusion prevention and detection;
	(c) the ability to collect and conduct complex forensic data analysis, and to reverse engineer cyber threats;
	(d) the ability to filter malign traffic;
	(e) the ability to enforce strong authentication and access privileges and controls; and
	(f) the ability to analyse cyber threats.

Amendment 143

Proposal for a directive
Article 10 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) monitoring cyber threats, vulnerabilities and incidents at national level;	(a) monitoring cyber threats, vulnerabilities and incidents at national level ***and acquiring real-time threat intelligence***;

Amendment 144

Proposal for a directive
Article 10 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) providing early warning, alerts, announcements and dissemination of information to essential and important entities as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents;	(b) providing early warning, alerts, announcements and dissemination of information to essential and important entities as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents***, if possible near-real-time***;

Amendment 145

Proposal for a directive
Article 10 – paragraph 2 – point c

Text proposed by the Commission	*Amendment*
(c) responding to incidents;	(c) responding to incidents ***and providing assistance to the entities involved***;

Amendment 146

Proposal for a directive
Article 10 – paragraph 2 – point e

Text proposed by the Commission	*Amendment*
(e) providing, upon request of an entity, a proactive scanning of the network and information systems used for the provision of their services;	(e) providing, upon request of an entity ***or in the case of a serious threat to national security***, a proactive scanning of the network and information systems used for the provision of their services;

Amendment 147

Proposal for a directive
Article 10 – paragraph 2 – point f a (new)

Text proposed by the Commission	*Amendment*
	(fa) providing, upon request of an entity, enabling and configuration of network logging to protect data, including personal data from unauthorised exfiltration;

Amendment 148

Proposal for a directive
Article 10 – paragraph 2 – point f b (new)

Text proposed by the Commission	*Amendment*
	(fb) contributing to the deployment of secure information sharing tools pursuant to Article 9(3).

Amendment 149

Proposal for a directive
Article 10 – paragraph 4 – introductory part

Text proposed by the Commission	*Amendment*
4. In order to facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following:	4. In order to facilitate cooperation, CSIRTs shall promote ***automation of information exchange,*** the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following:

Amendment 150

Proposal for a directive
Article 11 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that ***either their competent authorities or*** their CSIRTs receive notifications on incidents***,*** and ***significant*** cyber threats and near misses ***submitted pursuant to this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities,*** pursuant to Article ***20***.	2. Member States shall ensure that their CSIRTs receive notifications on ***significant*** incidents ***pursuant to Article 20*** and cyber threats and near misses pursuant to Article ***27 through the single entry point referred to in Article 20(4a)***.

Amendment 151

Proposal for a directive
Article 11 – paragraph 4

Text proposed by the Commission	*Amendment*
4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities ***and*** single points of contact ***and*** law enforcement authorities, data protection authorities, ***and*** the authorities responsible for critical infrastructure	4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities***,*** single points of contact***, CSIRTs,*** law enforcement authorities, ***national regulatory authorities or other competent authorities responsible for***

pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State.	***public electronic communications networks or for publicly available electronic communications services pursuant to Directive (EU) 2018/1972,*** data protection authorities, the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State ***in line with their respective competences***.
[39] [insert the full title and OJ publication reference when known]	[39] [insert the full title and OJ publication reference when known]

Amendment 152

Proposal for a directive
Article 11 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Member States shall ensure that their competent authorities regularly provide information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber threats and incidents affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those risks and incidents.	5. Member States shall ensure that their competent authorities regularly provide ***timely*** information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber threats and incidents affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those risks and incidents.

Amendment 153

Proposal for a directive
Article 12 – paragraph 3 – subparagraph 1

Text proposed by the Commission	*Amendment*
The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as ***an observer***. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group.	The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European ***Parliament and the European*** External Action Service shall participate in the activities of the Cooperation Group as ***observers***. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group.

Amendment 154

Proposal for a directive
Article 12 – paragraph 3 – subparagraph 2

Text proposed by the Commission	*Amendment*
Where appropriate, the Cooperation Group may invite representatives of relevant stakeholders to participate in its work.	Where appropriate, the Cooperation Group may invite representatives of relevant stakeholders***, such as the European Data Protection Board and representatives of industry,*** to participate in its work.

Amendment 155

Proposal for a directive
Article 12 – paragraph 4 – point b

Text proposed by the Commission	*Amendment*
(b) exchanging best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, trainings, exercises and skills, ***building*** capacity ***as well as*** standards and technical specifications;	(b) exchanging best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, trainings, exercises and skills, capacity ***building,*** standards and technical specifications ***as well as the identification of essential and important entities***;

Amendment 156

Proposal for a directive
Article 12 – paragraph 4 – point b a (new)

Text proposed by the Commission	*Amendment*
	(ba) mapping the national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across the Union;

Amendment 157

Proposal for a directive
Article 12 – paragraph 4 – point c

Text proposed by the Commission	*Amendment*
(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives;	(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives ***and the overall consistency of sector-specific cybersecurity requirements***;

Amendment 158

Proposal for a directive
Article 12 – paragraph 4 – point f

Text proposed by the Commission	*Amendment*
(f) discussing reports on the peer review referred to in Article 16(7);	(f) discussing reports on the peer review referred to in Article 16(7)***, and drawing up conclusions and recommendations***;

Amendment 159

Proposal for a directive
Article 12 – paragraph 4 – point f a (new)

Text proposed by the Commission	*Amendment*
	(fa) carrying out coordinated security risk assessments that may be initiated pursuant to Article 19(1), in cooperation with the Commission and ENISA;

Amendment 160

Proposal for a directive
Article 12 – paragraph 4 – point k a (new)

Text proposed by the Commission	*Amendment*
	(ka) submitting to the Commission for the purpose of the review referred to in Article 35 reports on the experience gained at a strategic and operational level;

Amendment 161

Proposal for a directive
Article 12 – paragraph 4 – point k b (new)

Text proposed by the Commission	*Amendment*
	(kb) providing a yearly assessment in cooperation with ENISA, Europol and national law enforcement institutions on which third countries are harbouring ransomware criminals.

Amendment 162

Proposal for a directive
Article 12 – paragraph 8

Text proposed by the Commission	*Amendment*
8. The Cooperation Group shall meet regularly and at least ***once*** a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ***promote*** strategic cooperation and ***exchange of*** information.	8. The Cooperation Group shall meet regularly and at least ***twice*** a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ***facilitate*** strategic cooperation and information ***exchange***.

Amendment 163

Proposal for a directive
Article 13 – paragraph 3 – point a a (new)

Text proposed by the Commission	*Amendment*
	(aa) facilitating the sharing and transferring of technology and relevant measures, policies, best practices and frameworks among the CSIRTs;

Amendment 164

Proposal for a directive
Article 13 – paragraph 3 – point b a (new)

Text proposed by the Commission	*Amendment*
	(ba) ensuring interoperability with regard to information sharing standards;

Amendment 165

Proposal for a directive
Article 14 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of information among Member States and Union institutions, bodies and agencies, the European Cyber Crises Liaison Organisation Network (EU - CyCLONe) is hereby established.	1. In order to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of ***relevant*** information among Member States and Union institutions, bodies and agencies, the European Cyber Crises Liaison Organisation Network (EU - CyCLONe) is hereby established.

Amendment 166

Proposal for a directive
Article 14 – paragraph 2

Text proposed by the Commission	*Amendment*
2. EU-CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission and ENISA. ENISA shall provide the secretariat of the ***network*** and	2. EU - CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission and ENISA. ENISA shall provide the secretariat of the ***EU -***

support the secure exchange of information.	***CyCLONe*** and support the secure exchange of information.

Amendment 167

Proposal for a directive
Article 14 – paragraph 5

Text proposed by the Commission	*Amendment*
5. EU-CyCLONe shall regularly report to the Cooperation Group on ***cyber threats,*** incidents and trends, focusing in particular on their impact on essential and important entities.	5. EU - CyCLONe shall regularly report to the Cooperation Group on ***large-scale*** incidents and ***crises, as well as*** trends, focusing in particular on their impact on essential and important entities.

Amendment 168

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 ***and shall submit and present it to the European Parliament***. The report ***shall be delivered in machine-readable format and*** shall in particular include an assessment of the following:

Amendment 169

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 and hygiene among citizens and entities, including SMEs, as well as the general level of security of connected devices;

Amendment 170

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 cybersecurity capabilities ***across the Union, including the alignment of Member States national cybersecurity strategies***.

Amendment 171

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 particular ***identification of obstacles and*** 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.

Amendment 172

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 methodology including the relevant variables of the cybersecurity index referred to in paragraph 1, point (c).

Amendment 173

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 ***peer-reviews*** shall be conducted ***in consultation with ENISA*** by cybersecurity technical experts drawn from ***at least two*** Member States different than the one reviewed and shall cover at least the following:

Amendment 174

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 operational capabilities and effectiveness of CSIRTs ***in executing their tasks***;

Amendment 175

Proposal for a directive
Article 16 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The organisational aspects of the peer reviews shall be decided by the Commission, supported by ENISA, and, following consultation of the Cooperation Group, be based on criteria defined in the methodology referred to in paragraph 1. Peer reviews shall assess the aspects referred to in paragraph 1 for all Member States and sectors, including targeted issues specific to one or several Member States or one or several sectors.	3. The organisational aspects of the peer reviews shall be decided by the Commission, supported by ENISA, and, following consultation of the Cooperation Group, be based on criteria defined in the methodology referred to in paragraph 1. Peer reviews shall assess the aspects referred to in paragraph 1 for all Member States and sectors, including targeted issues specific to one or several Member States or one or several sectors. ***The***

designated experts carrying out the review shall communicate these targeted issues to the Member State under peer-review, prior to its commencement.

Amendment 176

Proposal for a directive
Article 16 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. Prior to the commencement of the peer-review process, the Member State under to the peer-review shall carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated experts.

Amendment 177

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 Member States being reviewed shall provide the designated experts with the requested information necessary for the assessment of the reviewed aspects. ***The Commission, in cooperation with ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated experts.*** 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.

Amendment 178

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 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***, before the commencement of the peer-review process***.

Amendment 179

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 include recommendations to enable improvement on the aspects covered by the peer-review process.*** 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***, excluding sensitive and confidential information***.

Amendment 180

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	2. Member States shall ensure that members of the management body ***of essential and important entities*** follow specific ***training***, ***and shall encourage essential and important entities to offer similar training to all employees*** on a

practices and their impact on the ***operations of*** the entity.	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.

Amendment 181

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 and prevent or minimise the impact of incidents on recipients of their services and on other*** services. Having regard to the state of the art ***and to European or international standards***, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.

Amendment 182

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;

Amendment 183

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

Text proposed by the Commission	*Amendment*
(c) business continuity and crisis	(c) business continuity***, such as***

management;	***backup management and disaster recovery,*** and crisis management;

Amendment 184

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 services or managed security services***;	(d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers;

Amendment 185

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;

Amendment 186

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

Text proposed by the Commission	*Amendment*
	(fa) basic computer hygiene practices and cybersecurity training;

Amendment 187

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***, such as*** encryption***, where appropriate;***

Amendment 188

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

Text proposed by the Commission	*Amendment*
	(ga) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate.

Amendment 189
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, without undue delay, take all necessary***, appropriate and proportionate*** corrective measures to bring the service concerned into compliance.

Amendment 190

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.	***deleted***

Amendment 191

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.	6. The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 ***of this Article*** to take account of new cyber threats, technological developments or sectorial specificities ***as well as to supplement this Directive by laying down the technical and the methodological specifications of the measures referred to in paragraph 2 of this Article***.

Amendment 192

Proposal for a directive
Article 19 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.	1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT ***and information and communication system (ICS)*** services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.

Amendment 193

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	2. The Commission, after consulting the Cooperation Group and ENISA***, and, where applicable, relevant stakeholders***, shall identify the specific critical ICT ***and ICS*** services, systems or products that may

referred to in paragraph 1.	be subject to the coordinated risk assessment referred to in paragraph 1.

Amendment 194

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 CSIRT in accordance with paragraphs 3 and 4 of any significant ***incident***. Member States shall ensure that those entities report, among others, any information enabling the CSIRT to determine any cross-border impact of the incident.

Amendment 195

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 any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities	Where applicable, ***Member States shall ensure that essential and important*** entities ***inform*** the recipients of their services***, without undue delay, of protective*** measures or remedies ***to particular incidents and known risks, which can be taken by the*** recipients.

shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.	Where appropriate, the entities shall ***inform the*** recipients of ***their services of the incident or known risk*** itself. ***Informing of recipients shall take place on a 'best efforts' basis and*** shall not ***subject*** the notifying entity ***to an increase in*** liability.

Amendment 196

Proposal for a directive
Article 20 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
3. ***An*** incident shall be ***considered significant if***:	3. ***In order to determine the significance of the*** incident***, where available, the following parameters*** shall be ***taken into account***:

Amendment 197

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

Text proposed by the Commission	*Amendment*
(a) the incident ***has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned***;	(a) ***the number of recipients of the services affected by*** the incident;

Amendment 198

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 duration of*** the incident***;***

Amendment 199

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

Text proposed by the Commission	*Amendment*
	(ba) the geographical spread of the area affected by the incident;

Amendment 200

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

Text proposed by the Commission	*Amendment*
	(bb) the extent to which the functioning and continuity of the service is affected by the incident;

Amendment 201

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

Text proposed by the Commission	*Amendment*
	(bc) the extent of the impact of the incident on economic and societal activities.

Amendment 202

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

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

Amendment 203

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***	(a) an initial notification ***of the***

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;***

significant incident***, which shall contain information available to the notifying entity on a best efforts basis as follows:***

Amendment 204

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

Text proposed by the Commission	*Amendment*
	(i) with regard to incidents that significantly disrupt the availability of the services provided by the entity, the CSIRT shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident;

Amendment 205

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

Text proposed by the Commission	*Amendment*
	(ii) with regard to incidents that have a significant impact on the entity other than on the availability of the services provided by that entity, the CSIRT shall be notified without undue delay and in any event within 72 hours of becoming aware of the incident;

Amendment 206

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

Text proposed by the Commission	*Amendment*
	(iii) with regard to incidents that have a significant impact on the services of a trust services provider as defined in Article 3, point (19) of Regulation (EU) No 910/2014 or on the personal data

	maintained by that trust service provider, the CSIRT shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident;

Amendment 207

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) an intermediate report on relevant status updates***, upon the request of a CSIRT***;

Amendment 208

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 ***initial notification***, including at least the following:

Amendment 209

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

Text proposed by the Commission	*Amendment*
	(ca) in the case of an ongoing incident at time of the submission of the comprehensive report referred to in point (c), a final report shall be provided one month after the incident has been resolved.

Amendment 210

Proposal for a directive
Article 20 – paragraph 4 – subparagraph 2

Text proposed by the Commission	*Amendment*
Member States shall provide that in duly justified cases and in agreement with ***the competent authorities or*** the CSIRT, the entity concerned can deviate from the deadlines laid down in points (a) and (c).	Member States shall provide that in duly justified cases and in agreement with the CSIRT, the entity concerned can deviate from the deadlines laid down in points (a)***(i) and (ii) and point (c)***. ***Member States shall ensure the confidentiality and appropriate protection of sensitive information about incidents shared with CSIRTs, and shall adopt measures and procedures for sharing and reuse of incident information.***

Amendment 211

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

Text proposed by the Commission	*Amendment*
	4a. Member States shall establish a single entry point for all notifications required under this Directive and other relevant Union law. ENISA, in cooperation with the Cooperation Group, shall develop and continuously improve common notification templates by means of guidelines to simplify and streamline the reporting information required under Union law and decrease the burden on reporting entities.

Amendment 212

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

Text proposed by the Commission	*Amendment*
	4b. Essential and important entities referred to in Article 24(1) may meet the requirements of paragraph 1 of this Article by notifying the CSIRT of the Member State in which the entities have the main establishment within in the Union, and by notifying the essential and

	important entities they provide services to of any significant incident that is known to impact the recipient of the services.

Amendment 213

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 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 ***the*** request of the entity, guidance ***and actionable advice*** on the implementation of possible mitigation measures. CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities. ***The CSIRT may share information on the incident with other important and essential entities, while ensuring the confidentiality of the information provided by the reporting entity.***

Amendment 214

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	6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the CSIRT shall inform the other affected Member States and ENISA of the incident ***and provide relevant information***. In so doing, the CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies

legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.	with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

Amendment 215

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 CSIRT, and where appropriate 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.

Amendment 216

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

Text proposed by the Commission	*Amendment*
	7a. CSIRTs shall, without undue delay, provide the single point of contact and where relevant, the competent authorities, with the information on significant incidents notified in accordance with paragraph 1.

Amendment 217

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	8. At the request of the CSIRT, the single point of contact shall forward notifications received pursuant to

pursuant to ***paragraphs 1 and 2*** to the single points of contact of other affected Member States.	***paragraph 1*** to the single points of contact of other affected Member States***, while ensuring confidentiality and appropriate protection of the information provided by the reporting entity***.

Amendment 218

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.

Amendment 219

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 of this Article and Article 27*** 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].

Amendment 220

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, may adopt implementing acts further specifying the procedure of a notification submitted pursuant to ***paragraph 1 of this Article and Article 27***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Amendment 221

Proposal for a directive
Article 20 – paragraph 11 a (new)

Text proposed by the Commission	*Amendment*
	11a. The Commission is empowered to adopt delegated acts, in accordance with Article 36, to supplement this Directive by specifying the type of information to be submitted pursuant to paragraph 1 of this Article and by further specifying the parameters which are to be taken into account when determining the significance of an incident as referred to in paragraph 3 of this Article.

Amendment 222

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	1. Member States ***shall, following guidance from ENISA, the Commission and the Cooperation Group, 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***.

certain ICT products, ICT services and ICT processes***, either developed by the essential or important entity or procured from third parties,*** under European cybersecurity schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 ***or, if not yet available, under similar internationally recognised*** certification ***schemes. Furthermore, Member States shall encourage*** essential ***and*** important ***entities to use qualified trust services pursuant to Regulation (EU) No 910/2014***.

Amendment 223

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. The Commission ***is*** empowered to adopt delegated acts***, in accordance with Article 36, to supplement this Directive by*** specifying which categories of essential ***and important*** entities ***are*** required to obtain a certificate under specific European cybersecurity schemes pursuant to ***Article 49 of Regulation (EU) 2019/881. Such*** delegated acts shall be ***considered where insufficient levels of cybersecurity have been identified, shall be preceded by an impact assessment and shall provide for an implementation period***.

Amendment 224

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	3. The Commission may***, after consulting the Cooperation Group and the European Cybersecurity Certification Group,*** request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases

paragraph 2 is available.

where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.

Amendment 225

Proposal for a directive
Article 22 – paragraph 2

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

Amendment 226

Proposal for a directive
Article 22 – paragraph 3

Text proposed by the Commission	*Amendment*
	3. The Commission, in collaboration with ENISA, shall support and promote the development and implementation of standards set by relevant Union and international standardisation bodies for the convergent implementation of Article 18 (1) and (2). The Commission shall support the update of the standards in the light of technological developments.

Amendment 227

Proposal for a directive
Article 23 – title

Text proposed by the Commission	*Amendment*
Databases of domain names and registration data	***Database structure*** of domain names and registration data

Amendment 228

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 ***require*** TLD registries and the entities providing domain name registration services ***to*** collect and maintain accurate***, verified*** and complete domain name registration data in a database ***structure operated for that purposes***.

Amendment 229

Proposal for a directive
Article 23 – paragraph 2

Text proposed by the Commission	*Amendment*
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.	2. Member States shall ensure that the ***database structure*** of domain name registration data referred to in paragraph 1 ***contains*** relevant information***, which shall include at least the registrants' name, their physical and email address as well as their telephone number,*** to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.

Amendment 230

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	3. Member States shall ensure that the TLD registries and entities providing domain name registration services have policies and procedures in place to ensure

to ensure that the ***databases include*** accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.

that the ***database structure includes*** accurate***, verified*** and complete information. Member States shall ensure that such policies and procedures are made publicly available.

Amendment 231

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 entities providing domain name registration services ***make publicly available***, without undue delay after the registration of a domain name, domain registration data which are not personal data. ***For legal persons as registrants, the domain registration data publicly available shall include at least the registrants' name, their physical and email address as well as their telephone number.***

Amendment 232

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 ***require*** TLD registries and entities providing domain name registration services ***to*** 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 ***require*** TLD registries and entities providing domain name registration services ***to*** reply without undue delay ***and in any event within 72 hours upon the receipt of the*** requests for access. Member States shall ensure that policies and procedures to disclose such data are made

publicly available.

Amendment 233

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 ***either*** where the entities have the establishment with the highest number of employees in the Union ***or the establishment where cybersecurity operations are carried out***.

Amendment 234

Proposal for a directive
Article 25 – title

Text proposed by the Commission	*Amendment*
Registry ***for essential and important entities***	***ENISA*** registry

Amendment 235

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 ***of*** essential and important entities referred to in Article 24(1)***, which*** shall ***include*** the following information:

Amendment 236

Proposal for a directive
Article 25 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) up-to-date contact details, including email addresses ***and*** telephone numbers of the entities.	(c) up-to-date contact details, including email addresses***, IP ranges,*** telephone numbers ***and relevant sectors and subsectors*** of the entities ***referred to in Annexes I and II***.

Amendment 237

Proposal for a directive
Article 25 – paragraph 1 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	By ... [12 months after the date of entry into force of this Directive], the essential and important entities shall submit the information referred to in the first subparagraph to ENISA.

Amendment 238

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 ***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, ***near misses,*** vulnerabilities, techniques and procedures, ***metadata and content data, indicators of compromise, adversarial tactics, modus operandi, actor specific information,*** cybersecurity alerts***, industrial espionage tactics and recommended security tool configurations***, where such information sharing:

Amendment 239

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 ***or promoting collaborative cyber threat research between public and private entities***.

Amendment 240

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 ***and their service providers or, where relevant, other suppliers***. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared.

Amendment 241

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***	3. Member States shall ***facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by making***

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).	operational elements (including the use of dedicated ICT platforms ***and automation tools***) ***and*** content ***available***. ***Member States*** shall lay down the details of the involvement of public authorities in such arrangements ***and may impose certain conditions on the information made available by competent authorities or CSIRTs***. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).

Amendment 242

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 notifications ***may be submitted to the CIRTS***, on a voluntary basis, ***by:***

Amendment 243

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

Text proposed by the Commission	*Amendment*
	(a) essential and important entities with regard to cyber threats and near misses;

Amendment 244

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

Text proposed by the Commission	*Amendment*
	(b) entities falling outside the scope of this Directive, with regard to significant incidents, cyber threats or near misses.

Amendment 245

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

Text proposed by the Commission	*Amendment*
	When processing such 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. Where necessary, CSIRTs shall provide the single point of contact and, where relevant, the competent authorities, with the information on notifications received pursuant this Article, while ensuring confidentiality and appropriate protections of the information provided by the reporting entity. Voluntary notification 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.

Amendment 246

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	2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents

resulting in personal data breaches.	resulting in personal data breaches. ***This shall be done in accordance with their competence and tasks pursuant to Regulation (EU) 2016/679.***

Amendment 247

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 ***conducted by trained professionals***;

Amendment 248

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

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

Amendment 249

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

Text proposed by the Commission	*Amendment*
(b) ***regular*** audits;	(b) ***annual and targeted security*** audits ***carried out by a qualified independent body or a competent authority***;

Amendment 250

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) ***ad hoc*** audits ***in cases justified on the ground of a significant incident or non-compliance by the essential entity***;

Amendment 251

Proposal for a directive
Article 29 – paragraph 2 – subparagraphs 1 a and 1 b (new)

Text proposed by the Commission	*Amendment*
	The targeted security audits, referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.
	The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by a qualified independent body shall be paid by the entity concerned.

Amendment 252

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

Text proposed by the Commission	*Amendment*
	2a. Where exercising their powers under paragraph 2, points (a) to (d), the competent authorities shall minimise the impact on the business processes of the entity.

Amendment 253

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 with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation,*** or an order requiring those entities to remedy the deficiencies identified or the infringements

	of the obligations laid down in this Directive;

Amendment 254

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***

Amendment 255

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 points (a) to (i) of this paragraph, depending on the circumstances of each individual case.	(j) impose or request the imposition by the relevant bodies or courts ***in accordance with*** national ***law*** of an administrative fine pursuant to Article 31 in addition to the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case.

Amendment 256

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) ***temporarily*** suspend or request a certification or authorisation body to ***temporarily*** suspend a certification or authorisation concerning part or all ***relevant*** services or activities provided by an essential entity;

Amendment 257

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) ***as ultima ratio,*** request the imposition by the relevant bodies or courts ***in accordance with*** national ***law*** 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.

Amendment 258

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.	***Temporary suspensions or bans pursuant to this paragraph*** shall be applied only until the entity ***concerned*** takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. ***The imposition of such temporary suspensions or bans shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection, due process, presumption of innocence and right of defence.***

Amendment 259

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***	(c) the damage caused or losses incurred***, including*** financial or economic losses, effects on other services ***and the***

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***;	number of users affected;

Amendment 260

Proposal for a directive
Article 29 – paragraph 7 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) any relevant previous infringements by the entity concerned;

Amendment 261

Proposal for a directive
Article 29 – paragraph 9

Text proposed by the Commission	*Amendment*
9. Member States shall ensure that their competent authorities inform the relevant competent authorities of ***the*** Member ***State concerned*** designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. Upon request of competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.	9. Member States shall ensure that their competent authorities inform the relevant competent authorities of ***all relevant*** Member ***States*** designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. Upon request of competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.

Amendment 262

Proposal for a directive
Article 29 – paragraph 9 a (new)

Text proposed by the Commission	*Amendment*
	9a. Member States shall ensure that their competent authorities cooperate with the relevant competent authorities of the Member State concerned designated pursuant to Regulation (EU) XXXX/XXXX [DORA].

Amendment 263

Proposal for a directive
Article 30 – paragraph 1

Text proposed by the Commission	*Amendment*
1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through ex post supervisory measures.	1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through ex post supervisory measures. ***Member States shall ensure that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.***

Amendment 264

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

Text proposed by the Commission	*Amendment*
(a) on-site inspections and off-site ex post supervision;	(a) on-site inspections and off-site ex post supervision ***conducted by trained professionals***;

Amendment 265

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

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

Amendment 266

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 ***carried out by a qualified independent body or a competent authority***;

Amendment 267

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;

Amendment 268

Proposal for a directive
Article 30 – paragraph 2 – subparagraphs 1 a and 1 b (new)

Text proposed by the Commission	*Amendment*
	The targeted security audits, referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.
	The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by a qualified independent body shall be paid by the

	entity concerned.

Amendment 269

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***

Amendment 270

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

Text proposed by the Commission	*Amendment*
(i) 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 points (a) to (h) of this paragraph, depending on the circumstances of each individual case.	(i) impose or request the imposition by the relevant bodies or courts ***in accordance with*** national ***law*** of an administrative fine pursuant to Article 31 in addition to the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.

Amendment 271

Proposal for a directive
Article 31 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to***, or instead of,*** measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).	2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).

Amendment 272

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 ***in*** Article 4***, point*** (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 and in any event*** within ***72 hours of becoming aware of a data breach***.

Amendment 273

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.

Amendment 274

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	***By... [42 months after the date of entry into force of this Directive] and every 36 months thereafter,*** the Commission shall 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 ***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]***.

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. ***To that end*** 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 report shall be ***accompanied, where necessary, by a legislative proposal***.

Amendment 275

Proposal for a directive
Article 36 – paragraph 2

Text proposed by the Commission	*Amendment*
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 […]	2. The power to adopt delegated acts referred to in Articles 18(6)***, 20(11a)*** and 21(2) shall be conferred on the Commission for a period of five years from […]

Amendment 276

Proposal for a directive
Article 36 – paragraph 3

Text proposed by the Commission	*Amendment*
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.	3. The delegation of power referred to in Articles 18(6)***, 20(11a)*** 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.

Amendment 277

Proposal for a directive
Article 36 – paragraph 6

Text proposed by the Commission	*Amendment*
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.	6. A delegated act adopted pursuant to Articles 18(6)***, 20(11a)*** 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.

Amendment 278

Proposal for a directive
Article 42 – paragraph 1a (new)

Text proposed by the Commission	*Amendment*
	However, Articles 39 and 40 shall apply from ... [18 months after the date of entry into force of this Directive].

Amendment 279

Proposal for a directive
Annex I – point 2 – point d – indent 2 (new)

Text proposed by the Commission		*Amendment*
2. Transport	(d) Road	***— Operators of smart charging services for electric vehicles***

Amendment 280

Proposal for a directive
Annex II – table – row 6 a (new)

Text proposed by the Commission

Amendment

6a. Education and research		***— Higher education institutions and research institutions***

EXPLANATORY STATEMENT

The Rapporteur wants Europe to become the best place to live in and to carry out business in.

The Rapporteur therefore welcomes the Directive on measures for a high common level of cybersecurity across the Union (NIS2), which replaces the original NIS Directive (NIS1). The proposal reflects the changed cybersecurity threat landscape and introduces a minimum harmonization of measures across the EU.

Nowadays, European police forces increasingly struggle to cope with the steep rise of cybercrime incidents. These can include high-tech crime, cyber enabled crime and CEO-fraud, but the Rapporteur wishes to explicitly highlight the aggressive rise in ransomware gangs hacking and blackmailing European targets, irrespective of their size or turnover. In turn, adversarial nation state actors are focussing on intellectual property theft on an industrial scale, which requires a corresponding answer.

Yet, according to ENISA, the general spending on cybersecurity is 41 % lower by organisations in the EU than by their US counterparts. Moreover, information sharing between countries and within countries has been seriously hampered due to GDPR-liability fears. This is evident in both public and private entities who are fearful of sharing data. The NIS2 must therefore be clear that information sharing is essential for the requirements on cybersecurity to be met.

A common level of cybersecurity in the EU is crucial for the functioning of the internal market. Well-defined legislation is necessary so that enterprises who operate in different Member States fall under the same set of rules. NIS2 wants to remove uncertainty and the current lack of clarity.

In an age where cybercrime, espionage or sabotage operations can have cascading effects, the NIS2 justly widens the **scope** significantly. The proposal includes sectors that previously were not considered essential or important, but are definitely regarded as such by ransomware gangs or certain nation states. Based on the services entities deliver for societies, these are divided into the following two legal categories: ‘essential’ and ‘important’ entities. The

Rapporteur shares the ambition of the proposal by the Commission, and believes research and academic institutions should be included as a new sector. These institutions are heavily targeted, and their intellectual property deserves protection under the NIS2.

The administrative burden and **red tape on enterprises** must be a constant concern to all legislators. The Rapporteur supports the exclusion of micro- and small enterprises. He, furthermore, believes that the NIS2 should not just focus on compliance and penal measures, but also on positive incentives, such as providing guidance and assistance to SMEs, who have specific needs and interests, or on freely offered services to check email-server and website configuration. Such proposals are also meant to illustrate, in this respect, that governments need to be service-orientated.

Incident reporting is critical to cybersecurity: it can prevent others from becoming victims of a cyberattack. The Rapporteur wishes to mention that in his former capacity in the cybersecurity field, he often found it impossible to report an incident within 24 hours. Usually at this early stage an incident is still unclear until later on. To the Rapporteur, the proposed timeframe of 24 hours seems unreasonable, also due to the fact that the experts efforts are invested in mitigating the problem; reporting at this stage is of secondary interest. The cyber incident and its implications are rarely understood well within 24 hours, and notifications within 24 hours could lead to incorrect reporting, over-reporting and further confusion. Moreover, these incidents often happen over the weekend. Therefore, the Rapporteur proposes to align this Directive with other Union law, such as the GDPR, thus increasing the timeline to within 72 hours.

The Rapporteur does not find it desirable to make the **reporting of potential incidents** mandatory. Voluntary sharing of potential incidents or near misses should be encouraged, but medium and large entities can potentially have tens or even hundreds of significant cyber threats in a single day. Reporting these potential incidents would be burdensome and would inhibit the effectiveness of the response. It could also harm the efficacy of the authorities that have to deal with these notifications, undermining the confidence of the reporting system and their ability to act upon actual incidents.

Reporting potential cyber threats to CSIRTs or competent authorities should also not be mandatory. Compliance and liability will discourage the activities of threat hunters; an essential part of the cyber security ecosystem. Furthermore, there are (serious) occasions where it would be better to report a threat to the intelligence community, when it is in their area of competence, instead of to the NIS authorities.

Cybersecurity measures should be appropriate to the size of the entity and the cybersecurity risks it faces. **Supervision and enforcement** should therefore be proportionate. The fines and penal measures are essential if the NIS2 legislation is to be effective, but the Rapporteur believes legislators should emphasize that there is an escalation-ladder, and only after demonstrable negligence of repeated warnings, should senior management be prepared to feel the force of the law. **Preventing double oversight** trough sector-specific legislation is also important for entities who fall in the scope of both NIS2 and a sector-specific one, such as DORA.

The Rapporteur encourages every member state to formulate a **national cybersecurity strategy on active cyber defence**. In Europe, we have become good at coordinating after an incident has occurred, but the increase of knowledge (public and private) about cyberattacks before they occur, also entails a responsibility. Merely passively sharing that knowledge is not sufficient; citizens and entities expect an active posture from their governments on

cybersecurity protection. Member States must initiate capabilities to thwart attacks and actively prevent them from occurring.

The core of the internet needs attention too. DNS services need to offer secure and privacy minded services to customers. This is not commonly accepted yet. The Rapporteur is concerned that citizens who have their own DNS service on a laptop or small server at home, fall in scope in the proposal of the Commission. The Rapporteur wishes that these persons, often tech-savvy individuals, to be excluded from this Directive. Another problem is that operators of root name servers are included in the scope of the NIS2. Since the Internet grew in the 1970s, 1980s and further, these services are operated by good expert-volunteers. As this service is not monetised, and as it can be argued that governments should not regulate it, the Rapporteur believes that root servers should be **excluded from the scope**.

The Rapporteur finds it of great importance to strengthen the overall security of electronic communication networks and services and improve the integrity of the internet. This means that throughout Europe inter-operable trust-techniques should be used. European DNS resolvers with extra focus on privacy and security are greatly encouraged, as well as the physical protection of internet backbones and submarine communication cables. This Directive should therefore be seen in light of the full package of the cybersecurity strategy as was launched by the Commission: we need a more secure core of the internet.

The NIS2 further provides the legal basis for **coordinated security risk assessments** by the Cooperation Group. The 5G toolbox has served as an excellent example. The Rapporteur believes that these risk assessments could widely improve the security and strategic sovereignty of the Union and believes that these risk assessments should be done on a wide-range of ICT services, systems or products. Cargo-scanners at airports and ports is an explicit example he wishes to mention in this regard.

Unintendedly, essential information sharing has been severely hampered and should be improved. An example: in the past years, police forces discovered and decrypted servers from ransomware gangs, containing sometimes millions of victims, in the EU and outside the EU. The police's job is to work on new cases, so they enable CSIRTs to reach out to targets and mitigate the cyber threats with the uncovered information on those servers. Unfortunately, due to unjustified perceived legal hurdles hardly any victim has been notified or assisted. Therefore, it is essential that the NIS2 creates a clear legal basis to mitigate such threats and to share information not only inside the EU, but also with partners outside the EU.

With the enhancement of the scope, CSIRTs must prepare to offer **scalable and automated solutions** for the swift and secure distribution of coordinated vulnerability disclosure, incident reporting and threat intelligence. The automation of information sharing is not just a derivative of this Directive: it is at the core of it. Providing the **legal basis for CSIRTs and companies to share data**, with their customers, peers, and authorities, both in and outside the EU, is a prerequisite of all good intentions of the NIS2.

Using **standards and certification schemes** is another positive feature from the Commission's proposal. Certification should be possible through specific European- and internationally recognized schemes, preferable over national schemes. Harmonization should be the aim; rules in one Member State should be similar to rules in other Member States.

The NIS2 proposal requires ENISA to develop and maintain a European vulnerability registry. The Rapporteur believes that a **European vulnerability database** should be preferred over a registry. There is little reason to double what is already in place and used by the cybersecurity community as a common standard in all parts of the world. Doubling will

sow discord and confusion within the expert community. A European database, not a registry, should leverage the CVE registry; the list of records of international publicly known cybersecurity vulnerabilities used throughout the world. The Rapporteur believes that ENISA should have a prominent new role within the CVE registry, which is now mainly US based. Duplication of efforts should furthermore be prevented; the desirable outcome should be a database with unique challenges for European organisations. Finally yet importantly, the Rapporteur stresses it is of utmost importance for ENISA to have the infrastructure and procedures in place to deal with classified information. Cybersecurity should be handled from the unclassified level up to the (top) secret level.

WHOIS data, the authoritative record of domain ownership, is the only viable means to obtain the information necessary to identify criminal actors, track threat actors, prevent harms and protect the online ecosystem. The cybersecurity community relies on it, and it enables threat researchers to hunt adversaries, so that citizens and entities can protect themselves against upcoming threats. It is the only reliable accountability mechanism in an otherwise anonymous internet. However, over the past three years, following the entry into force of the GDPR, WHOIS data is regarded by some as a liability issue. The standing practise of WHOIS data has been halted, unfortunately and unjustified. The Rapporteur therefore reiterates in his report the lawfulness of processing data for cybersecurity reasons under the GDPR, in the explicit legislative wish for WHOIS data to be shared again.

Overall, the Rapporteur believes that the NIS2 is the necessary step to take to harmonise our internal market and improve cybersecurity throughout the EU.

15.10.2021

OPINION OF THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

for the Committee on Industry, Research and Energy

on the proposal for a 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 (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Rapporteur for opinion (*): Lukas Mandl(*)
Associated committee – Rule 57 of the Rules of Procedure

SHORT JUSTIFICATION

The proposal for a Directive of the European Parliament and the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS2 Directive)[1] is part of a wider set of initiatives at Union level that seek to increase the resilience of public and private entities against threats. The proposal aims to address the shortcomings of the existing legislation and to enable the entities covered by its scope to respond better to the new challenges identified by the Commission in its impact assessment, which included an extensive stakeholder consultation. These challenges include in particular the increased digitisation of the internal market and the evolving security threat landscape.

The legal basis of the proposal is Article 114 TFEU, i.e. internal market. From a LIBE perspective it is however important to highlight that the measures imposed on network and information systems by the NIS2 Directive do not only serve to ensure the proper functioning of the internal market. **The Directive should also help to contribute to the security of the Union as a whole**, inter alia by avoiding diverging vulnerability to cybersecurity risks between Member States.

To this end, it is crucial to **eliminate existing divergences between Member States** resulting from different interpretations of the law by the Member States. For this reason, the Rapporteur welcomes the uniform condition established by the Regulation to determine the entities falling within the scope of the Directive. Additional suggestions are made to prevent divergence in implementation, notably to oblige the Commission to issue guidelines on the implementation of the *lex specialis* and the criteria applicable to SMEs (which should also ensure legal clarity and avoid unnecessary burden) and to require the Cooperation Group to further specify non-technical factors to be taken into account in the supply chain risk assessments. It is moreover stressed that cooperation between competent authorities need to take place both within and *between* Member States, in real time.

[1] 2020/0359(COD).

The draft report also takes on board a number of **recommendations made by the EDPS** in its opinion on the Cybersecurity Strategy and the NIS 2.0 Directive[2]. Most importantly, it is clarified both in the recitals and in the operative part of the text that any personal data processing under the NIS2 Directive is without prejudice to Regulation (EU) 2016/679 (GDPR)[3] and Directive 2002/58/EC[4] (ePrivacy). Given the narrower scope of the term 'security of networks and information systems' (only covers protection of technology) compared to 'cybersecurity' (also covers activities to protect users) the former term is only used when the context is purely technical. In relation to domain names and registration data, clarifications are proposed regarding 1) the legal basis of the publication of 'relevant information' for the purposes of identification and contacting, 2) the categories of data domain registration data subject to publication (based on an ICANN recommendation), and 3) the entities that might constitute 'legitimate access seekers'. It is also specified in the legal text that the proposal does not affect the attribution of jurisdiction and the competences of data protection supervisory authorities under the GDPR. Finally, a more comprehensive legal basis is provided for the cooperation and exchange of relevant information between the competent authorities under the Proposal and other relevant supervisory authorities, notably supervisory authorities under the GDPR.

Other changes introduced to the Commission proposal by the LIBE rapporteur relate to the following:

- To ensure coherence between the NIS2-Directive and the proposed Directive on resilience of critical entities (ECI)[5], the language of some provisions was aligned with those of the ECI proposal. In line with a similar change envisaged for the ECI Directive which should cover the same sectors as the NIS2 Directive, it is proposed to add 'food production, processing and distribution' to the scope.
- As regards personal data, it is clarified that the scanning of networks and information systems by CSIRTs should not only be in line with Regulation (EU) 2016/679 (GDPR)[6] but also with Directive 2002/58/EC[7] (ePrivacy). International transfers of personal data under this Directive should be in compliance with Chapter V of the GDPR.
- The Cooperation Group should meet twice rather than once a year to take stock of the

---

[2] Opinion 5/2021: https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) *OJ L 119, 4.5.2016, p. 1–88.*

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ L 201, 31.7.2002, p. 37–47.*

[5] 2020/0365(COD).

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) *OJ L 119, 4.5.2016, p. 1–88.*

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ L 201, 31.7.2002, p. 37–47.*

latest developments regarding cybersecurity. The EDPB should participate in the meetings of the Cooperation Group as an observer.

- ENISA should issue annual rather than biennial reports on the state of cybersecurity in the Union. The report should also take into account the impact of cybersecurity incidents on the protection of personal data in the Union.
- The notification deadline of incidents is aligned with the deadline for the notification of breaches under the GDPR, namely 72 hours.
- While the notification of actual cybersecurity incidents by essential and important entities should indeed be mandatory, the notification of cyber threats should be voluntary to limit administrative burden and avoid over-reporting. To be considered significant, an incident should have caused actual damage and affected other natural and legal persons rather than such damage or effect being 'possible'.
- The circumstances to be taken into account when deciding on a sanction following a breach of the cybersecurity rules are aligned with the GDPR. As this would go against the current liability practice in Union law, it should not be possible to impose a temporary ban of natural persons from exercising managerial functions.
- To avoid reputational damage, entities should not be obliged to make public aspects of non-compliance with the requirements under this Directive or the identity natural or legal persons responsible for the infringement.

AMENDMENTS

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

Amendment 1

Proposal for a directive
Recital 1

Text proposed by the Commission	*Amendment*
(1) Directive (EU) 2016/1148 of the European Parliament and the Council[11] aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's economy and society to function effectively.	(1) Directive (EU) 2016/1148 of the European Parliament and the Council[11] aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's ***security and to the effective functioning of its*** economy and society to function effectively.

[11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016 p. 1).

[11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016 p. 1).

Amendment 2

Proposal for a directive
Recital 2

Text proposed by the Commission	*Amendment*
(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national cybersecurity strategies, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group***[12]*** and a network of national Computer Security Incident Response Teams ('CSIRTs network')***[13]*** . Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges.	(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national cybersecurity strategies, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group and a network of national Computer Security Incident Response Teams ('CSIRTs network'). Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges. ***Moreover, the expansion of online activities in the context of the COVID-19 pandemic has highlighted the importance of cybersecurity, which is essential for EU citizens to be able to trust innovation and connectivity, as well as large-scale***

education and training thereon. The Commission should therefore support Member States in the design of educational programmes on cybersecurity with a view to enable important and essential entities to recruit cybersecurity experts who allow them to comply with the obligations arising from this Directive.

[12] Article 11 of Directive (EU) 2016/1148.

[13] Article 12 of Directive (EU) 2016/1148.

[12] Article 11 of Directive (EU) 2016/1148.

[13] Article 12 of Directive (EU) 2016/1148.

Amendment 3

Proposal for a directive
Recital 3

Text proposed by the Commission	*Amendment*
(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence ***and*** cause major damage to the Union economy ***and*** society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market.	(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence***,*** cause major damage to the Union economy***, the functioning of our democracy, and the values and freedom on which our*** society ***is based***. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the ***Union's security and the*** proper functioning of the internal market ***in light of the digital***

transformation of day-to-day activities across the Union. This requires closer cooperation of authorities within and between Member States as well as between national authorities and responsible Union bodies.

Amendment 4

Proposal for a directive
Recital 5

Text proposed by the Commission	*Amendment*
(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards. This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.	(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards. ***Ultimately, these divergences can lead to higher vulnerability of some Member States to cybersecurity threats, with potential spillover effects across the Union, both with regard to its internal market and its overall security.*** This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective ***and real time*** cooperation among the responsible authorities in each Member State***, between the competent authorities of the Member States***, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

Amendment 5

Proposal for a directive
Recital 6

Text proposed by the Commission	*Amendment*
(6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14] , are of relevance.	(6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their ***national*** security, to safeguard public policy and public security, and to allow for the ***prevention,*** investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14] , are of relevance.
[14] The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).	[14] The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).

Amendment 6

Proposal for a directive
Recital 8

Text proposed by the Commission	*Amendment*
(8) In accordance with Directive (EU) 2016/1148***, Member States were responsible*** for determining which entities meet the criteria to qualify as operators of essential services (‘identification process’)***. In order to eliminate the*** wide divergences	(8) ***The responsibility of Member States*** in accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services (‘identification process’)

among Member States in that regard ***and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities***, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[15] , that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion.

[15] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

has led to wide divergences among Member States in that regard***. Without prejudice to the specific exceptions provided in this Directive***, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive ***to eliminate these divergences and ensure legal certainty regarding the risk management requirements and reporting obligations for all relevant entities***. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[15] , that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion.

[15] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Amendment 7

Proposal for a directive
Recital 8 a (new)

Text proposed by the Commission	*Amendment*
	(8 a) Taking into consideration the differences in the national public administration frameworks, Member States retain their decision-making capacity regarding the designation of entities within the scope of this Directive.

Amendment 8

Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(9) ***However,*** small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission.	(9) Small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services ***based on a risk-assessment, including entities defined as critical entities or entities equivalent to critical entities under Directive (EU) XXX/XXX of the European Parliament and the Council[1a]***, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission.
	[1a] Directive (EU)[XXX/XXX]of the European Parliament and of the Council of XXX on the resilience of critical entities (OJ...).

Amendment 9

Proposal for a directive
Recital 10

Text proposed by the Commission	*Amendment*
(10) The Commission, in cooperation with the Cooperation Group, ***may*** issue guidelines on the implementation of the criteria applicable to micro and small ***enterprises***.	(10) The Commission, in cooperation with the Cooperation Group, ***should*** issue guidelines on the implementation of the criteria applicable to micro and small ***entities***.

Amendment 10

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ***may*** issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.	(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ***should*** issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

Amendment 11

Proposal for a directive
Recital 14

Text proposed by the Commission	*Amendment*
(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for	(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive***, wherever possible and appropriate***. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies

enhanced coordination between the competent ***authority*** under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information, particularly ***in*** relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to ***exercise their supervisory and enforcement powers on an*** essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose.

provide for a policy framework for enhanced coordination between the competent ***authorities within and between Member States,*** under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on ***cyber*** incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives ***within and between Member States*** should cooperate and exchange information, particularly ***on*** relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by ***competent authorities under this Directive relevant for*** critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to ***assess the cybersecurity of*** essential entity identified as critical. Both authorities should cooperate and exchange information ***in real time*** for this purpose.

---

[17] [insert the full title and OJ publication reference when known]

[17] [insert the full title and OJ publication reference when known]

Amendment 12

Proposal for a directive
Recital 18

Text proposed by the Commission

(18) Services offered by data centre service providers may not always be provided in a form of cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to ***the*** security ***of network and information systems***, this Directive should cover also providers of such data centre services that are not cloud computing services. For the purpose of this Directive, the term ‘data centre service’

Amendment

(18) Services offered by data centre service providers may not always be provided in a form of cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to ***cyber***security, this Directive should cover also providers of such data centre services that are not cloud computing services. For the purpose of this Directive, the term ‘data centre service’ should cover provision of a service

should cover provision of a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term ‘data centre service’ does not apply to in-house, corporate data centres owned and operated for own purposes of the concerned entity.

that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term ‘data centre service’ does not apply to in-house, corporate data centres owned and operated for own purposes of the concerned entity.

Amendment 13

Proposal for a directive
Recital 20

Text proposed by the Commission	*Amendment*
(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic ***has*** shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.	(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water***, food production, processing and distribution***, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The ***intensified attacks against information systems during the*** COVID-19 pandemic ***have*** shown the vulnerability of our increasingly

interdependent societies in the face of low-probability risks. ***Therefore, further investments in cybersecurity are required.***

Amendment 14

Proposal for a directive
Recital 20 a (new)

Text proposed by the Commission	*Amendment*
	(20 a) It is crucial to raise cyber-awareness and cyber-resilience in all critical and important entities, including public administration entities.

Amendment 15

Proposal for a directive
Recital 21

Text proposed by the Commission	*Amendment*
(21) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of essential and important entities under this Directive. Member States should be able to assign this role to an existing authority.	(21) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of essential and important entities under this Directive. Member States should be able to assign this role to an existing authority ***and ensure that it has adequate resources to carry out its tasks effectively and efficiently***.

Amendment 16

Proposal for a directive
Recital 22

Text proposed by the Commission	*Amendment*
(22) In order to facilitate cross-border cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to ***the security of network and information systems*** and cross-border cooperation at Union level.	(22) In order to facilitate cross-border cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to ***cybersecurity*** and cross-border cooperation at Union level.

Amendment 17

Proposal for a directive
Recital 23

Text proposed by the Commission	*Amendment*
(23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way. The single points of contact should be tasked with forwarding incident notifications to the single points of contact of other ***affected*** Member States. At the level of Member States' authorities, to ensure one single entry point in every Member States, the single points of contacts should also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive.	(23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way. The single points of contact should be tasked with forwarding incident notifications ***in real time*** to the single points of contact of ***all*** other Member States. At the level of Member States' authorities, to ensure one single entry point in every Member States, the single points of contacts should also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive.

Amendment 18

Proposal for a directive
Recital 25

Text proposed by the Commission	*Amendment*
(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] ***as regards personal data***, on behalf of and upon request by an entity under this Directive, a ***proactive scanning*** of the ***network and*** information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.	(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] ***and with Directive 2002/58/EC***, on behalf of and upon request by an entity under this Directive, a ***security scan*** of the information systems ***and the network range*** used for the provision of their services ***to identify, mitigate or prevent specific threats***. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs. ***Furthermore, cybersecurity risks should never be used as a pretext for violations of fundamental rights.***
[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).	[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

Amendment 19

Proposal for a directive
Recital 27

Text proposed by the Commission	*Amendment*
(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20] , a large-scale incident should mean an incident with a significant impact on at least two Member	(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20] , a large-scale incident should mean an incident with a significant impact on at least two Member

States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.

[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market ***or posing serious public security risks in several Member States or the Union as a whole***. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union. ***Member States should monitor the way in which EU rules are implemented, support each other in the event of any cross-border problems, establish a more structured dialogue with the private sector and cooperate on security risks and the threats associated with new technologies, as was the case with 5G technology.***

[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

Amendment 20

Proposal for a directive
Recital 33

Text proposed by the Commission	*Amendment*
(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of existing	(33) When developing guidance documents, the Cooperation Group should consistently: map national ***and sectoral*** solutions and experiences, assess the impact of Cooperation Group deliverables on national ***and sectoral*** approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of

rules.	existing rules.

Amendment 21

Proposal for a directive
Recital 34

Text proposed by the Commission	*Amendment*
(34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should ***consider inviting*** Union bodies and agencies involved in cybersecurity policy, ***such as the European Cybercrime Centre (EC3)***, the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.	(34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should ***invite relevant*** Union bodies and agencies involved in cybersecurity policy, ***notably Europol***, the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.

Amendment 22

Proposal for a directive
Recital 36

Text proposed by the Commission	*Amendment*
(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. ***Such agreements*** should ***ensure adequate protection of data***.	(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. ***To the extent that personal data is transferred to a third country or international organisation, Chapter V of Regulation (EU) 2016/679*** should ***apply***.

Amendment 23

Proposal for a directive
Recital 37

Text proposed by the Commission	*Amendment*
(37) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework set out in Recommendation (EU) 2017/1584 through the existing cooperation networks, notably the Cyber Crisis Liaison Organisation Network (EU-CyCLONe), CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements defining the modalities of that cooperation. The EU-CyCLONe's rules of procedures should further specify the modalities through which the network should function, including but not limited to roles, cooperation modes, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis management at Union level, relevant parties should rely on the Integrated Political Crisis Response (IPCR) arrangements. The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for this purpose. If the crisis entails an important external or Common Security and Defence Policy (CSDP) dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated.	(37) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework set out in Recommendation (EU) 2017/1584 through the existing cooperation networks, notably the Cyber Crisis Liaison Organisation Network (EU-CyCLONe), CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements defining the modalities of that cooperation. The EU-CyCLONe's rules of procedures should further specify the modalities through which the network should function, including but not limited to roles, cooperation modes, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis management at Union level, relevant parties should rely on the Integrated Political Crisis Response (IPCR) arrangements. The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for this purpose. If the crisis ***concerns two or more Member States and is suspected to be of criminal nature, the activation of the EU Law Enforcement Emergency Response Protocol should be considered. If the crisis*** entails an important external or Common Security and Defence Policy (CSDP) dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated.

Amendment 24

Proposal for a directive
Recital 45

Text proposed by the Commission	*Amendment*
(45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of the entities, when relying on data transformation and data analytics services from third parties, the entities should take all appropriate cybersecurity measures.	(45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of the entities, when relying on data transformation and data analytics services from third parties, the entities should take all appropriate cybersecurity measures ***and report any potential cyber attacks that they identify***.

Amendment 25

Proposal for a directive
Recital 46 a (new)

Text proposed by the Commission	*Amendment*
	(46 a) Particular consideration should be given to the fact that ICT services, systems or products subject to specific requirements in the country of origin that might represent an obstacle to compliance with EU privacy and data protection law. Where appropriate, the EDPB should be consulted in the framework of such risk assessments. Free and open source software as well as open source hardware could bring huge benefits in terms of cybersecurity, in particular as regards transparency and verifiability of features. As this could help address and mitigate specific supply chain risks, their use should be preferred where feasible in line with Opinion 5/2021 of the EDPS[1a].

[1a] Opinion 5/2021 of the European Data Protection Supervisor on the Cybersecurity Strategy and the NIS 2.0 Directive, 11 March 2021

Amendment 26

Proposal for a directive
Recital 47

Text proposed by the Commission	*Amendment*
(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors ***including*** those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities.	(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors ***that should be further specified by the Coordination Group, and which include*** those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities.

Amendment 27

Proposal for a directive
Recital 48 a (new)

Text proposed by the Commission	*Amendment*
	(48a) Small and medium-sized enterprises (SMEs) often lack the scale and resources to fulfil abroad and growing range of cybersecurity needs in an interconnected world with an increase of remote work. Member States should therefore address in their national cybersecurity strategies guidance and support for SMEs.

Amendment 28

Proposal for a directive
Recital 50

Text proposed by the Commission	*Amendment*
(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security ***of network and information systems*** appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission.	(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of ***cyber***security appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission.

Amendment 29

Proposal for a directive
Recital 52

Text proposed by the Commission	*Amendment*
(52) Where appropriate, entities should inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. The requirement to inform those recipients of such threats should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge.	(52) Where appropriate, entities should ***be enabled to*** inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. The requirement to inform those recipients of such threats should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge.

Amendment 30

Proposal for a directive
Recital 53

Text proposed by the Commission	*Amendment*
(53) In particular, providers of public electronic communications networks or publicly available electronic communications services, should inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their communications, for instance by using specific types of software or encryption technologies.	(53) In particular, providers of public electronic communications networks or publicly available electronic communications services, should ***implement security by design and by default and be enabled to*** inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their ***devices and*** communications, for instance by using specific types of software or encryption technologies. ***To increase the security of hardware and software, providers should be encouraged to use open source and open hardware.***

Amendment 31

Proposal for a directive
Recital 54

Text proposed by the Commission	*Amendment*
(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' ***powers*** to ensure the protection of their essential security interests and public security, and to permit the ***investigation***, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, ***while providing an*** effective ***response to crime***.	(54) In order to safeguard the security of electronic communications networks and services ***as well as the fundamental rights to data protection and privacy***, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' ***responsibility*** to ensure the protection of their essential security interests and public security, and to permit the ***prevention***, detection and prosecution of criminal offences in compliance with Union ***and national*** law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications. ***Nothing in this Regulation should be viewed as an effort to weaken end-to-end encryption through "backdoors" or similar solutions, as encryption shortfalls may be exploited for malicious purposes. Any measure aimed at weakening encryption or circumventing the technology's architecture may incur significant risks to the*** effective ***protection capabilities it entails. Any unauthorised decryption or monitoring of electronic communications other than by legal authorities should be prohibited to ensure the effectiveness of the technology and its wider use***. ***It is important that Member States address problems encountered by legal authorities and vulnerability researchers. In some Member States entities and natural persons researching vulnerabilities are exposed to criminal and civil liability. Member States are therefore encouraged to issue guidelines for non-prosecution and non-liability of information security***

research.

Amendment 32

Proposal for a directive
Recital 56

Text proposed by the Commission	*Amendment*
(56) Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point ***for all notifications*** required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies.	(56) Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group ***and the European Data Protection Board,*** should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies.

Amendment 33

Proposal for a directive
Recital 57

Text proposed by the Commission	*Amendment*
(57) Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage essential and important entities, on the basis of applicable criminal proceedings rules in	(57) Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage essential and important entities, on the basis of applicable criminal proceedings rules in

compliance with Union law, ***to*** report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, and without prejudice to the personal data protection rules applying to Europol, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the ***EC3*** and ENISA.	compliance with Union law, ***should*** report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, and without prejudice to the personal data protection rules applying to Europol, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the ***European Cybercrime Centre (EC3) of Europol*** and ENISA.

Amendment 34

Proposal for a directive
Recital 58

Text proposed by the Commission	*Amendment*
(58) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities should cooperate and exchange information on all relevant matters with data protection authorities and the supervisory authorities pursuant to Directive 2002/58/EC.	(58) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities should cooperate and exchange information on all relevant matters with data protection authorities and the supervisory authorities pursuant to ***Regulation (EU) 2016/679 and*** Directive 2002/58/EC.

Amendment 35

Proposal for a directive
Recital 59

Text proposed by the Commission	*Amendment*
(59) Maintaining accurate and complete databases of domain names and registration data (so called ‘WHOIS data’) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.	(59) Maintaining accurate and complete databases of domain names and registration data (so called ‘WHOIS data’) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with ***applicable*** Union data protection law.

Amendment 36

Proposal for a directive
Recital 62

Text proposed by the Commission	*Amendment*
(62) TLD registries and the entities providing domain name registration services for them should make ***publically*** available domain name registration data ***that fall outside the scope of Union data protection rules***, such as ***data that concern*** legal ***persons***[25] . TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with ***Union data protection law***. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to requests from ***legitimate access seekers*** for the disclosure of domain name registration data. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board.	(62) ***To comply with a legal obligation in terms of Article 6(1)(c) and Article 6(3) of Regulation (EU) 2016/679,*** TLD registries and the entities providing domain name registration services for them should make ***publicly*** available ***certain*** domain name registration data ***specified in the Member State law to which they are subject***, such as ***the domain name and the name of the*** legal ***person***. TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, ***notably to competent authorities under this Directive or supervisory authorities under Regulation (EU) 2016/679*** in accordance with ***their powers***. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to ***lawful and duly justified*** requests from ***public authorities, including competent authorities under this Directive, competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, or supervisory authorities under Regulation (EU) 2016/679,*** for the disclosure of domain name registration data. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also

include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board.

_____ _____

[25] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL recital (14) whereby "this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person".

Amendment 37

Proposal for a directive
Recital 63

Text proposed by the Commission	*Amendment*
(63) All essential and important entities under this Directive should 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 should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions.	(63) ***For the purposes of this Directive,*** all essential and important entities under this Directive should 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 should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should ***agree on constituent classifications,*** cooperate ***wherever possible***, provide ***real time*** mutual assistance to each other and where appropriate, carry out joint supervisory actions.

Amendment 38

Proposal for a directive
Recital 64

Text proposed by the Commission	*Amendment*
(64) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.	(64) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. ***For the purposes of this Directive,*** jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of

the group of undertakings.

Amendment 39

Proposal for a directive
Recital 69

Text proposed by the Commission	*Amendment*
(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of ***the following types*** of personal data***:*** IP addresses, uniform resources locators (URLs), domain names, and email addresses.	(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services ***is necessary for compliance with their legal obligations under national law transposing this Directive, and is therefore covered by Articles 6(1)(c) and 6(3) of Regulation (EU) 2016/679. Moreover, such processing*** should constitute a legitimate interest of the data controller concerned, as referred to in ***Article 6(1)(f) of*** Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. ***In many cases, personal data are compromised following cyber incidents and, therefore, the competent authorities and data protection authorities of EU Member States should cooperate and exchange information on all relevant matters in order to tackle any personal data breaches.*** Such measures may require the processing of ***certain categories*** of personal data***, including*** IP addresses, uniform resources locators (URLs), domain

names, and email addresses.

Amendment 40

Proposal for a directive
Recital 71

Text proposed by the Commission	*Amendment*
(71) In order to make enforcement effective, a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such sanctions across the Union. Due regard should be given to the ***nature, gravity*** and duration of the infringement, the actual damage caused or losses incurred or potential damage or losses that could have been triggered, the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The ***imposition of*** penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection and due process.	(71) In order to make enforcement effective, a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such sanctions across the Union. Due regard should be given to the ***seriousness*** and duration of the infringement, the actual damage caused or losses incurred or potential damage or losses that could have been triggered***, any relevant previous infringements, the manner in which the infringement became known to the competent authority***, the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The penalties ***imposed,*** including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection and due process.

Amendment 41

Proposal for a directive
Recital 74

Text proposed by the Commission	*Amendment*
(74) Member States should be able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice.	(74) Member States should be able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive***. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation***. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice.

Amendment 42

Proposal for a directive
Recital 76

Text proposed by the Commission	*Amendment*
(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity ***and the imposition of a temporary ban from the exercise of managerial functions by a natural person***. Given their ***severity*** and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions	(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity. Given their ***seriousness*** and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the

laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial ***protection***, due process, presumption of innocence and right of defence.	entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial ***remedies***, due process, presumption of innocence and right of defence.

Amendment 43

Proposal for a directive
Recital 77

Text proposed by the Commission	*Amendment*
(77) This Directive should establish cooperation rules between the competent authorities and the supervisory ***authorities in accordance with*** Regulation (EU) 2016/679 to deal with infringements related to personal data.	(77) This Directive should establish cooperation rules between the competent authorities ***under this Directive*** and the supervisory ***under*** Regulation (EU) 2016/679 to deal with infringements related to personal data.

Amendment 44

Proposal for a directive
Recital 79

Text proposed by the Commission	*Amendment*
(79) A peer-review mechanism should be introduced, allowing the assessment by experts designated by the Member States of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources.	(79) A peer-review mechanism should be introduced, allowing the assessment by experts designated by the Member States of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources. ***The EU should facilitate a coordinated response to large-scale cyber incidents and crises and offer assistance in order to***

aid recovery following such cyber attacks.

Amendment 45

Proposal for a directive
Recital 82 a (new)

Text proposed by the Commission	*Amendment*
	(82 a) This Directive does not apply to Union institutions, offices, bodies and agencies. However, Union bodies could be considered essential or important entities under this Directive. To achieve a uniform level of protection through consistent and homogeneous rules, the Commission should publish a legislative proposal to include Union institutions, offices, bodies and agencies in the EU-wide cybersecurity framework by 31 December 2022.

Amendment 46

Proposal for a directive
Recital 84

Text proposed by the Commission	*Amendment*
(84) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles,	(84) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles, ***and in full compliance with existing Union legislation regulating these issues. Any processing of personal data under this Directive is subject to Regulation (EU) 2016/679 and Directive***

	2002/58/EC, in their respective scope of application, including the tasks and powers of the supervisory authorities competent to monitor compliance with those legal instruments.

Amendment 47

Proposal for a directive
Article 2 – paragraph 1

Text proposed by the Commission	*Amendment*
1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.[28]	1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.[28] ***Article 3 Paragraph 4 of the Annex to Commission Recommendation 2003/361/EC is not applicable.***
[28] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	[28] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Amendment 48

Proposal for a directive
Article 2 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:	2. However, regardless of their size ***and based on a risk assessment according to Article 18***, this Directive also applies to entities referred to in Annexes I and II, where:

Amendment 49

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

Text proposed by the Commission	*Amendment*
(c) the entity is the sole provider of a service ***in a Member State***;	(c) the entity is the sole provider of a service ***at national or regional level***;

Amendment 50

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

Text proposed by the Commission	*Amendment*
(d) a ***potential*** disruption of the service provided by the entity could have an impact on public safety, public security or public health;	(d) a disruption of the service provided by the entity could have an impact on public safety, public security or public health;

Amendment 51

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

Text proposed by the Commission	*Amendment*
(e) a ***potential*** disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;	(e) a disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;

Amendment 52

Proposal for a directive
Article 2 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. Any processing of personal data pursuant to this Directive shall comply with Regulation (EU) 2016/679 and with Directive 2002/58/EC and shall be limited to what is strictly necessary and proportionate for the purposes of this

Directive.

Amendment 53

Proposal for a directive
Article 2 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is ***relevant and proportionate*** to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.	5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is ***necessary*** to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.

Amendment 54

Proposal for a directive
Article 2 – paragraph 6 a (new)

Text proposed by the Commission	*Amendment*
	6 a. Before 31 December 2021, the Commission shall publish a legislative proposal to include Union institutions, offices, bodies and agencies (EUIs) in the overall EU-wide cybersecurity framework, with a view to achieving a uniform level of protection through consistent and homogeneous rules.

Amendment 55

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

Text proposed by the Commission	*Amendment*
(b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;	(b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data***, and that are integrated into the IT system and are used for the provision of their intended services***;

Amendment 56

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

Text proposed by the Commission	*Amendment*
(4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the ***security of network and information systems*** in that Member State;	(4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the ***cybersecurity*** in that Member State;

Amendment 57

Proposal for a directive
Article 4 – paragraph 1 – point 12

Text proposed by the Commission	*Amendment*
(12) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;	***deleted***

Amendment 58

Proposal for a directive
Article 4 – paragraph 1 – point 22

Text proposed by the Commission	*Amendment*
(22) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, and in particular, via chats, posts, videos and recommendations);	***deleted***

Amendment 59

Proposal for a directive
Article 4 – paragraph 1 – point 24

Text proposed by the Commission	*Amendment*
(24) 'entity' means any natural ***or*** legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;	(24) 'entity' means any natural ***person or any*** legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;

Amendment 60

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

Text proposed by the Commission	*Amendment*
(a) a definition of objectives and priorities of the Member States' strategy on cybersecurity;	(a) a definition of objectives and priorities of the Member States' strategy on cybersecurity***, taking into account the general level of cybersecurity awareness amongst citizens as well as on the general level of security of consumer connected devices***;

Amendment 61

Proposal for a directive
Article 5 – paragraph 1 – point f

Text proposed by the Commission	*Amendment*
(f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[38] [Resilience of Critical Entities Directive] for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks.	(f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[38] [Resilience of Critical Entities Directive]***, both within and between Member States,*** for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks.
[38] [insert the full title and OJ publication reference when known]	[38] [insert the full title and OJ publication reference when known]

Amendment 62

Proposal for a directive
Article 5 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement;	(b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement***, including but not limited to encryption requirements and the promotion of the use of open source cybersecurity products***;

Amendment 63

Proposal for a directive
Article 5 – paragraph 2 – point d a (new)

Text proposed by the Commission	*Amendment*
	(da) a policy related to sustaining the use of open data and open source as part of security through transparency;

Amendment 64

Proposal for a directive
Article 5 – paragraph 2 – point d b (new)

Text proposed by the Commission	*Amendment*
	(db) a policy promoting the privacy and security of personal data of users of online services;

Amendment 65

Proposal for a directive
Article 5 – paragraph 2 – point e

Text proposed by the Commission	*Amendment*
(e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives;	(e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives***, including the development of training programmes on cybersecurity to provide entities with specialists and technicians***;

Amendment 66

Proposal for a directive
Article 5 – paragraph 2 – point f

Text proposed by the Commission	*Amendment*
(f) a policy on supporting academic and research institutions ***to develop*** cybersecurity tools and secure network infrastructure;	(f) a policy on supporting academic and research institutions ***that contribute to the national cybersecurity strategy by developing and deploying*** cybersecurity tools and secure network infrastructure ***that contribute to the national cybersecurity strategy, including specific policies addressing issues related to gender representation and balance in this sector***;

Amendment 67

Proposal for a directive
Article 5 – paragraph 2 – point h

Text proposed by the Commission	*Amendment*
(h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats.	(h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats ***and their capability to respond to cybersecurity incidents***.

Amendment 68

Proposal for a directive
Article 6 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties. The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.	2. ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties. The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated. ***To ensure security and accessibility of the information included in the registry, ENISA shall apply state of the art security measures and make the information available in machine-readable formats through corresponding***

interfaces.

Amendment 69

Proposal for a directive
Article 7 – paragraph 3 – point a

Text proposed by the Commission	*Amendment*
(a) objectives of national preparedness measures and activities;	(a) objectives of national ***and, where relevant and applicable, regional and cross-border*** preparedness measures and activities;

Amendment 70

Proposal for a directive
Article 10 – paragraph 2 – point e

Text proposed by the Commission	*Amendment*
(e) providing, upon request of an entity, a ***proactive scanning*** of the ***network and*** information systems used for the provision of their services;	(e) providing, upon request of an entity, a ***security scan*** of the information systems ***and network range*** used for the provision of their services ***to identify, mitigate or prevent specific threats***; ***the processing of personal data in the context of such scanning shall be limited to what is strictly necessary, and in any case to IP addresses and URLs;***

Amendment 71

Proposal for a directive
Article 11 – paragraph 4

Text proposed by the Commission	*Amendment*
4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data	4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data

protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State.	protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State ***in line with their respective competences***.
[39] [insert the full title and OJ publication reference when known]	[39] [insert the full title and OJ publication reference when known]

Amendment 72

Proposal for a directive
Article 11 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Member States shall ensure that their competent authorities regularly provide information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber threats and incidents affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those risks and incidents.	5. Member States shall ensure that their competent authorities regularly provide ***timely*** information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber threats and incidents affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those risks and incidents.

Amendment 73

Proposal for a directive
Article 12 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
3. The Cooperation Group shall be composed of representatives of Member	3. The Cooperation Group shall be composed of representatives of Member

States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group.	States, the Commission and ENISA. The European External Action Service***, the European Cybercrime Centre at Europol and the European Data Protection Board*** shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group.

Amendment 74

Proposal for a directive
Article 12 – paragraph 3 – subparagraph 1

Text proposed by the Commission	*Amendment*
Where ***appropriate***, the Cooperation Group ***may*** invite representatives of relevant stakeholders to participate in its work.	Where ***relevant for the performance of its tasks***, the Cooperation Group ***shall*** invite representatives of relevant stakeholders to participate in its work ***and the European Parliament to participate as observer***.

Amendment 75

Proposal for a directive
Article 12 – paragraph 8

Text proposed by the Commission	*Amendment*
8. The Cooperation Group shall meet regularly and at least ***once*** a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ***promote*** strategic cooperation and ***exchange of*** information.	8. The Cooperation Group shall meet regularly and at least ***twice*** a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ***facilitate*** strategic cooperation and ***real time*** information ***exchange***.

Amendment 76

Proposal for a directive
Article 13 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT–EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support cooperation among the CSIRTs.	2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT–EU. The Commission ***and the European Cybercrime Centre at Europol*** shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support cooperation among the CSIRTs.

Amendment 77

Proposal for a directive
Article 14 – paragraph 2

Text proposed by the Commission	*Amendment*
2. EU-CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission and ENISA. ENISA shall provide the secretariat of the network and support the secure exchange of information.	2. EU-CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission and ENISA. ***The European Cybercrime Centre at Europol shall participate in the activities of EU-CyCLONe as an observer.*** ENISA shall provide the secretariat of the network and support the secure exchange of information.

Amendment 78

Proposal for a directive
Article 14 – paragraph 6

Text proposed by the Commission	*Amendment*
6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements.	6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements***, and with law enforcement in the framework of the EU Law Enforcement Emergency Response Protocol***.

Amendment 79

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, ***an annual*** report on the state of cybersecurity in the Union. The report shall ***be delivered in machine-readable format and*** in particular include an assessment of the following:

Amendment 80

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

Text proposed by the Commission	*Amendment*
	(ca) the impact of cybersecurity incidents on the protection of personal data in the Union.

Amendment 81

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

Text proposed by the Commission	*Amendment*
	(cb) 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.

Amendment 82

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	2. Member States shall ensure that members of the management body ***and***

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.	***responsible specialists for cybersecurity*** follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess ***evolving*** cybersecurity risks and management practices and their impact on the operations of the entity.

Amendment 83

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 ***cybersecurity*** of network and information systems ***used for*** the provision of their ***services, and in view of assuring the continuity of these*** services ***and to mitigate the risks posed to the rights of individuals when their personal data are processed***. Having regard to the state of the art, those measures shall ensure a level of ***cybersecurity*** of network and information systems appropriate to the risk presented.

Amendment 84

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.

Amendment 85

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 ***and proportionate*** 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. ***Competent authorities shall provide guidance to entities on the practical and proportionate application.***

Amendment 86

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

Text proposed by the Commission	*Amendment*
	6 a. Member States shall give the user of a network and information system provided by an essential or important entity the right to obtain from the entity information on the technical and organisational measures in place to manage the risks posed to the security of network and information systems. Member States shall define the limitations to that right.

Amendment 87

Proposal for a directive
Article 19 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Cooperation Group, in cooperation with the Commission and ENISA, ***may*** carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and,	1. The Cooperation Group, in cooperation with the Commission and ENISA, ***shall*** carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and,

where relevant, non-technical risk factors.

where relevant, non-technical risk factors.

Amendment 88

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 ***and in any event within 24 hours***, 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***, and the competent law enforcement authorities if the incident is of a suspected or known malicious nature.*** Those entities shall notify, without undue delay***, and in any event within 24 hours***, 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 way of exception, where public disclosure could trigger further cyberattacks, those entities may 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.

Amendment 89

Proposal for a directive
Article 20 – paragraph 2 – introductory part

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	2. Member States shall ensure that essential and important entities ***are able to*** notifythe competent authorities or the CSIRT of any significant cyber threat that

cyber threat that those entities identify that could have potentially resulted in a significant incident.	those entities identify that could have potentially resulted in a significant incident.

Amendment 90

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

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, those entities shall ***be allowed to*** notifythe 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 ***such notification is provided***, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.

Amendment 91

Proposal for a directive
Article 20 – paragraph 4 – 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:

Amendment 92

Proposal for a directive
Article 20 – paragraph 4 – point c – point ii

Text proposed by the Commission	*Amendment*
(ii) the type of threat or root cause that likely triggered the incident;	(ii) the type of ***cyber*** threat or root cause that likely triggered the incident;

Amendment 93

Proposal for a directive
Article 20 – paragraph 4 – point c – point iii

Text proposed by the Commission	*Amendment*
(iii) applied and ongoing mitigation measures.	(iii) applied and ongoing mitigation measures ***or remedies***.

Amendment 94

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 the other affected Member States and ENISA of the incident. ***If the incident concerns two or more Member States and is suspected to be of criminal nature, the competent authority or the CSIRT shall inform EUROPOL***. 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.

Amendment 95

Proposal for a directive
Article 22 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing	2. ENISA, ***after having consulted the EDPB and*** in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as

standards, including Member States' national standards, which would allow for those areas to be covered.	well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.

Amendment 96

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 ***have policies and procedures in place to ensure that*** accurate and complete domain name registration data ***is collected and maintained*** in a dedicated database facility ***in accordance*** with to Union data protection law as regards data which are personal data. ***Member States shall ensure that such policies and procedures are made publicly available.***

Amendment 97

Proposal for a directive
Article 23 – paragraph 2

Text proposed by the Commission	*Amendment*
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.	2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain ***the*** information ***necessary*** to identify and contact the holders of the domain names***, namely their name, their physical and e-mail address as well as their telephone number,*** and the points of contact administering the domain names under the TLDs.

Amendment 98

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.	***deleted***

Justification

This paragraph has been included in Article 23(1).

Amendment 99

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 entities providing domain name registration services for the TLD publish, ***in accordance with Article 6(1)(c) and Article 6(3) of Regulation (EU) 2016/679 and*** without undue delay after the registration of a domain name, ***certain*** domain ***name*** registration data***, such as the domain name and the name of the legal person***.

Amendment 100

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 entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of ***public authorities, including competent authorities under this Directive, competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, or supervisory authorities under Regulation (EU) 2016/679*** , 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 ***lawful and duly justified*** requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Amendment 101

Proposal for a directive
Article 24 – paragraph 3

Text proposed by the Commission	*Amendment*
3. If an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-compliance with the obligations under this	3. If an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. ***Without prejudice to the competences of the supervisory authorities under Regulation (EU) 2016/679,*** such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the

Directive.	entity provides services may take legal actions against the entity for non-compliance with the obligations under this Directive.

Amendment 102

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]:

Amendment 103

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 ***or Directive 2002/58/EC***, 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, ***and the location or identity of the attacker*** where such information sharing:

Amendment 104

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 ***supervisory*** authorities when addressing incidents resulting in personal data breaches ***without prejudice to the competences, tasks and powers of supervisory authorities pursuant to Regulation (EU) 2016/679. To this end, competent authorities and supervisory authorities shall exchange information relevant for their respective area of competence. Moreover, competent authorities shall, upon request of the competent supervisory authorities, provide them all information obtained in the context of any audits and investigations that relate to the processing of personal data.***

Amendment 105

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;	***deleted***

Amendment 106

Proposal for a directive
Article 29 – paragraph 5 – 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	***deleted***

other natural person held responsible for the breach, from exercising managerial functions in that entity.

Amendment 107

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

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.	***This sanction*** 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.

Amendment 108

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 ***material or non-material*** damage caused or losses incurred 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;

Amendment 109

Proposal for a directive
Article 29 – paragraph 7 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) any relevant previous infringements by the entity concerned;

Amendment 110

Proposal for a directive
Article 29 – paragraph 7 – point c b (new)

Text proposed by the Commission	*Amendment*
	(cb) the manner in which the infringement became known to the competent authority, in particular whether, and if so to what extent, the entity notified the infringement;

Amendment 111

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

Text proposed by the Commission	*Amendment*
(g) the level of cooperation ***of the natural or legal person(s) held responsible*** with the competent authorities***.***	(g) the level of cooperation with the competent authorities ***in order to remedy the infringement and mitigate possible adverse effects of the infringements;***

Amendment 112

Proposal for a directive
Article 29 – paragraph 7 – point g a (new)

Text proposed by the Commission	*Amendment*
	(ga) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly, from the infringement.

Amendment 113

Proposal for a directive
Article 29 – paragraph 9

Text proposed by the Commission	*Amendment*
9. Member States shall ensure that their competent authorities inform the relevant competent authorities of ***the*** Member ***State concerned*** designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. Upon request of competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.	9. Member States shall ensure that their competent authorities inform ***in real time*** the relevant competent authorities of ***all*** Member ***States*** designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. Upon request of competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.

Amendment 114

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;	***deleted***

Amendment 115

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	h) make a public statement which identifies the legal person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of

the nature of that infringement;	that infringement;

Amendment 116

Proposal for a directive
Article 31 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Administrative fines shall***, depending on the circumstances of each individual case,*** be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).	2. Administrative fines shall be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4)***, depending on the circumstances of each individual case***.

Amendment 117

Proposal for a directive
Article 31 – paragraph 3

Text proposed by the Commission	*Amendment*
3. ***Where*** deciding whether to impose an administrative fine ***and*** deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article 29(7).	3. Deciding whether to impose an administrative fine ***shall depend on the circumstances of each individual case, and when*** deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article 29(7).

Amendment 118

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	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***.	inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ***without undue delay and in any case*** within ***24 hours***.

Amendment 119

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.

Amendment 120

Proposal for a directive
Article 34 a (new)

Text proposed by the Commission	*Amendment*
	Article 34 a
	Liability for non-compliance
	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.

Amendment 121

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	The Commission shall review the functioning of this Directive ***every 3 years***, and report to the European Parliament and to the Council. The report shall in

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***]***.	particular assess ***to what extent the Directive has contributed to ensuring a high common level of security and integrity of network and information systems, while giving an optimal protection to private life and personal data, and*** 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***]***.

Amendment 122

Proposal for a directive
Annex I – Point 5 (Health) – indent 6 (new)

Text proposed by the Commission

Sector	Subsector	Type of entity
5. Health		– Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU (90)
		– EU reference laboratories referred to in Article 15 of Regulation XXXX/XXXX on serious cross-border threats to health[91]
		– Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC ([92])
		– Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2
		– Entities manufacturing medical devices considered as critical during a public health emergency (‘the public health emergency critical devices list’) referred to in Article 20 of Regulation XXXX[93]

[91] [Regulation of the European Parliament and of the Council on serious cross-border threats to

health and repealing Decision No 1082/2013/EU, reference to be updated once the proposal COM (2020)727 final is adopted]

[92] Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p.67).

[93] [Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal produces and medical devices, reference to be updated once the proposal COM(2020)725 final is adopted]

Amendment

Sector	Subsecto	Type of entity
5. Health		– Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU (90)
		– EU reference laboratories referred to in Article 15 of Regulation XXXX/XXXX on serious cross-border threats to health[91]
		– Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC ([92])
		– Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2
		– Entities manufacturing medical devices considered as critical during a public health emergency (‘the public health emergency critical devices list’) referred to in Article 20 of Regulation XXXX[93]
		– Entities holding a distribution authorisation referred to in Article 79 of Directive 2001/83/EC

[91] [Regulation of the European Parliament and of the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU, reference to be updated once the proposal COM (2020)727 final is adopted]

[92] Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p.67).

[93] [Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal produces and medical devices, reference to be updated once the proposal COM(2020)725 final is adopted]

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
References	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Committee responsible Date announced in plenary	ITRE 21.1.2021
Opinion by Date announced in plenary	LIBE 21.1.2021
Associated committees - date announced in plenary	20.5.2021
Rapporteur for the opinion Date appointed	Lukas Mandl 12.4.2021
Discussed in committee	16.6.2021 3.9.2021 11.10.2021
Date adopted	12.10.2021
Result of final vote	+: 44 –: 14 0: 4
Members present for the final vote	Magdalena Adamowicz, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Maria Grapini, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Javier Zarzalejos
Substitutes present for the final vote	Olivier Chastel, Tanja Fajon, Jan-Christoph Oetjen, Philippe Olivier, Anne-Sophie Pelletier, Thijs Reuten, Rob Rooken, Maria Walsh

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

44	+
ID	Nicolas Bay, Nicolaus Fest, Peter Kofod, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche
NI	Laura Ferrara
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Elissavet Vozemberg-Vrionidi, Maria Walsh, Javier Zarzalejos
Renew	Olivier Chastel, Anna Júlia Donáth, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Jan-Christoph Oetjen, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Marina Kaljurand, Juan Fernando López Aguilar, Javier Moreno Sánchez, Thijs Reuten, Birgit Sippel, Bettina Vollath
Verts/ALE	Damien Carême

14	-
ECR	Jorge Buxadé Villalba, Patryk Jaki, Assita Kanko, Nicola Procaccini, Rob Rooken, Jadwiga Wiśniewska
ID	Marcel de Graaff
NI	Martin Sonneborn, Milan Uhrík
Verts/ALE	Patrick Breyer, Saskia Bricmont, Terry Reintke, Diana Riba i Giner, Tineke Strik

4	0
The Left	Pernando Barrena Arza, Clare Daly, Cornelia Ernst, Anne-Sophie Pelletier

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

15.7.2021

OPINION OF THE COMMITTEE ON FOREIGN AFFAIRS

for the Committee on Industry, Research and Energy

on the proposal for a 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 (2020/0359(COD))

Rapporteur for opinion: Markéta Gregorová

AMENDMENTS

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

Amendment 1

Proposal for a directive
Recital 2

Text proposed by the Commission	*Amendment*
(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national cybersecurity strategies, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group[12]	(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national cybersecurity strategies, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group[12]

and a network of national Computer Security Incident Response Teams ('CSIRTs network')[13] . Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges.

and a network of national Computer Security Incident Response Teams ('CSIRTs network')[13]***. Directive (EU) 2016/1148 was the first Union-wide legislative act on cybersecurity, providing legal measures to boost the overall level of cyber resilience also in the security and defence domain in the Union by ensuring Member States' cooperation and a culture of security across sectors***. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges***, which very often originate from outside the Union, posing a serious threat to internal and external security at Union level***.

[12] Article 11 of Directive (EU) 2016/1148.

[13] Article 12 of Directive (EU) 2016/1148.

[12] Article 11 of Directive (EU) 2016/1148.

[13] Article 12 of Directive (EU) 2016/1148.

Amendment 2

Proposal for a directive
Recital 3 a (new)

Text proposed by the Commission	*Amendment*
	(3a) The Union understands hybrid campaigns to be 'multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological) to destabilise the adversary. They are designed to be difficult to detect or attribute, and can be used by state and non-state actors'[1a]. The internet and online networks allow State and non-State actors to conduct aggressive action in new ways. They can be used to hack critical infrastructure and democratic processes, launch persuasive disinformation and propaganda campaigns, steal information and upload sensitive data into the public

domain. In the worst cases, cyber attacks allow an adversary to take control of assets such as military systems and command structures[1b]. At the same time, thorough cooperation with the private sector and civilian stakeholders, including industries and entities involved in the management of critical infrastructures, is crucial and should be reinforced due to the intrinsic characteristics of the cyber domain, in which technological innovation is mainly driven by private companies that often do not operate in the military field. Such large-scale cybersecurity incidents and crises at Union level should be adequately prepared for and protected against via joint training exercises as they have the potential to invoke Article 222 TFEU (the 'solidarity clause').

[1a] European Commission/High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats", JOIN(2018) 16 final, Brussels, June 13, 2018, p. 1.

[1b]

https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf

Amendment 3

Proposal for a directive
Recital 3 b (new)

Text proposed by the Commission	*Amendment*
	(3b) During large-scale cyber security incidents and crises at Union level, the high degree of interdependence between sectors and countries require a coordinated action to ensure a rapid and effective response, as well as better prevention and preparedness for similar situations in the future. The availability of

cyber-resilient networks and information systems and the availability, confidentiality and integrity of data are vital for the security of the Union within as well as beyond its borders. The Union's ambition to acquire a more prominent geopolitical role also rests on credible cyber defence and deterrence, including the capacity to identify malicious actions in a timely, effective manner and to respond adequately. Given the blurring of lines between the realms of civilian and military matters and the dual-use nature of cyber tools and technologies, there is a need for a comprehensive and holistic approach to the digital domain. This also applies to Common Security and Defence Policy (CSDP) operations and missions conducted by the Union to ensure peace and stability in its neighbourhood and beyond. In this regard the Union's Strategic Compass should enhance and guide the implementation of the Union's level of ambition in the field of security and defence, and translate that ambition into capability needs in cyber defence, thereby increasing the ability of the Union and Member States to prevent, discourage, deter, respond to and recover from malicious cyber activities by strengthening its posture, situational awareness, tools, procedures and partnerships. The Union's cooperation with international organisations such as NATO contributes to discussions on how to prevent, deter and respond to hybrid and cyber-attacks, and explore ways to establish a common cyber threat analysis.

Amendment 4

Proposal for a directive
Recital 6

Text proposed by the Commission	*Amendment*
(6) This Directive leaves unaffected the ability of Member States to take the	(6) This Directive leaves unaffected the ability of Member States to take the

necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14] , are of relevance.

[14] The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).

necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences, in compliance with Union law ***and fundamental rights. Independently of the technological environment, it is essential tofully respect due process and other safeguards, in particular fundamental rights, such as the right to respect for private life and communications and the right to the protection of personal data. Similarly, in order to ensure an all-encompassing resilience, it is necessary not only to strengthen technological infrastructures and to possess response capabilities, but also to raise public awareness about cyber risks and security.*** In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14] , are of relevance.

[14] The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).

Amendment 5

Proposal for a directive
Recital 14 a (new)

Text proposed by the Commission	*Amendment*
	(14a) With a view to develop a secure connectivity system and build on the

European quantum communication infrastructure (EuroQCI) and the European Union Governmental Satellite Communication (GOVSATCOM), in particular the implementation of GALILEO GNSS for defence users, where future possible development should, inter alia, take into account the impact of merging the speed and sophistication of quantum computing with highly autonomous military systems, Member States should ensure the protection of entire electronic communications infrastructure, such as space, land and submarine network systems. At the same time, a common vision on Cloud Adoption Strategy for sensitive sectors should be established, with the aim of defining a Union approach based on shared standards among like-minded partner countries.

Amendment 6

Proposal for a directive
Recital 20

Text proposed by the Commission	*Amendment*
(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have	(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. ***Infrastructure that is owned, managed or operated by or on behalf of the Union as part of its space programmes is***

cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.

particularly important for the security of the Union and its Member States and the proper functioning of the CSDP missions. Such infrastructure is to be adequately protected in accordance with Regulation (EU) 2021/696 of the European Parliament and of the Council[18a]. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market ***and put at risk the security and safety of Union citizens***. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.

[18a] Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU (OJ L 170, 12.5.2021, p. 69).

Amendment 7

Proposal for a directive
Recital 26

Text proposed by the Commission	*Amendment*
(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive.	(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive***, in order to contribute to the development of Union standards that can shape the cybersecurity landscape at international level. Member States could also explore the possibility of increasing cooperation with like-minded partner***

countries and international organisations such as the Council of Europe, the North Atlantic Treaty Organisation, the Organisation for Economic Cooperation and Development, the Organisation for Security and Co-operation in Europe and the United Nations with the aim to secure multilateral agreements on cyber norms, responsible state and non-state behaviour in cyberspace and effective global digital governance as well as to create an open, free, stable and secure cyberspace based in international law.

Amendment 8

Proposal for a directive
Recital 27

Text proposed by the Commission	*Amendment*
(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20], a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.	(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20], a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market ***or risk the security and safety of citizens and the economic and financial interest of the Union***. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union. ***The Union and Member States should also further promote exercises and scenario-based policy discussion on crisis management framework, to ensure internal and external policy coherence***

	and to build a common understanding of the procedures for the implementation of the solidarity clause.
[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).	[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

Amendment 9

Proposal for a directive
Recital 36

Text proposed by the Commission	*Amendment*
(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. Such agreements ***should*** ensure adequate protection of data.	(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. Such agreements ***are to*** ensure adequate protection of data ***and should promote market access as well as address security risks while increasing global resilience and raise awareness about cyber threats and malicious cyber activities. The Union should also continue to support capacity building in third countries. Member States should, where appropriate, encourage the participation of like-minded partner countries, which share our Union values, in relevant PESCO projects. Therefore, the Union should investigate the possibility to re-launch processes aiming at concluding formal and structured frameworks for cooperation in this field in the future.***

Amendment 10

Proposal for a directive
Recital 37

Text proposed by the Commission	*Amendment*
(37) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework set out in Recommendation (EU) 2017/1584 through the existing cooperation networks, notably the Cyber Crisis Liaison Organisation Network (EU-CyCLONe), CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements defining the modalities of that cooperation. The EU-CyCLONe's rules of procedures should further specify the modalities through which the network should function, including but not limited to roles, cooperation modes, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis management at Union level, relevant parties should rely on the Integrated Political Crisis Response (IPCR) arrangements. The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for this purpose. If the crisis entails an important external or ***Common Security and Defence Policy (***CSDP***)*** dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated.	(37) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework set out in Recommendation (EU) 2017/1584 through the existing cooperation networks, notably the Cyber Crisis Liaison Organisation Network (EU-CyCLONe), CSIRTs network and the Cooperation Group***, the European Cybercrime Centre and the Union's Intelligence and Situation Centre (EU INTCEN), to advance strategic intelligence cooperation on cyber threats and activities, in order to further support Union situational awareness and decision-making on a joint diplomatic response.*** EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements defining the modalities of that cooperation. The EU-CyCLONe's rules of procedures should further specify the modalities through which the network should function, including but not limited to roles, cooperation modes, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis management at Union level, relevant parties should rely on the Integrated Political Crisis Response (IPCR) arrangements***, which also support the coordination at political level of the response to the invoking of the solidarity clause.*** The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for this purpose. If the crisis entails an important external or CSDP dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated***, as well as any measure aiming to protect CSDP missions and operations and Union delegations. In addition, the Union should make full use of its cyber diplomacy toolbox.***

Amendment 11

Proposal for a directive
Recital 40 a (new)

Text proposed by the Commission	*Amendment*
	(40a) Member States should consider an active cyber defence programme to be part of their national cybersecurity strategy that incorporates regular joint training exercises between Member States and across international organisations. Such a programme should provide a synchronised, real-time capability to discover, detect, analyse, and mitigate threats. Active cyber defence operates at network speed using sensors, software and intelligence to detect and stop malicious activity ideally before it can affect networks and systems. Moreover, Member States should significantly enhance information sharing method, to define a common communication standard that could be used for classified and non-classified information, in order to enhance the rapid action. The Union and the Member States should also strengthen their capabilities to attribute cyber attacks in order to effectively deter and respond to cyber attacks in a proportionate manner, in line with international law.

Amendment 12

Proposal for a directive
Recital 40 b (new)

Text proposed by the Commission	*Amendment*
	(40b) Member States should come forward with an active cyber defence programme in their national cybersecurity strategies. Active cyber defence is the proactive detection, analysis and mitigation of network security breaches in real-time combined with the use of capabilities deployed outside the victim network. It is based on a defensive

strategy that excludes offensive measures against the adversaries critical civilian infrastructure which would constitute a breach of international law (such as of the 1977 Additional Protocol to the Geneva Conventions). The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enabling unity of effort in successfully detecting and preventing cyber attacks. Active cyber defence activities could include email server configurations, website configurations, logging enabling and DNS filtering. Member State should adopt policies able to ensure the widest possible access to the most performing cybersecurity tools, supporting companies, small and medium-sized enterprises and businesses with low financial capabilities, trough benefits, grants, loans or fiscal advantages dedicated to the acquisition of highest-level cybersecurity products and services, avoiding that their costs represent an element of discrimination. Member States should also aim to promote partnerships with academic institutions and other research centres aiming to foster R&D cybersecurity programme in order to develop new common technologies, tools and skills applicable in both civilian and defence sectors through a multidisciplinary approach. Partnerships should be financed by existing and new funding tools under the auspices of the Commission.

Amendment 13

Proposal for a directive
Recital 43

Text proposed by the Commission	*Amendment*
(43) Addressing cybersecurity risks stemming from an entity's supply chain	(43) Addressing cybersecurity risks stemming from an entity's supply chain

and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their ***risk-management systems***, secure development procedures ***in accordance with Union cybersecurity standards***.

Amendment 14

Proposal for a directive
Recital 43 a (new)

Text proposed by the Commission	*Amendment*
	(43a) Potential non-technical risk factors, such as undue influence by a third country on suppliers and service providers, especially in the case of alternative models of governance, include concealed vulnerabilities or backdoors and potential systemic supply disruptions, especially in case of technological lock-in or provider dependency. Since the exploitation of vulnerabilities in defence sector may cause significant disruption and harm, cyber security of defence industry requires special measures to ensure the security of the supply chains, particularly entities lower in supply chains, which do not require access to classified information, but that could carry serious risks to the entire sector. Special consideration should be given to the impact any breach could have and the threat of any potential manipulation of network data that could render critical defence assets useless or even override their operating systems making them

	vulnerable to hijacking.

Amendment 15

Proposal for a directive
Recital 46

Text proposed by the Commission	*Amendment*
(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission ENISA should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21] , with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.	(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission***,*** ENISA ***and the European External Action Service*** should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21] , with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.
[21] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).	[21] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

Amendment 16

Proposal for a directive
Recital 68

Text proposed by the Commission	*Amendment*
(68) Entities should be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus	(68) Entities should be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus

necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules.	necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. ***In addition, Member States could also explore the possibility of reaching out to like-minded partner countries.*** Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules. ***To the same end, Member States should support competent authorities and CSIRTs to establish free-of-charge or accessible cybersecurity assistance, education, and audit programs for entities that fall outside the scope of this Directive, in particular start-ups, SMEs and non-governmental organisations(NGOs).***

Amendment 17

Proposal for a directive
Recital 68 a (new)

Text proposed by the Commission	*Amendment*
	(68a) Given that cybersecurity has both a civilian and a military dimension, information exchange across sectors (defence, civilian, law enforcement and external action) should also be encouraged. The Joint Cyber Unit could play an important role in protecting the Union from cyber-attacks by helping actors to acquire a common understanding of the threat landscape and to coordinate their response.

Amendment 18

Proposal for a directive
Recital 73

Text proposed by the Commission	*Amendment*
(73) Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers by the competent authorities or of other penalties laid down in the national rules transposing this Directive.	(73) Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine***, without prejudice to the objectives of this Directive***. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers by the competent authorities or of other penalties laid down in the national rules transposing this Directive.

Amendment 19

Proposal for a directive
Article 5 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services;	(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services***, based on a comprehensive assessment of potential threats to supply chains***;

Amendment 20

Proposal for a directive
Article 5 – paragraph 2 – point b a (new)

Text proposed by the Commission	*Amendment*

	(ba) a policy for promoting interoperability and adherence to common Union standards in cybersecurity;

Amendment 21

Proposal for a directive
Article 5 – paragraph 2 – point d

Text proposed by the Commission	*Amendment*
(d) a policy related to sustaining the general availability and integrity of the public core of the open internet;	(d) a policy related to sustaining the general availability and integrity of the public core of the open internet***, including cybersecurity, where applicable, of undersea communications cables***;

Amendment 22

Proposal for a directive
Article 5 – paragraph 2 – point f

Text proposed by the Commission	*Amendment*
(f) a policy on supporting academic and research institutions ***to develop*** cybersecurity tools and secure network infrastructure;	(f) a policy on supporting academic and research institutions ***in cybersecurity research and in the development of*** cybersecurity tools and secure network infrastructure;

Amendment 23

Proposal for a directive
Article 5 – paragraph 2 – point h

Text proposed by the Commission	*Amendment*
(h) a policy addressing specific needs of ***SMEs***, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats***.***	(h) a policy addressing specific needs of ***start-ups, SMEs and NGOs***, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats***, responding to cybersecurity incidents, and seeking cybersecurity assistance;***

Amendment 24

Proposal for a directive
Article 5 – paragraph 2 – point h a (new)

Text proposed by the Commission	*Amendment*
	(ha) a policy to promote the use and development of open source software.

Amendment 25

Proposal for a directive
Article 6 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of ***coordinated*** vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.	1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of ***mandatory responsible*** vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.

Amendment 26

Proposal for a directive
Article 6 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in	2. ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in

particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties. The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.	particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties. ***In accordance with Article 10(2), CSIRTs shall facilitate access to information on vulnerabilities registered in the European vulnerability registry, alongside risk mitigation assistance, to entities that do not fall within the scope of this Directive, in particular start-ups, SMEs and NGOs.*** The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.

Amendment 27

Proposal for a directive
Article 7 – paragraph 3 – point f

Text proposed by the Commission	*Amendment*
(f) national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.	(f) national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level***, including responses to relevant requests under the solidarity clause***.

Amendment 28

Proposal for a directive

Article 7 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall communicate to the Commission the designation of their competent authorities referred to in paragraph 1 and submit their national cybersecurity incident and crisis response plans as referred to in paragraph 3 within three months from that designation and the adoption of those plans. Member States may exclude specific information from the plan where and to the extent that it is strictly necessary for their national security.	4. Member States shall communicate to the Commission the designation of their competent authorities referred to in paragraph 1 and submit their national cybersecurity incident and crisis response plans as referred to in paragraph 3 within three months from that designation and the adoption of those plans. Member States may exclude specific information from the plan where and to the extent that it is strictly necessary for their national security. ***In the event of a large-scale cybersecurity incident and crisis involving more than one Member State, and with relevance to the Union level, appropriate crisis management and governance shall be established. Such structures shall organise exchange of information, coordination and cooperation with the Union's external security and military crisis management structures, and Member States's bodies in charge of security and defence.***

Amendment 29

Proposal for a directive
Article 9 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. CSIRTs shall cooperate and exchange relevant information with national institutions responsible for the maintenance of public security, defence, and national security.

Amendment 30

Proposal for a directive
Article 9 – paragraph 4 b (new)

Text proposed by the Commission	*Amendment*
	4b. CSIRTs shall cooperate and, without prejudice to Union law, in particular Regulation (EU) 2016/679, exchange relevant information with trusted third countries and international organisations on cyber threats, vulnerabilities, best practices, and standards.

Amendment 31

Proposal for a directive
Article 9 – paragraph 4 c (new)

Text proposed by the Commission	*Amendment*
	4c. CSIRTs shall, without prejudice to Union law, in particular Regulation (EU) 2016/679, provide cybersecurity assistance to CSIRTs or equivalent structures in Union candidate countries and to other third countries in the Western Balkans and the Eastern Partnership.

Amendment 32

Proposal for a directive
Article 10 – paragraph 2 – point e a (new)

Text proposed by the Commission	*Amendment*
	(ea) establishing free-of-charge or accessible cybersecurity assistance, education, and audit programs for entities that fall outside the scope of this Directive, in particular start-ups, SMEs and NGOs;

Amendment 33

Proposal for a directive
Article 11 – paragraph 4

Text proposed by the Commission	*Amendment*
4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State.	4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities***, national supervisory authorities for artificial intelligence, national competent authorities for data governance***, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State.
[39] [insert the full title and OJ publication reference when known]	[39] [insert the full title and OJ publication reference when known]

Amendment 34

Proposal for a directive
Article 12 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
3. The Cooperation Group shall be composed of representatives of Member States, the Commission ***and*** ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] ***may*** participate in the activities of the Cooperation Group.	3. The Cooperation Group shall be composed of representatives of Member States, the Commission***, EU – CyCLONe,*** ENISA***, and the European Defence Agency***. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. ***National supervisory authorities for artificial intelligence, national competent authorities for data governance, and*** the European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] ***shall*** participate in the activities of the Cooperation Group.

Amendment 35

Proposal for a directive
Article 12 – paragraph 4 – point e a (new)

Text proposed by the Commission	*Amendment*
	(ea) without prejudice to Union law, engaging in cooperation, mutual assistance, and exchanging best practices and information with trusted third countries and international organisations;

Amendment 36

Proposal for a directive
Article 13 – paragraph 3 – point k

Text proposed by the Commission	*Amendment*
(k) cooperating and exchanging information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and threats across the Union;	(k) cooperating and exchanging information with regional and Union-level Security Operations Centres (SOCs) ***and, where appropriate, with military CERTs*** in order to improve common situational awareness on incidents and threats across the Union;

Amendment 37

Proposal for a directive
Article 14 – paragraph 2

Text proposed by the Commission	*Amendment*
2. EU-CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission and ENISA. ENISA shall provide the secretariat of the network and support the secure exchange of information.	2. EU-CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission***, the EEAS*** and ENISA. ENISA shall provide the secretariat of the network and support the secure exchange of information. ***Such national crisis management authorities shall be provided by advice by a civil society based advisory***

	group. For large-scale cybersecurity incidents and crises at Union level involving more than one Member State, a Union level crisis management structure involving all relevant actors shall be established. That structure shall include Joint Cyber Unit, CSIRTs, the CSIRTs network, the Coordination Group, the Commission, the EEAS and ENISA. It shall also prepare and implement the invoking and use of the solidarity clause.

Amendment 38

Proposal for a directive
Article 14 – paragraph 3 – point a

Text proposed by the Commission	*Amendment*
(a) increasing the level of preparedness of the management of large scale incidents and crises;	(a) increasing the level of preparedness of the management of large scale incidents and crises ***and liaising with Member State agencies in charge of state security and territorial defence***;

Amendment 39

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 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. ***Member States shall encourage essential and important entities to evaluate, on a regular basis, members of the management bodies referenced in paragraph 1 of this Article on the adequacy of their skills for ensuring compliance with Article 18.***

Amendment 40

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 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 ***in accordance with Union cybersecurity standards and law and potential non-technical risk factors, such as concealed vulnerabilities or backdoors and potential systemic supply disruptions***.

Amendment 41

Proposal for a directive
Article 19 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Cooperation Group, in cooperation with the Commission ***and*** ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.	1. The Cooperation Group, in cooperation with the Commission***,*** ENISA ***and the European External Action Service***, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.

Amendment 42

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 European External Action Service***, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.

Amendment 43

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

Text proposed by the Commission	*Amendment*
	2a. Upon identifying risks to specific critical ICT services, systems or production supply chains, the Commission, after consulting the Cooperation Group, ENISA, and the European External Action Service shall issue recommendations to Member States and the national competent authorities defined in this Regulation for remedying and increasing resilience to the identified risks.

Amendment 44

Proposal for a directive
Article 25 – paragraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) information on the management body responsible for the cybersecurity risk management measures laid down in Article 18, in accordance with Article 17;

Amendment 45

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 or risk-related available information***, including on risks related to supply chains as defined in Article 18(3)***;

Amendment 46

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 or risk-related available information***, including on risks related to supply chains as defined in Article 18(3)***;

Amendment 47

Proposal for a directive
Annex I – ESSENTIAL ENTITIES: SECTORS, SUBSECTORS AND TYPES OF ENTITIES – Sector 6 a (new)

Text proposed by the Commission	*Amendment*
	6a. Education and research — Higher education institutions and research institutions

Amendment 48

Proposal for a directive
Annex I – ESSENTIAL ENTITIES: SECTORS, SUBSECTORS AND TYPES OF ENTITIES – Sector 9 Public administration – Type of entities

Text proposed by the Commission	*Amendment*
– Public administration entities of central governments	– Public administration entities of central governments
– Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 ([27])	– Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 ([27]***, 27 a (new)***)
– Public administration entities of NUTS level 2 regions listed in Annex I of	– Public administration entities of NUTS level 2 regions listed in Annex I of

Regulation (EC) No 1059/2003	Regulation (EC) No 1059/2003 *(27 b (new))*
[27] Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1).	[27] Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1). *27 a (new)* ***Or the equivalent administrative units, in Member States where the NUTS classification is not yet reflected in the administration institutional setup.*** *27 b (new)* ***Or the equivalent administrative units, in Member States where the NUTS classification is not yet reflected in the administration institutional setup.***

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
References	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Committee responsible Date announced in plenary	ITRE 21.1.2021
Opinion by Date announced in plenary	AFET 21.1.2021
Rapporteur for the opinion Date appointed	Markéta Gregorová 22.2.2021
Discussed in committee	25.5.2021 16.6.2021 17.6.2021
Date adopted	14.7.2021
Result of final vote	+: 59 –: 5 0: 6
Members present for the final vote	Alviina Alametsä, Alexander Alexandrov Yordanov, Maria Arena, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Reinhard Bütikofer, Fabio Massimo Castaldo, Susanna Ceccardi, Włodzimierz Cimoszewicz, Katalin Cseh, Tanja Fajon, Anna Fotyga, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Raphaël Glucksmann, Klemen Grošelj, Bernard Guetta, Márton Gyöngyösi, Andrzej Halicki, Sandra Kalniete, Dietmar Köster, Maximilian Krah, Andrius Kubilius, Ilhan Kyuchyuk, David Lega, Miriam Lexmann, Nathalie Loiseau, Antonio López-Istúriz White, Jaak Madison, Claudiu Manda, Thierry Mariani, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Javier Nart, Urmas Paet, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Manu Pineda, Giuliano Pisapia, Thijs Reuten, Jérôme Rivière, María Soraya Rodríguez Ramos, Nacho Sánchez Amor, Isabel Santos, Jacek Saryusz-Wolski, Andreas Schieder, Radosław Sikorski, Jordi Solé, Sergei Stanishev, Tineke Strik, Hermann Tertsch, Hilde Vautmans, Harald Vilimsky, Idoia Villanueva Ruiz, Viola Von Cramon-Taubadel, Thomas Waitz, Witold Jan Waszczykowski, Charlie Weimers, Isabel Wiseler-Lima, Salima Yenbou, Željana Zovko
Substitutes present for the final vote	Ioan-Rareş Bogdan, Andrey Kovatchev, Marisa Matias, Gabriel Mato, Milan Zver

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

59	+
ECR	Anna Fotyga, Jacek Saryusz-Wolski, Hermann Tertsch, Witold Jan Waszczykowski
ID	Anna Bonfrisco, Susanna Ceccardi
NI	Fabio Massimo Castaldo, Márton Gyöngyösi
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Ioan-Rareş Bogdan, Michael Gahler, Sunčana Glavak, Andrzej Halicki, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Miriam Lexmann, Antonio López-Istúriz White, Gabriel Mato, Vangelis Meimarakis, Francisco José Millán Mon, Radosław Sikorski, Isabel Wiseler-Lima, Željana Zovko, Milan Zver
Renew	Petras Auštrevičius, Katalin Cseh, Klemen Grošelj, Bernard Guetta, Ilhan Kyuchyuk, Nathalie Loiseau, Javier Nart, Urmas Paet, María Soraya Rodríguez Ramos, Hilde Vautmans
S&D	Maria Arena, Włodzimierz Cimoszewicz, Tanja Fajon, Raphaël Glucksmann, Dietmar Köster, Claudiu Manda, Sven Mikser, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Isabel Santos, Andreas Schieder, Sergei Stanishev
Verts/ALE	Alviina Alametsä, Reinhard Bütikofer, Jordi Solé, Tineke Strik, Viola Von Cramon-Taubadel, Thomas Waitz, Salima Yenbou

5	-
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Marisa Matias, Manu Pineda, Idoia Villanueva Ruiz

6	0
ECR	Charlie Weimers
ID	Maximilian Krah, Jaak Madison, Thierry Mariani, Jérôme Rivière, Harald Vilimsky

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

14.7.2021

OPINION OF THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION

for the Committee on Industry, Research and Energy

on the proposal for a 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 (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Rapporteur for opinion: Morten Løkkegaard

SHORT JUSTIFICATION

In general, the Rapporteur welcomes the legislative proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS 2). The Rapporteur believes that in an increasingly digitalised world, security online is key to guarantee a safe digital environment as well as the functioning of the single market, where consumers and economic operators can act freely.

The NIS 2 proposal is a significant improvement compared to the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS 1). It enumerates the key deficiencies by the NIS 1, such as the low level of cyber resilience of businesses and sectors, as well as the inconsistent resilience and low levels of joint situation awareness and crisis response in and between Member States. The Rapporteur welcomes the ambitions to correct this with the NIS 2.

Scope

The Rapporteur appreciates the extended scope of the NIS 2 proposal, in particular, the inclusion of new sectors such as the public administration. The explicit list of sectors and services included will surely reduce the discretion of Member States in defining the concrete entities subject to the Directive and will consequently reduce fragmentation in the single market.

Within the sectors and services covered, the Commission proposed the size-cap rule as a uniform criterion to determine the entities falling within the scope of application of the Directive. This criterion undoubtedly presents the advantage of ensuring legal certainty, while reducing divergences among Member States.

However, while welcoming the extended sector-based scope, the Rapporteur is of the opinion that this general criterion should be combined with an assessment of the criticality of entities within each sector. This would allow for medium and large entities which, following a risk

assessment, are considered to be of a low level of criticality and dependency on otherwise critical entities, to be left outside the scope of the Directive.

The Rapporteur stresses that this should not be considered an open door for discrepant interpretation between Member States. To ensure that this does not add to fragmented implementation between Member States, the Commission is encouraged to issue clear guidance on this.

Finally, while welcoming the exclusion of micro and small companies from the scope, the Rapporteur is of the view that there is a need to encourage their voluntary inclusion, as micro and small entities are also subject to, and affected by, cyberattacks.

Coordinated cybersecurity regulatory frameworks

The Rapporteur welcomes the chapter defining different elements of the national cybersecurity strategies and their crisis management tools. As part of their national cybersecurity strategy, it is proposed that Member States adopt a policy promoting the use of cryptography and encryption, especially by SMEs.

The Rapporteur welcomes the development of a European vulnerability registry by ENISA, however, believes that it is important that the registration respects business confidentiality and trade secrets and does not burden entities unnecessarily.

Cooperation among Member States

The more structured cooperation among Member States within the Cooperation Group, the CSIRTs network and the newly created group for large-scale incidents in the NIS 2 are particularly welcomed. However, there is a need to ensure that the level of confidence and willingness to exchange information among Member States is increased, as the effectiveness of this cooperation plays a key role in ensuring a high level of cybersecurity in the EU.

In light of this position, a number of amendments have been drafted to strengthen the role of the networks. In particular, the Rapporteur considers peer review a fruitful way to increase Member States´ shared confidence, and supports that they should play a crucial role in assessing the effectiveness of individual Member States´ cybersecurity policies.

Cybersecurity risk management

The extension of the risk assessment to the whole supply chain (Article 18 and Article 19) is appreciated, however, the Rapporteur stresses that the point needs clarifications to provide clear guidance to entities subject to this requirement and to Member States when carrying out a coordinated security risk evaluation of specifically critical sectors or supply chains.

Reporting obligations

The Rapporteur believes that more clarity should be provided on specific points of the reviewed Directive, mainly concerning some of the obligations imposed on companies in the scope of the NIS 2. The Rapporteur has sought to reduce the bureaucracy and make it easier for businesses to comply with the new rules having in mind the final objective of an effective implementation of the Directive.

The Rapporteur´s proposal is to extend the suggested deadline of 24 hours in the reporting obligations for the first notifications to 72 hours, to allow companies to effectively address the ongoing cybersecurity attack prior to notification. Furthermore, it is proposed to delete any reference to the mandatory notification of so-called 'potential incidents'.

AMENDMENTS

The Committee on the Internal Market and Consumer Protection calls on the Committee on Industry, Research and Energy, as the committee responsible, to take into account the following amendments:

Amendment 1
Proposal for a directive
Recital 5

Text proposed by the Commission	*Amendment*
(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards. This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.	(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards. This Directive aims to remove such wide divergences among Member States ***and strengthen the internal market***, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

Amendment 2
Proposal for a directive
Recital 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) The Directive is without prejudice to the rules laid down by Union law on the protection of personal data.

Amendment 3
Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission.	(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission. ***The Commission should provide clear guidance on the criteria establishing which small or micro entities would be essential or important, especially when providing services in several Member States.***

Amendment 4
Proposal for a directive
Recital 10

Text proposed by the Commission	*Amendment*
(10) The Commission, in cooperation with the Cooperation Group, ***may*** issue guidelines on the implementation of the criteria applicable to micro and small enterprises.	(10) The Commission, in cooperation with the Cooperation Group, ***should*** issue guidelines on the implementation of the criteria applicable to micro and small enterprises.

Amendment 5
Proposal for a directive
Recital 12 a (new)

Text proposed by the Commission	*Amendment*
	(12a) The extension of the scope of this Directive entails the inclusion of entities subject to sector-specific regulation. To avoid any regulatory duplication or burden, the Commission should ensure that sector-specific acts that require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, are consistent with this Directive.

Amendment 6
Proposal for a directive
Recital 12 b (new)

Text proposed by the Commission	*Amendment*
	(12b) The Commission should publish clear guidelines accompanying this Directive to help ensure harmonisation in implementation across Member States and avoid fragmentation.

Amendment 7
Proposal for a directive
Recital 12 c (new)

Text proposed by the Commission	*Amendment*
	(12c) The Commission should also issue guidelines to support Member States in correctly implementing the provisions on the scope, and to evaluate the proportionality of the obligations set out by this Directive in consideration of the criticality of entities falling in the scope, especially when applying to entities with complex business models or operating environments, whereby an entity may

simultaneously fulfil the criteria assigned to both essential and important entities, or may simultaneously conduct activities that are some within and some outside the scope of this Directive. In cases where entities have their main activity outside the scope of this Directive, but some other secondary activity inside the scope, the provisions should only apply to the function or unit level within an entity, which falls within the scope of this Directive.

Amendment 8
Proposal for a directive
Recital 14

Text proposed by the Commission	*Amendment*
(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under	(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their ***national*** cybersecurity strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and the one under Directive (EU) XXX/XXX in the context of ***incident reporting,*** information sharing on incidents***, near misses*** and cyber threats and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by critical entities. Upon request of competent authorities under Directive (EU)

this Directive should be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose.

XXX/XXX, competent authorities under this Directive should be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose.

[17] [insert the full title and OJ publication reference when known]

[17] [insert the full title and OJ publication reference when known]

Amendment 9
Proposal for a directive
Recital 15

Text proposed by the Commission

(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.

Amendment

(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy***, the internal market*** and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers***, and privacy or proxy registration service providers, domain brokers or resellers, and any other services that are related to the registration of domain names***.

Amendment 10
Proposal for a directive
Recital 20

Text proposed by the Commission

(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures

Amendment

(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures

across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.	across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks ***and the need to protect the internal market through joint strategies and actions at Union level***.

Amendment 11
Proposal for a directive
Recital 23

Text proposed by the Commission	*Amendment*
(23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in ***an*** effective and efficient way. The single points of contact should be tasked with forwarding incident notifications to the single points of contact of other affected Member States. ***At the level of Member States' authorities,*** to ensure one single entry point in every Member States, the single points of contacts should also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate, to the relevant	(23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in ***a standardised,*** effective and efficient way. The single points of contact should be tasked with forwarding incident notifications to the single points of contact of other affected Member States. To ensure one single entry point in every Member States, the single points of contacts should also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate, to the relevant national

national competent authorities or CSIRTs under this Directive.

competent authorities or CSIRTs under this Directive.

Amendment 12
Proposal for a directive
Recital 25

Text proposed by the Commission	*Amendment*
(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] as regards personal data, on behalf of and upon request by an entity under this Directive, a ***proactive*** scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.	(25) ***To identify, mitigate and prevent specific threats*** as regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] as regards personal data, on behalf of and upon request by an entity under this Directive, a scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.
[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).	[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

Amendment 13
Proposal for a directive
Recital 26 a (new)

Text proposed by the Commission	*Amendment*
	(26a) As a part of their national cybersecurity strategies, Member States should adopt policies on the promotion and integration of intelligent systems in

	the prevention and detection of cybersecurity incidents and threats. Member States should, in accordance with their national cybersecurity strategies, put in place policies directed at cybersecurity awareness and literacy, with a view of protecting consumers. When adopting national cybersecurity strategies, Member States should ensure policy frameworks to address lawful access to information.

Amendment 14
Proposal for a directive
Recital 27

Text proposed by the Commission	*Amendment*
(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20] , a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.	(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20], a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it***, thus endangering the internal market***. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.
[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).	[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

Amendment 15
Proposal for a directive
Recital 28

Text proposed by the Commission	*Amendment*
(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC 29417 provide guidance on vulnerability handling and vulnerability disclosure respectively. As regards vulnerability disclosure, coordination between reporting entities and manufacturers or providers of ICT products or services is particularly important. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also comprise coordination between the reporting entity and the organisation as regards the timing of remediation and publication of vulnerabilities.	(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm ***to businesses and consumers***, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC 29417 provide guidance on vulnerability handling and vulnerability disclosure respectively. As regards vulnerability disclosure, coordination between reporting entities and manufacturers or providers of ICT products or services is particularly important. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also comprise coordination between the reporting entity and the organisation as regards the timing of remediation and publication of vulnerabilities.

Amendment 16
Proposal for a directive
Recital 28 a (new)

Text proposed by the Commission	*Amendment*
	(28a) The Commission, ENISA and the Member States should continue to foster international alignment with standards and existing industry best practices in the area of risk management, for example in the areas of supply chain security assessments, information sharing and vulnerability disclosure.

Amendment 17
Proposal for a directive
Recital 30

Text proposed by the Commission	*Amendment*
(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. In that regard, sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability ***registry*** where, essential and important entities and their suppliers, as well as entities which do not fall in the scope of application of this Directive may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures.	(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. In that regard, sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability ***database*** where, essential and important entities and their suppliers, as well as entities which do not fall in the scope of application of this Directive may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures.

Amendment 18
Proposal for a directive
Recital 31

Text proposed by the Commission	*Amendment*
(31) Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A	(31) Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A

European vulnerability ***registry*** maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with ***similar*** registries in third country jurisdictions.	European vulnerability ***database*** maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with ***vulnerability databases or*** registries in third country jurisdictions ***and transmitting reports to appropriate registries provided that any such actions do not undermine the protection of confidentiality and trade secrets***.

Amendment 19
Proposal for a directive
Recital 32

Text proposed by the Commission	*Amendment*
(32) The Cooperation Group should establish a work programme every two years including the actions to be undertaken by the Group to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive should be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Group.	(32) The Cooperation Group should ***discuss political priorities and key challenges on cybersecurity and*** establish a work programme every two years including the actions to be undertaken by the Group to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive should be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Group.

Amendment 20
Proposal for a directive
Recital 32 a (new)

Text proposed by the Commission	*Amendment*
	(32a) The Cooperation Group should be composed of representatives of Member States, the Commission and ENISA.

Amendment 21
Proposal for a directive
Recital 34

Text proposed by the Commission	*Amendment*
(34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should consider inviting Union bodies and agencies involved in cybersecurity policy, such as the European Cybercrime Centre (EC3), the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.	(34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should consider inviting Union bodies and agencies involved in cybersecurity policy, such as the European Cybercrime Centre (EC3), the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work ***as well as other relevant Union bodies and agencies***.

Amendment 22
Proposal for a directive
Recital 35

Text proposed by the Commission	*Amendment*
(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes for officials from other Member States in order to improve cooperation. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the activities of the host competent authority.	(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes ***and joint training programmes*** for officials from other Member States in order to improve cooperation ***and strengthen trust among Member States***. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the activities of the host competent authority ***or CSIRT***.

Amendment 23
Proposal for a directive
Recital 39

Text proposed by the Commission	*Amendment*
(39) For the purposes of this Directive, the term 'near misses' should refer to an event which could potentially have caused harm, but was successfully prevented from fully transpiring.	***deleted***

Amendment 24
Proposal for a directive
Recital 45 a (new)

Text proposed by the Commission	*Amendment*
	(45a) Additionally, entities should also ensure adequate cybersecurity education and training of their staff at all levels of the organisation.

Amendment 25
Proposal for a directive
Recital 46

Text proposed by the Commission	*Amendment*
(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21] , with the aim of identifying ***per*** sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.	(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21], with the aim of identifying ***in each*** sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.

[21] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

[21] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

Amendment 26
Proposal for a directive
Recital 47

Text proposed by the Commission	*Amendment*
(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities.	(47) The supply chain risk assessments, in light of the features of the sector concerned ***and its criticality***, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities.

Amendment 27
Proposal for a directive
Recital 51

Text proposed by the Commission	*Amendment*
(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto.	(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet***, and consumers rely on it for essential parts of their daily lives***. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto.

Amendment 28
Proposal for a directive
Recital 52

Text proposed by the Commission	*Amendment*
(52) ***Where appropriate,*** entities should inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves***. The requirement to inform those recipients of such threats*** should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge.	(52) Entities should ***aim to*** inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves***, in particular when such measures may increase consumer protection. This*** should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge ***and drafted in a language easily comprehensible***.

Amendment 29
Proposal for a directive
Recital 53

Text proposed by the Commission	*Amendment*
(53) In particular, providers of public electronic communications networks or publicly available electronic communications services, should inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their communications, for instance by using specific types of software or encryption technologies.	(53) In particular, providers of public electronic communications networks or publicly available electronic communications services, should inform the service recipients of particular and significant cyber threats and of ***additional*** measures they can take to protect the security of their ***devices and*** communications, for instance by using specific types of software or encryption technologies.

Amendment 30
Proposal for a directive
Recital 54

Text proposed by the Commission	*Amendment*
(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of ***Article 18***. The use of end-to-end encryption ***should be reconciled with*** the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime.	(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of ***cybersecurity risk management measures***. The use of end-to-end encryption ***is without prejudice to*** the Member State' powers***, policies and procedures*** to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime. ***Any action taken has to strictly adhere to the principles of proportionality and subsidiarity.***

Amendment 31
Proposal for a directive
Recital 55

Text proposed by the Commission	*Amendment*
(55) This Directive lays down a ***two-stage*** approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within ***24*** hours, followed by a final report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines ***of 24 hours for the initial notification and one month for the final report***.	(55) This Directive lays down a ***consecutive*** approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident ***or a near miss***, they should be required to submit an initial notification within ***72*** hours, followed by a ***comprehensive report not later than three months after submitting the initial notification and a*** final report not later than one month after ***the incident has been mitigated***. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. ***The initial notification should be preceded by an early warning within the first 24 hours without any obligation of additional information disclosures. This early warning should be submitted as soon as possible, allowing entities to seek support from competent authorities or CSIRTs swiftly, and enabling competent authorities or CSIRTs to mitigate the potential spread of the reported incident,***

	as well as serving as a situational awareness tool for CSIRTs. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines ***foreseen***.

Amendment 32
Proposal for a directive
Recital 56

Text proposed by the Commission	*Amendment*
(56) Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies.	(56) Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents ***and upholding the once-only principle***, Member States should establish a single entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies.

Amendment 33
Proposal for a directive
Recital 59

Text proposed by the Commission	*Amendment*
(59) Maintaining accurate and complete databases of domain names and registration data (so called 'WHOIS data') and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.	(59) Maintaining accurate***, verified*** and complete databases of domain names and registration data (so called 'WHOIS data') and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.

Amendment 34
Proposal for a directive
Recital 61

Text proposed by the Commission	*Amendment*
(61) In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the entities providing domain name registration services ***for the TLD (so-called*** registrars) should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules.	(61) In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the entities providing domain name registration services ***(including services provided by domain name registries and*** registrars***, privacy or proxy registration service providers, domain brokers or resellers, and any other services which are related to the registration of domain names***) should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules.

Amendment 35
Proposal for a directive
Recital 68

Text proposed by the Commission	*Amendment*
(68) Entities should be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules.	(68) Entities should be encouraged ***and supported by Member States*** to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules.

Amendment 36
Proposal for a directive
Recital 69

Text proposed by the Commission	*Amendment*
(69) The processing of personal data, ***to the extent*** strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those	(69) The processing of personal data, ***which should be limited to what is*** strictly necessary and proportionate for the purposes of ensuring network and information security***, and of ensuring consumer protection,*** by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary

incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.

exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.

Amendment 37
Proposal for a directive
Recital 70

Text proposed by the Commission	*Amendment*
(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to ensuring a fair balance of obligations for both entities and competent authorities. Thus, essential entities should be subject to a fully-fledged supervisory regime (ex-ante and ex-post), while important entities should be subject to a light supervisory regime, ex-post only. For the latter, this means that important entities should not document systematically compliance with cybersecurity risk management requirements, while competent authorities should implement a reactive ex -post approach to supervision and, hence, not have a general obligation to supervise those entities.	(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance ***and to achieve a common high level of security throughout the digital sector including by preventing risks for users or other networks, information systems and services***, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to ensuring a fair balance of obligations for both entities and competent authorities. Thus, essential entities should be subject to a fully-fledged supervisory regime (ex-ante and ex-post), while important entities should be subject to a light supervisory regime, ex-post only***, taking into account a risk based approach***. For the latter, this means that important entities should not document systematically compliance with cybersecurity risk management requirements, while competent authorities should implement a reactive ex -post approach to supervision and, hence, not have a general obligation to supervise those entities***, except where there is a***

demonstrable breach of obligations.

Amendment 38
Proposal for a directive
Recital 76

Text proposed by the Commission	*Amendment*
(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning ***part or all the*** services provided by an essential entity ***and the imposition of a temporary ban from the exercise of managerial functions by a natural person***. Given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection, due process, presumption of innocence and right of defence.	(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning ***relevant*** services provided by an essential entity. Given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection, due process, presumption of innocence and right of defence.

Amendment 39
Proposal for a directive
Recital 79

Text proposed by the Commission	*Amendment*
(79) A peer-review mechanism should be introduced, allowing the assessment by experts designated by the Member States of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources.	(79) A peer-review mechanism should be introduced, allowing the assessment by experts designated by the Member States ***and of ENISA*** of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources***, and the exchange of best practices***.

Amendment 40
Proposal for a directive
Recital 80

Text proposed by the Commission	*Amendment*
(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should ***also*** be empowered to adopt delegated acts establishing ***which categories of*** essential entities ***shall*** be ***required to obtain a certificate and under which specific European cybersecurity certification schemes***. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[26] . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member	(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should be empowered to adopt delegated acts establishing ***the technical elements related to risk management measures. The Commission should also be empowered to adopt delegated acts by specifying the type of information submitted by*** essential ***and important*** entities ***of any incident having a significant impact on the provision of their services or of any near miss and by specifying the cases in which an incident should*** be ***considered to be significant***. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-

States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

[26] OJ L 123, 12.5.2016, p. 1.

institutional Agreement of 13 April 2016 on Better Law-Making[26]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

[26] OJ L 123, 12.5.2016, p. 1.

Amendment 41
Proposal for a directive
Recital 81

Text proposed by the Commission	*Amendment*
(81) In order to ensure uniform conditions for the implementation of the relevant provisions of this Directive concerning the procedural arrangements necessary for the functioning of the Cooperation Group***, the technical elements related to risk management measures or the type of information***, the format and the procedure of incident notifications, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.[27]	(81) In order to ensure uniform conditions for the implementation of the relevant provisions of this Directive concerning the procedural arrangements necessary for the functioning of the Cooperation Group, the format and the procedure of incident notifications, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.[27]

[27] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

[27] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

Amendment 42
Proposal for a directive
Article 1 – paragraph 1

Text proposed by the Commission	*Amendment*
1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union.	1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union***, in order to achieve a trusted digital environment for consumers and economic operators, and to improve and remove barriers to the functioning of the internal market***.

Amendment 43
Proposal for a directive
Article 2 – paragraph 2 – subparagraph 1 – introductory part

Text proposed by the Commission	*Amendment*
2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:	2. However, regardless of their size, this Directive also applies to entities ***of a type*** referred to in Annexes I and II, where:

Amendment 44
Proposal for a directive
Article 2 – paragraph 2 – subparagraph 2 a (new)

Text proposed by the Commission	*Amendment*
	The Commission shall issue guidelines in order to support Member States in correctly implementing the provisions on the scope as well as in order to grant possible derogations for specific important entities from the scope of the Directive or from some of its provisions, in consideration of their low level of criticality in their specific sector and/or their low level of dependency from other sectors or types of services. Member States, taking fully into account the Commission's guidelines, shall notify their motivated decisions in this regard to the Commission.

Amendment 45
Proposal for a directive
Article 4 – paragraph 1 – point 4

Text proposed by the Commission	*Amendment*
(4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the security of network and information systems in that Member State;	(4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the security of network and information systems in that Member State***, as well as policies needed to achieve them***;

Amendment 46
Proposal for a directive
Article 4 – paragraph 1 – point 5 a (new)

Text proposed by the Commission	*Amendment*
	(5a) 'cross-border incident' means any incident which impacts operators under the supervision of national competent authorities from at least two different Member States;

Amendment 47
Proposal for a directive
Article 4 – paragraph 1 – point 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) ´near miss´ means an event which could potentially have caused harm, but was successfully prevented from fully transpiring;

Amendment 48
Proposal for a directive
Article 4 – paragraph 1 – point 15 a (new)

Text proposed by the Commission	*Amendment*
	(15a) 'domain name registration

	services' means services provided by domain name registries and registrars, privacy or proxy registration service providers, domain brokers or resellers, and any other services which are related to the registration of domain names;

Amendment 49
Proposal for a directive
Article 5 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:	1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures***, including appropriate human and financial resources***, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:

Amendment 50
Proposal for a directive
Article 5 – paragraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of public bodies and entities as well as other relevant actors;	(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of public bodies and entities as well as other relevant actors***, including those responsible for cyber intelligence and cyber defence***;

Amendment 51
Proposal for a directive
Article 5 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) an assessment to identify relevant assets and cybersecurity risks in that	(c) an assessment to identify relevant assets and cybersecurity risks in that

Member State;	Member State***, including potential shortages that may negatively impact the Single Market***;

Amendment 52
Proposal for a directive
Article 5 – paragraph 1 – point e

Text proposed by the Commission	*Amendment*
(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;	(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy***, including a one-stop-shop for SMEs***;

Amendment 53
Proposal for a directive
Article 5 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement;	(b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement***, including the use of open source cybersecurity products***;

Amendment 54
Proposal for a directive
Article 5 – paragraph 2 – point c

Text proposed by the Commission	*Amendment*
(c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6;	(c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6 ***including by laying down guidelines and best practices based on already established internationally recognised standards on vulnerability handling and disclosure***;

Amendment 55
Proposal for a directive
Article 5 – paragraph 2 – point e

Text proposed by the Commission	*Amendment*
(e) a policy on promoting ***and developing*** cybersecurity skills***, awareness raising*** and research and development initiatives;	(e) a policy on promoting ***cybersecurity for consumers, raising their awareness about cyber threats, increasing cyber literacy, enhancing trust of users, technology neutral*** cybersecurity skills and ***education as well as promoting*** research and development initiatives ***and the cybersecurity of connected products***;

Amendment 56
Proposal for a directive
Article 5 – paragraph 2 – point e a (new)

Text proposed by the Commission	*Amendment*
	(ea) a policy on promoting the use of cryptography and encryption, in particular by SMEs;

Amendment 57
Proposal for a directive
Article 5 – paragraph 2 – point h

Text proposed by the Commission	*Amendment*
(h) a policy addressing specific needs of SMEs***, in particular*** those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats.	(h) a policy ***promoting cybersecurity and*** addressing ***the*** specific needs of SMEs ***in complying with obligations set by this Directive, as well as the specific needs of*** those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats ***including, for example funding and education to support the uptake of cybersecurity measures***.

Amendment 58
Proposal for a directive
Article 5 – paragraph 2 – point h a (new)

Text proposed by the Commission	*Amendment*
	(ha) this policy shall include the establishment of a national single point of contact for SMEs and a framework for the most efficient use of Digital Innovation Hubs and available funds in the achievement of policy objectives;

Amendment 59
Proposal for a directive
Article 5 – paragraph 2 – point h b (new)

Text proposed by the Commission	*Amendment*
	(hb) a policy promoting the coherent and synergic use of available funds;

Amendment 60
Proposal for a directive
Article 5 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon request, in the development of a national strategy and of key performance indicators for the assessment of the strategy.	4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon request, in the development of a national strategy and of key performance indicators for the assessment of the strategy. ***ENISA shall also address recommendations to Member States on the development of key performance indicators for the assessment of the national strategy, comparable at Union level.***

Amendment 61
Proposal for a directive
Article 6 – title

Text proposed by the Commission	*Amendment*
Coordinated vulnerability disclosure and a European vulnerability ***registry***	Coordinated vulnerability disclosure and a European vulnerability ***database***

Amendment 62
Proposal for a directive
Article 6 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ENISA shall develop and maintain a European vulnerability ***registry***. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties***. The registry*** shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.	2. ENISA shall develop and maintain a European vulnerability ***database***. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures ***as well as the appropriate disclosure policies*** with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and ***easily*** register vulnerabilities present in ICT products or ICT services, as well as to provide access to the ***relevant*** information on vulnerabilities contained in the registry to all interested parties***, provided that such actions do not undermine the protection of confidentiality and trade secrets. The vulnerability database*** shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated. ***To avoid duplication of efforts, ENISA shall enter into information sharing agreement and structured cooperation agreement with the Common Vulnerabilities and Exposures (CVE) registry, and, where relevant, with other databases globally developed and***

maintained by trusted partners.

Amendment 63
Proposal for a directive
Article 7 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. Where a Member State designates more than one competent authority referred to in paragraph 1, it shall clearly indicate which of these competent authorities will serve as the main point of contact during a large-scale incident or crisis.

Amendment 64
Proposal for a directive
Article 7 – paragraph 3 – point f

Text proposed by the Commission	*Amendment*
(f) national procedures and ***arrangements*** between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.	(f) national procedures and ***coordination*** between relevant national authorities and bodies***, including those responsible for cyber intelligence and cyber defence,*** to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.

Amendment 65
Proposal for a directive
Article 10 – paragraph 2 – point d

Text proposed by the Commission	*Amendment*
(d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;	(d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity***, including through the analysis of early warnings and notifications as referred to in Article 20***;

Amendment 66
Proposal for a directive
Article 10 – paragraph 2 – point e

Text proposed by the Commission	*Amendment*
(e) providing, upon request of an entity, a ***proactive*** scanning of the network and information systems used for the provision of their services;	(e) providing, upon request of an entity, a scanning of the network and information systems used for the provision of their services ***to identify, mitigate or prevent specific threats***;

Amendment 67
Proposal for a directive
Article 10 – paragraph 2 – point f

Text proposed by the Commission	*Amendment*
(f) participating in the CSIRTs network and providing mutual assistance to other members of the network upon their request**.**	(f) ***actively*** participating in the CSIRTs network and providing mutual assistance to other members of the network upon their request***;***

Amendment 68
Proposal for a directive
Article 10 – paragraph 2 – point f a (new)

Text proposed by the Commission	*Amendment*
	(fa) providing operational assistance and guidance to entities referred to in Annex I and II, and especially to SMEs;

Amendment 69
Proposal for a directive
Article 10 – paragraph 2 – point f b (new)

Text proposed by the Commission	*Amendment*
	(fb) participating in joint cybersecurity exercises at Union level.

Amendment 70
Proposal for a directive
Article 11 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that either their competent authorities or their CSIRTs receive notifications on incidents, and significant cyber threats and near misses submitted pursuant to this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to Article 20.	2. Member States shall ensure that either their competent authorities or their CSIRTs receive notifications on incidents, and significant cyber threats and near misses submitted pursuant to this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to ***effectively*** carry out their tasks, be granted ***adequate*** access to data on incidents notified by the essential or important entities, pursuant to Article 20.

Amendment 71
Proposal for a directive
Article 11 – paragraph 4

Text proposed by the Commission	*Amendment*
4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State.	4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State***, as well as with cyber defence and cyber intelligence authorities***.
[39] [insert the full title and OJ publication	[39] [insert the full title and OJ publication

reference when known]

reference when known]

Amendment 72
Proposal for a directive
Article 12 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.	2. The Cooperation Group shall ***meet regularly and*** carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.

Amendment 73
Proposal for a directive
Article 12 – paragraph 3 – subparagraph 2

Text proposed by the Commission	*Amendment*
Where appropriate, the Cooperation Group may invite representatives of relevant stakeholders to participate in its work.	Where appropriate, the Cooperation Group may invite representatives of relevant ***Union bodies and agencies as well as*** stakeholders to participate in its work.

Amendment 74
Proposal for a directive
Article 12 – paragraph 4 – point a

Text proposed by the Commission	*Amendment*
(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive;	(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive ***and promoting its uniform implementation in the Member States***;

Amendment 75
Proposal for a directive
Article 12 – paragraph 4 – point a a (new)

Text proposed by the Commission	*Amendment*
	(aa) exchanging information on political priorities and key challenges on

cybersecurity and defining the main objectives of the cybersecurity;

Amendment 76
Proposal for a directive
Article 12 – paragraph 4 – point a b (new)

Text proposed by the Commission	*Amendment*
	(ab) discussing national strategies of Member States and their preparedness;

Amendment 77
Proposal for a directive
Article 12 – paragraph 4 – point c

Text proposed by the Commission	*Amendment*
(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives;	(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives***, and with the European External Action Service on geopolitical aspects of the cybersecurity in the Union***;

Amendment 78
Proposal for a directive
Article 12 – paragraph 4 – point f

Text proposed by the Commission	*Amendment*
(f) discussing reports on the peer review referred to in Article 16(7);	(f) discussing reports on the peer review referred to in Article 16(7)***, assessing its functioning and drawing up conclusions and recommendations***;

Amendment 79
Proposal for a directive
Article 12 – paragraph 4 – point k a (new)

Text proposed by the Commission	*Amendment*
	(ka) supporting ENISA in organising joint training of national competent

authorities at Union level.

Amendment 80
Proposal for a directive
Article 12 – paragraph 6

Text proposed by the Commission	*Amendment*
6. By … [***24*** months after the date of entry into force of this Directive] and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148.	6. By … [***12*** months after the date of entry into force of this Directive] and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148.

Amendment 81
Proposal for a directive
Article 12 – paragraph 8 a (new)

Text proposed by the Commission	*Amendment*
	8a. The Cooperation Group shall regularly publish a summary report of its activities, without prejudice of the confidentiality of information shared during its meetings.

Amendment 82
Proposal for a directive
Article 13 – paragraph 3 – point a

Text proposed by the Commission	*Amendment*
(a) exchanging information on CSIRTs' capabilities;	(a) exchanging information on CSIRTs' capabilities ***and preparedness***;

Amendment 83
Proposal for a directive
Article 13 – paragraph 3 – point b

Text proposed by the Commission	*Amendment*
(b) exchanging relevant information on incidents, near misses, cyber threats, risks and vulnerabilities;	(b) exchanging relevant information on incidents, near misses, cyber threats, risks and vulnerabilities ***and supporting Member States operational capabilities***;

Amendment 84
Proposal for a directive
Article 13 – paragraph 3 – point d a (new)

Text proposed by the Commission	*Amendment*
	(da) exchanging and discussing information in relation to cross-border incidents;

Amendment 85
Proposal for a directive
Article 13 – paragraph 3 – point g – point i a (new)

Text proposed by the Commission	*Amendment*
	(i a) information sharing;

Amendment 86
Proposal for a directive
Article 13 – paragraph 3 – point j

Text proposed by the Commission	*Amendment*
(j) ***at the request of an individual CSIRT,*** discussing the capabilities and preparedness of ***that CSIRT***;	(j) discussing the capabilities and preparedness of ***CSIRTs***;

Amendment 87
Proposal for a directive
Article 13 – paragraph 4

Text proposed by the Commission	*Amendment*
4. For the purpose of the review referred to in Article 35 and by [24 months	4. For the purpose of the review referred to in Article 35 and by [24 months

after the date of entry into force of this Directive], and every ***two years*** thereafter, the CSIRTs network shall assess the progress made with the operational cooperation and produce a report. The report shall, in particular, draw conclusions on the outcomes of the peer reviews referred to in Article 16 carried out in relation to national CSIRTs, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.

after the date of entry into force of this Directive], and every ***year*** thereafter, the CSIRTs network shall assess the progress made with the operational cooperation and produce a report. The report shall, in particular, draw conclusions on the outcomes of the peer reviews referred to in Article 16 carried out in relation to national CSIRTs, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.

Amendment 88
Proposal for a directive
Article 14 – paragraph 3 – point a

Text proposed by the Commission	*Amendment*
(a) increasing the level of preparedness of the management of large scale incidents and crises;	(a) increasing the level of preparedness of the management of large scale incidents and crises***, including cross-border cyber threats***;

Amendment 89
Proposal for a directive
Article 14 – paragraph 5

Text proposed by the Commission	*Amendment*
5. EU-CyCLONe shall regularly report to the Cooperation Group on cyber threats, incidents and trends, focusing in particular on their impact on essential and important entities.	5. EU-CyCLONe shall regularly report to the Cooperation Group on cyber threats, incidents and trends, focusing in particular on their impact on essential and important entities ***and on their resilience***.

Amendment 90
Proposal for a directive
Article 14 – paragraph 6

Text proposed by the Commission	*Amendment*
6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements.	6. EU-CyCLONe shall ***closely*** cooperate with the CSIRTs network on the basis of agreed procedural arrangements.

Amendment 91
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 ***and present it to the European Parliament***. The report shall in particular include an assessment of the following:

Amendment 92
Proposal for a directive
Article 15 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) the development of cybersecurity capabilities across the Union;	(a) the development of cybersecurity capabilities across the Union***, including the general level of skills and competences in cybersecurity, the overall degree of resilience of the internal market towards cyber threats and the level of implementation of the Directive across the Member States***;

Amendment 93
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 cybersecurity capabilities ***including an overall assessment of cybersecurity for consumers;***

Amendment 94
Proposal for a directive
Article 15 – paragraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) the geopolitical aspects having a direct or indirect impact on the state of cybersecurity in the Union.

Amendment 95
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 ***12*** 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 ***at least two*** Member States ***and of ENISA*** different than the one reviewed and shall cover at least the following:

Amendment 96
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	2. The methodology shall include objective, non-discriminatory***, technology-neutral***, 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.	allocation of experts for each peer review.

Amendment 97
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 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. ***Those measures shall be appropriate and proportionate to the level of criticality of the sector or of the type of service, as well as the level of dependency of the entity from other sectors or types of services, and shall be adopted following a risk-based assessment.*** 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. ***In particular, measures shall be taken to prevent and minimise the impact of security incidents on recipients of their services.***

Amendment 98
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 services or managed security services;	(d) ***measures for*** supply chain security ***risk assessment*** including ***on*** security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;

Amendment 99
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 (testing and auditing) ***and regular cybersecurity exercises*** to assess the effectiveness of cybersecurity risk management measures;

Amendment 100
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***,*** encryption ***and in particular end-to-end-encryption;***

Amendment 101
Proposal for a directive
Article 18 – paragraph 2 – point g a (new)

Text proposed by the Commission	*Amendment*
	(ga) policies to ensure adequate cybersecurity training and awareness.

Amendment 102
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***, where they have access to the relevant information,*** 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.

Amendment 103
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 ***is empowered to*** adopt ***delegated*** acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2, and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications. ***In developing delegated acts, the Commission shall also consult all relevant stakeholders.***

Amendment 104
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***.	6. The Commission***, in cooperation with the Cooperation Group and ENISA, shall provide guidance and best practices on the compliance by entities, in a proportionate manner, in accordance with the requirements*** laid down in paragraph 2 ***and in particular with the requirement in point (d) of that paragraph***.

Amendment 105
Proposal for a directive
Article 19 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT	1. ***In view to increase the overall level of cybersecurity,*** the Cooperation Group, in cooperation with the Commission and ENISA, may carry out

services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.	coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors***, such as geopolitical risks***.

Amendment 106
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 ***or of any near miss***. 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 the near miss***.

Amendment 107
Proposal for a directive
Article 20 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. For the purpose of simplifying reporting obligations, Member States shall establish a single entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC.

Amendment 108
Proposal for a directive
Article 20 – paragraph 1 b (new)

Text proposed by the Commission	*Amendment*
	1b. 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 and decrease the compliance burden for companies.

Amendment 109
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***

Amendment 110
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***

Amendment 111
Proposal for a directive
Article 20 – paragraph 3 – point a

Text proposed by the Commission	*Amendment*
(a) the incident has caused ***or has the potential to cause*** substantial operational disruption or financial losses for the entity concerned;	(a) the incident has caused substantial operational disruption or financial losses for the entity concerned;

Amendment 112
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 other natural or legal persons by causing considerable material or non-material losses.

Amendment 113
Proposal for a directive
Article 20 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. The Commission is empowered to adopt delegated acts, in accordance with Article 36, to supplement this Directive by specifying the type of information submitted pursuant to paragraph 1 of this Article and by further specifying the cases in which an incident shall be considered to be significant as referred to in paragraph 3 of this Article.

Amendment 114
Proposal for a directive
Article 20 – paragraph 4 – 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 obligation on the entity concerned to disclose additional information regarding the incident;

Amendment 115
Proposal for a directive
Article 20 – paragraph 4 – 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;

Amendment 116
Proposal for a directive
Article 20 – paragraph 4 – 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 ***three months*** after the submission of the report under point (a), including at least the following:

Amendment 117
Proposal for a directive
Article 20 – paragraph 4 – point c – point i

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

Amendment 118
Proposal for a directive
Article 20 – paragraph 4 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) in case of a still ongoing incident at time of submission of the comprehensive report under letter (c), a final report shall be provided one month after the incident has been mitigated;

Amendment 119
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.

Amendment 120
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.

Amendment 121
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*** 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.

Amendment 122
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].

Amendment 123
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	11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to ***paragraph 1***. The Commission may also adopt implementing acts to

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).	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).

Amendment 124
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 ***and to increase the level of cybersecurity***, Member States, ***after having consulted the Cooperation Group and ENISA, shall encourage*** essential and important entities to certify certain ICT products, ICT services and ICT processes***, either developed by the essential or important entity or procured from third parties,*** under European cybersecurity schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 ***or under similar internationally recognised*** certification ***schemes. Whenever possible, Member States shall encourage the use of adopted certification schemes in a harmonised way***.

Amendment 125
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***	2. The Commission shall ***regularly assess the efficiency and use of the adopted European cybersecurity certification schemes under Article 49 of Regulation (EU) 2019/881 and shall identify*** which categories of essential entities shall be ***encouraged*** to obtain a certificate and under which specific

accordance with Article 36.	European cybersecurity certification schemes pursuant to paragraph 1.

Amendment 126
Proposal for a directive
Article 22 – paragraph -1 (new)

Text proposed by the Commission	*Amendment*
	-1. The Commission, in collaboration with ENISA, shall support and promote the development and implementation of standards set by relevant Union and international standardisation bodies for the convergent implementation of Article 18 (1) and (2). The Commission shall support the update of the standards in the light of technological developments.

Amendment 127
Proposal for a directive
Article 22 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to promote the convergent implementation of Article 18(1) and (2), Member States 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.	1. In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, ***and according to guidance from ENISA and the Cooperation Group,*** encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

Amendment 128
Proposal for a directive
Article 23 – title

Text proposed by the Commission	*Amendment*
Databases of domain names and registration data	Databases ***infrastructure*** of domain names and registration data

Amendment 129
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 the entities providing domain name registration services for the TLD***,*** shall collect***, verify*** and maintain accurate and complete domain name registration data ***necessary for the provisions of their services*** in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.

Amendment 130
Proposal for a directive
Article 23 – paragraph 2

Text proposed by the Commission	*Amendment*
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.	2. Member States shall ensure that the ***database infrastructure*** of domain name registration data referred to in paragraph 1 ***contains*** relevant information***, which shall include at least the registrants' name, their physical and email address as well as their telephone number, necessary*** to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs***, including at least the registrants' name, physical address, email address, and telephone number***.

Amendment 131
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 entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the ***database infrastructure includes*** accurate***, verified*** and complete information***, and that inaccurate or incomplete data shall be corrected or erased by the registrant without delay***. Member States shall ensure that such policies and procedures are made publicly available.

Amendment 132
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 entities providing domain name registration services ***make publicly available***, without undue delay ***and in any event within 24 hours*** after the registration of a domain name, ***all*** domain registration data ***of legal persons as registrants***.

Amendment 133
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	5. Member States shall ensure that TLD registries and entities providing domain name registration services ***are required to*** provide access to specific domain name registration data upon duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that TLD registries and entities providing

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.

domain name registration services reply without undue delay ***and in any event within 72 hours*** to all ***lawful and duly justified*** requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Amendment 134
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 highest number of employees in the Union. ***This shall be done in a manner that ensures that no disproportionate burden falls on national regulatory bodies.***

Amendment 135
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). ***For that purpose,*** the entities shall submit the following information to ENISA by [12 months after entering into force of the Directive at the latest]:

Amendment 136
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 ***and prevention*** techniques, mitigation strategies, or response and recovery stages.

Amendment 137
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 ***guidelines*** 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 ***guidelines*** shall also ***include*** the details of the involvement***, where relevant,*** of public authorities ***and independent experts*** 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).

Amendment 138
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 paragraph 2 by providing best practices and guidance***, as well as by facilitating information-sharing at Union level, while safeguarding business-sensitive information. At the request of essential and important entities, the Cooperation Group shall be invited to provide best practices and guidance.***

Amendment 139
Proposal for a directive
Article 27 – paragraph -1 (new)

Text proposed by the Commission	*Amendment*
	-1. Member States shall ensure that essential and important entities may submit notifications, on a voluntary basis, of cyber threats that those entities identify that could have potentially resulted in a significant incident. Member States shall ensure that, for the purpose of these notifications, entities shall act in accordance with the procedure laid down in Article 20. Voluntary notifications shall not result in the imposition of any additional obligations upon the reporting entity.

Amendment 140
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	***1.*** 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 ***shall*** prioritise the processing of mandatory notifications over voluntary notifications.

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.	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***, but the Member State may grant it assistance from CSIRTs***.

Amendment 141
Proposal for a directive
Article 28 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in Articles 18 and 20.	1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in Articles 18 and 20***, and are provided with the adequate means to perform their roles***.

Amendment 142
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**,** ***including data protection authorities from other Member States whenever relevant***.

Amendment 143
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 or risk-related available information***, carried out by a qualified independent body or a competent authority***;

Amendment 144
Proposal for a directive
Article 29 – paragraph 2 – point f

Text proposed by the Commission	*Amendment*
(f) requests to access data, documents or ***any*** information necessary for the performance of their supervisory tasks;	(f) requests to access ***relevant*** data, documents or information necessary for the performance of their supervisory tasks;

Amendment 145
Proposal for a directive
Article 29 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request ***and*** specify the information requested.	3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request***,*** specify the information requested ***and shall limit their requests to the scope of the incident or issue of concern***.

Amendment 146
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 ***relevant*** services or activities provided by an essential entity;

Amendment 147
Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) impose or request the imposition	***deleted***

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.

Amendment 148
Proposal for a directive
Article 30 – paragraph 1

Text proposed by the Commission	*Amendment*
1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through ex post supervisory measures.	1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary ***and taking into account a risk based approach***, through ex post supervisory measures.

Amendment 149
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 or risk-related available information***, carried out by a qualified independent body or a competent authority***;

Amendment 150
Proposal for a directive
Article 30 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Where exercising their powers	3. Where exercising their powers

pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request ***and*** specify the information requested.	pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request***,*** specify the information requested ***and shall limit their requests to the scope of the incident or issue of concern***.

Amendment 151
Proposal for a directive
Article 31 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of ***at least*** 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.	4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.

Amendment 152
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 and in any event*** within ***72 hours***.

Amendment 153
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 also*** inform the supervisory authority established in the same Member State.

Amendment 154
Proposal for a directive
Article 36 – paragraph 2

Text proposed by the Commission	*Amendment*
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 […]	2. The power to adopt delegated acts referred to in Articles ***18(5) and 20(3)*** shall be conferred on the Commission for a period of five years from […]

Amendment 155
Proposal for a directive
Article 36 – paragraph 3

Text proposed by the Commission	*Amendment*
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***.	3. ***A delegated act adopted pursuant to*** Articles ***18(5) and 20(3) shall enter into force only if no objection has been expressed either*** by the European Parliament or by the Council ***within a period of three 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 three months at the initiative*** of the European ***Parliament or of the Council***.

Amendment 156
Proposal for a directive
Article 36 – paragraph 6

Text proposed by the Commission	*Amendment*
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.	6. A delegated act adopted pursuant to Articles ***18(5) and 20(3)*** 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.

ANNEX: LIST OF ENTITIES OR PERSONS FROM WHOM THE RAPPORTEUR HAS RECEIVED INPUT

The following list is drawn up on a purely voluntary basis under the exclusive responsibility of the rapporteur. The rapporteur has received input from the following entities or persons in the preparation of the opinion, until the adoption thereof in committee:

Person	Entity
	BSA (The Software Alliance)
	BusinessEurope
	Confederation of Danish Industries
	Danish Permanent Representation
	Deutsche Telekom
	Digital Europe
	DOT Europe
	ETNO (European Telecommunications Network Operators)
	French Permanent Representation
	German Permanent Representation
	HUAWEI
	IFPI
	INTEL
	ITI (The Information Technology Industry Council)
	Kaspersky
	MÆRSK
	Microsoft
	ICANN
	MOTION PICTURE ASSOCIATION
	Orgalim
	Palo Alto Networks

	Rettighedsalliancen

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
References	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Committee responsible Date announced in plenary	ITRE 21.1.2021
Opinion by Date announced in plenary	IMCO 21.1.2021
Rapporteur for the opinion Date appointed	Morten Løkkegaard 9.2.2021
Discussed in committee	26.5.2021 21.6.2021
Date adopted	12.7.2021
Result of final vote	+: 42 –: 1 0: 2
Members present for the final vote	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Andrea Caroppo, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Carlo Fidanza, Evelyne Gebhardt, Alexandra Geese, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Antonius Manders, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Marco Zullo
Substitutes present for the final vote	Clara Aguilera, Maria da Graça Carvalho, Christian Doleschal, Claude Gruffat, Jiří Pospíšil, Kosma Złotowski

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

42	+
ECR	Adam Bielan, Carlo Fidanza, Kosma Złotowski
ID	Alessandra Basso, Hynek Blaško, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle
PPE	Pablo Arias Echeverría, Andrea Caroppo, Maria da Graça Carvalho, Deirdre Clune, Christian Doleschal, Andrey Kovatchev, Antonius Manders, Jiří Pospíšil, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Sandro Gozi, Morten Løkkegaard, Marco Zullo
S&D	Alex Agius Saliba, Clara Aguilera, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Claude Gruffat, Marcel Kolaja

1	-
NI	Miroslav Radačovský

2	0
ECR	Eugen Jurzyca
Renew	Svenja Hahn

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

14.7.2021

OPINION OF THE COMMITTEE ON TRANSPORT AND TOURISM

for the Committee on Industry, Research and Energy

on the proposal for a 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 (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Rapporteur for opinion: Jakop G. Dalunde

SHORT JUSTIFICATION

The transport sector is increasingly vulnerable to and affected by cybersecurity threats. Due to the sector's particular features, it is also subject to a range of distinct vulnerabilities. The amendments in this draft opinion, although general in nature, are therefore proposed with these particularities in mind. My proposals are relevant to transport for the following reasons:

- Transport is often an international enterprise in which many entities fall under the jurisdiction of several Member States. The sector is therefore strongly impacted by excessive disparity in the cybersecurity risk management and reporting obligations between Member States;

- The transport sector relies on the safe data exchange between various actors. Due to the interconnected nature of logistics, insufficient cybersecurity in one entity could endanger the entire system and lead to serious consequences for the operations of other entities;

- Transport is a labour-intensive sector and therefore especially sensitive to cybersecurity threats targeting employees;

For these reasons, the amendments focus on the following subjects: assessing the degree of divergence between Member states in terms of cybersecurity obligations, fostering the alignment of these obligations through non-legislative means, promoting staff training and knowledge of cyber security risks.

In addition to these general points, it is worth noting that the transport sector increasingly uses remote sensors capable of connecting to the internet in the provision of services, and that vehicles themselves are increasingly digitised. Although not necessarily part of the wider information systems, these devices may require specific security assessments.

AMENDMENTS

The Committee on Transport and Tourism calls on the Committee on Industry, Research and Energy, as the committee responsible, to take into account the following amendments:

Amendment 1

Proposal for a directive
Recital 3

Text proposed by the Commission	*Amendment*
(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence ***and cause*** major damage to the Union economy and society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market.	(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, ***contributing to the growth of new business models and services, such as those relating to the gig, on-demand and platform economy,*** including in cross-border exchanges ***and the Mobility as-a-Service approach (MaaS)***. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, cyber incidents can ***harm the wellbeing of society,*** impede the pursuit of economic activities in the internal market ***as well as of social activities,*** generate financial losses, undermine user ***and worker*** confidence***, causing*** major damage to the Union economy and society ***or even constitute a terrorist threat***. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to ***safeguard the fundamental rights and freedoms of the Union and*** the proper functioning of the internal market. ***Moreover, cybersecurity is a key enabler for many critical sectors, such as transport, to successfully embrace the digital transformation and to fully grasp***

the economic, social and sustainable benefits of digitalisation.

Amendment 2

Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission.	(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission. ***This exercise should be carried out with full understanding of the specificity of small and medium-sized enterprises (SMEs), and should not constitute an excessive administrative burden on SMEs.***

Amendment 3

Proposal for a directive
Recital 10

Text proposed by the Commission	*Amendment*
(10) The Commission, in cooperation with the Cooperation Group, may issue guidelines on the implementation of the criteria applicable to micro and small enterprises.	(10) The Commission, in cooperation with the Cooperation Group ***and relevant stakeholders***, may issue guidelines on the implementation of the criteria applicable to micro and small enterprises. ***The Commission should also ensure that appropriate guidance is given to all micro and small enterprises falling within the scope of this Directive. The Commission should, with the support of the Member States, provide microenterprises and small enterprises with informationin this regard. .***

Amendment 4

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission may issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.	(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. ***In order to avoid legal uncertainty in the interpretation and application of this Directive the Commission should ensure coherence between this Directive and the applicable sector-specific legislation. To that end, the Commission should identify duplication and redundancies in the relevant legislation, regulatory requirements or procedures, with a view to removing them.*** The Commission may issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

Amendment 5

Proposal for a directive
Recital 15 a (new)

Text proposed by the Commission	*Amendment*
	(15a) The increased digitalisation of key economic sectors, such as transport,

should be carried out in a secure way, with built-in resilience to ensure that the whole supply chain responds adequately to risks and threats. There is therefore a need for a coordinated approach ensuring a minimal level of security for connected devices, in particular in sectors such as transport and where it is included in vehicles and deploys end-to-end encryption by default.

Amendment 6

Proposal for a directive
Recital 17

Text proposed by the Commission	*Amendment*
(17) Given the emergence of innovative technologies ***and*** new business models, new cloud computing deployment and service models are expected to appear on the market in response to evolving customer needs. In that context, cloud computing services may be delivered in a highly distributed form, even closer to where data are being generated or collected, thus moving from the traditional model to a highly distributed one ('edge computing').	(17) Given the emergence of innovative technologies***, such as artificial intelligence,*** new business models ***and new models of flexible and remote work***, new cloud computing deployment and service models are expected to appear on the market in response to evolving customer ***and business*** needs. In that context, cloud computing services may be delivered in a highly distributed form, even closer to where data are being generated or collected, thus moving from the traditional model to a highly distributed one ('edge computing').

Amendment 7

Proposal for a directive
Recital 18 a (new)

Text proposed by the Commission	*Amendment*
	(18a) Given that the roll-out of autonomous mobility will bring considerable benefits, but will also entail a variety of new risks, namely with regard to road traffic safety, cybersecurity, intellectual property rights, issues relating to data protection and data access, technical infrastructure, standardisation,

	and employment, it is essential to ensure that the Union legal framework adequately responds to those challenges and effectively manages all risks posed to the security of network and information systems.

Amendment 8

Proposal for a directive
Recital 18 b (new)

Text proposed by the Commission	*Amendment*
	(18b) The coronavirus pandemic has demonstrated the importance of preparing the Union for the digital decade and the need to improve cyber-resilience on an ongoing basis. This Directive therefore aims to provide for minimum rules regarding the functioning of the coordinated regulatory framework to enable the digital transformation, innovation in autonomous transport, logistics and traffic management in all transport modes and to improve among users, in particular microenterprises, SMEs and start-ups, resilience against cyber-attacks and the capacity to address vulnerabilities.

Amendment 9

Proposal for a directive
Recital 19

Text proposed by the Commission	*Amendment*
(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council[18] , as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services. Transport services that are not undertaken in	(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council[18] , as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services. Transport ***or delivery*** services that are not undertaken in

conjunction with one of those steps should fall outside of the scope of postal services.

[18] Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998, p. 14).

conjunction with one of those steps should fall outside of the scope of postal services.

[18] Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998, p. 14).

Amendment 10

Proposal for a directive
Recital 27 a (new)

Text proposed by the Commission	*Amendment*
	(27a) Member States should, in their national cybersecurity strategies, address specific cybersecurity needs of SMEs, namely low cyber-awareness, a lack of remote IT security, a high cost of cybersecurity solutions and an increased level of threat. Member States should have a cybersecurity point of contact for SMEs to access relevant information, service and guidance.

Amendment 11

Proposal for a directive
Recital 33

Text proposed by the Commission	*Amendment*
(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of existing rules.	(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations***, particularly on facilitating alignment in the transposition of this Directive among Member States,*** to be addressed through better

	implementation of existing rules. ***The Cooperation Group should also map the national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across Europe. This is particularly relevant for the sectors that have an international and cross-border nature such as transport.***

Amendment 12

Proposal for a directive
Recital 34

Text proposed by the Commission	*Amendment*
(34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should consider inviting Union bodies and agencies involved in cybersecurity policy, such as the European Cybercrime Centre (EC3), the European Union Aviation Safety Agency (EASA) ***and*** the European Union Agency for Space Programme (EUSPA) to participate in its work.	(34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should consider inviting ***where relevant,*** Union bodies and agencies involved in cybersecurity policy, such as the European Cybercrime Centre (EC3), the European ***Cybersecurity Industrial, Technology, and Research Competence Centre, the European Union agencies responsible for safe transport - European*** Union Aviation Safety Agency (EASA)***, European Maritime Safety Agency (EMSA), European Union Agency for Railways (ERA) -*** the European Union Agency for Space Programme (EUSPA) ***and any other body and agency whose expertise is relevant to the discussions of the group*** to participate in its work.

Amendment 13

Proposal for a directive
Recital 37 a (new)

Text proposed by the Commission	*Amendment*
	(37a) Excessive disparity in the cybersecurity risk management and reporting obligations in Member States' transposition of this Directive could put the common level of cybersecurity within the Union at risk. ENISA should therefore, in cooperation with the Commission, evaluate the degree of divergence in cybersecurity risk management and reporting obligations among Member States in its biennial report on the state of cybersecurity in the Union.

Amendment 14

Proposal for a directive
Recital 46 a (new)

Text proposed by the Commission	*Amendment*
	(46a) In order to preserve and protect critical supply chains, the focus should also lay on the protection of the entire transport and logistics chain. The transport and logistics chain is made up of a large number of interlinked actors and systems, where goods are being transported in an intermodal fashion using air, road, rail, inland waterways and maritime transport. This process requires swift and reliable exchange of data between the various links of the transport and logistics chain through various interfaces. Due to the interconnected nature of the various links in the chain, insufficient cybersecurity risks to endanger the functioning of the entire chain through domino effects created by a cyber incident in one or several parts of the transport and logistics chain.

Amendment 15

Proposal for a directive
Recital 47

Text proposed by the Commission	*Amendment*
(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities.	(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events***; (iva) the extent to which specific critical ICT services, systems or products directly used by consumers are resilient and compliant with a customer-friendly approach;*** and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities.

Amendment 16

Proposal for a directive
Recital 55

Text proposed by the Commission	*Amendment*
(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps	(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps

mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within ***24*** hours, followed by a final report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of ***24*** hours for the initial notification and one month for the final report.	mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within ***36*** hours, followed by a final report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of ***36*** hours for the initial notification and one month for the final report.

Amendment 17

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

Text proposed by the Commission	*Amendment*
Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a	Member States***, in close cooperation with relevant industry stakeholders,*** shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the

regular basis, and at least every two years thereafter and, where appropriate, update it.	transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.

Amendment 18

Proposal for a directive
Article 2 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.	6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, ***including as to the power, mandate and functions of the respective supervisory authorities,*** the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.

Amendment 19

Proposal for a directive
Article 5 – paragraph 2 – point h

Text proposed by the Commission	*Amendment*
(h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats.	(h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance***, providing necessary and comprehensive information*** and support in improving their resilience to cybersecurity threats.

Amendment 20

Proposal for a directive
Article 12 – paragraph 4 – point a

Text proposed by the Commission	*Amendment*
(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive;	(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive***, so as to minimise disparities between cybersecurity risk management and reporting obligation standards among the Member States***;

Amendment 21

Proposal for a directive
Article 12 – paragraph 4 – point b a (new)

Text proposed by the Commission	*Amendment*
	(ba) mapping the national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across the Union;

Amendment 22

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

Text proposed by the Commission	*Amendment*
	(ca) the degree of disparity of cybersecurity risk management and reporting obligations between Member States, and the extent to which that disparity affects the common level of cybersecurity in the Union.

Amendment 23

Proposal for a directive
Article 16 – paragraph 1 – point iii a (new)

Text proposed by the Commission	*Amendment*
	(iiia) recommendations on how to improve coherence and legal certainty in the interpretation and application of this

	Directive and the applicable sector-specific legislation, with a focus on identifying and removing duplication and redundancies n the relevant legislation, regulatory requirements or procedures;

Amendment 24

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

Text proposed by the Commission	*Amendment*
	(ba) policies, programmes and procedures to ensure that employees have reasonable knowledge to apprehend cybersecurity risks and practical experience meeting high cybersecurity standards.

Amendment 25

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

Text proposed by the Commission	*Amendment*
(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	(e) security in network and information systems***, including mobile elements such as vehicles and remote sensors, their*** acquisition, development and maintenance, including vulnerability handling and disclosure;

Amendment 26

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***	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. ***The delegated acts*** shall ***be adopted*** in accordance with Article ***36*** and follow, to the greatest extent possible,

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

Amendment 27

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

Text proposed by the Commission	*Amendment*
	6a. In order to ensure an efficient policy and facilitate its implementation, the Commission shall consultt essential and important entities, in particular before adopting the delegated acts referred to in paragraphs 5 and 6.

Amendment 28

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 ***36*** 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;

Amendment 29

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

Text proposed by the Commission	*Amendment*
(iii) applied and ongoing mitigation measures.	(iii) applied and ongoing mitigation measures ***and results thereof***.

Amendment 30

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 may adopt ***delegated*** acts ***in accordance with Article 36*** further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2 ***of this Article***. 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).

Amendment 31

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***, either developed by the essential or important entity or procured from third parties,*** under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 ***or under similar internationally recognised*** certification ***schemes***.

Amendment 32

Proposal for a directive
Article 21 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. The requirements of this Directive regarding cybersecurity certification shall be without prejudice to Article 56(2) and

(3) of Regulation (EU) 2019/881.

Amendment 33

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***

Amendment 34

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. ***In order to elevate the overall level of cybersecurity resilience,*** the Commission may request ENISA to prepare a candidate scheme pursuant to ***Articles 47 and 48*** of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme is available. ***Such candidate schemes shall comply with the requirements laid down in Article 56(2) and Article 56(3) of Regulation (EU) 2019/881.***

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
References	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Committee responsible Date announced in plenary	ITRE 21.1.2021
Opinion by Date announced in plenary	TRAN 21.1.2021
Rapporteur for the opinion Date appointed	Jakop G. Dalunde 3.2.2021
Date adopted	12.7.2021
Result of final vote	+: 48 –: 0 0: 1
Members present for the final vote	Magdalena Adamowicz, Andris Ameriks, Izaskun Bilbao Barandica, Paolo Borchia, Marco Campomenosi, Massimo Casanova, Ciarán Cuffe, Jakop G. Dalunde, Johan Danielsson, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Giuseppe Ferrandino, Mario Furore, Søren Gade, Isabel García Muñoz, Elsi Katainen, Kateřina Konečná, Julie Lechanteux, Peter Lundgren, Benoît Lutgen, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Philippe Olivier, João Pimenta Lopes, Rovana Plumb, Dominique Riquet, Dorien Rookmaker, Massimiliano Salini, Sven Schulze, Vera Tax, Barbara Thaler, Henna Virkkunen, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Roberts Zīle, Kosma Złotowski
Substitutes present for the final vote	Clare Daly, Nicola Danti, Angel Dzhambazki, Tomasz Frankowski, Michael Gahler, Maria Grapini, Alessandra Moretti, Marianne Vind

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

48	+
ECR	Angel Dzhambazki, Peter Lundgren, Roberts Zīle, Kosma Złotowski
ID	Paolo Borchia, Marco Campomenosi, Massimo Casanova, Julie Lechanteux, Philippe Olivier
NI	Mario Furore, Dorien Rookmaker
PPE	Magdalena Adamowicz, Gheorghe Falcă, Tomasz Frankowski, Michael Gahler, Elżbieta Katarzyna Łukacijewska, Benoît Lutgen, Marian-Jean Marinescu, Cláudia Monteiro de Aguiar, Massimiliano Salini, Sven Schulze, Barbara Thaler, Henna Virkkunen, Elissavet Vozemberg-Vrionidi
Renew	Izaskun Bilbao Barandica, Nicola Danti, Søren Gade, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen, Dominique Riquet
S&D	Andris Ameriks, Johan Danielsson, Giuseppe Ferrandino, Isabel García Muñoz, Maria Grapini, Alessandra Moretti, Rovana Plumb, Vera Tax, Marianne Vind, Petar Vitanov
The Left	Clare Daly, Kateřina Konečná
Verts/ALE	Ciarán Cuffe, Jakop G. Dalunde, Karima Delli, Anna Deparnay-Grunenberg, Tilly Metz

0	-

1	0
The Left	João Pimenta Lopes

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

PROCEDURE – COMMITTEE RESPONSIBLE

Title	Measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148			
References	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)			
Date submitted to Parliament	16.12.2020			
Committee responsible Date announced in plenary	ITRE 21.1.2021			
Committees asked for opinions Date announced in plenary	AFET 21.1.2021	ECON 21.1.2021	IMCO 21.1.2021	TRAN 21.1.2021
	CULT 21.1.2021	LIBE 21.1.2021		
Not delivering opinions Date of decision	ECON 26.1.2021	CULT 11.1.2021		
Associated committees Date announced in plenary	LIBE 20.5.2021			
Rapporteurs Date appointed	Bart Groothuis 14.1.2021			
Discussed in committee	13.4.2021	26.5.2021		
Date adopted	28.10.2021			
Result of final vote	+: –: 0:	70 3 1		
Members present for the final vote	Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Michael Bloss, Manuel Bompard, Paolo Borchia, Marc Botenga, Markus Buchheit, Cristian-Silviu Buşoi, Carlo Calenda, Maria da Graça Carvalho, Ignazio Corrao, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Pilar del Castillo Vera, Christian Ehler, Valter Flego, Niels Fuglsang, Lina Gálvez Muñoz, Claudia Gamon, Bart Groothuis, Christophe Grudler, András Gyürk, Henrike Hahn, Robert Hajšel, Ivo Hristov, Ivars Ijabs, Romana Jerković, Eva Kaili, Seán Kelly, Izabela-Helena Kloc, Łukasz Kohut, Zdzisław Krasnodębski, Andrius Kubilius, Miapetra Kumpula-Natri, Thierry Mariani, Marisa Matias, Eva Maydell, Georg Mayer, Joëlle Mélin, Dan Nica, Angelika Niebler, Ville Niinistö, Aldo Patriciello, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Clara Ponsatí Obiols, Manuela Ripa, Robert Roos, Sara Skyttedal, Maria Spyraki, Jessica Stegrud, Beata Szydło, Riho Terras, Grzegorz Tobiszowski, Isabella Tovaglieri, Viktor Uspaskich, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho			
Substitutes present for the final vote	Rasmus Andresen, Marek Paweł Balt, Klemen Grošelj, Adam Jarubas, Elena Lizzi, Adriana Maldonado López, Bronis Ropė, Jordi Solé, Nils Torvalds			
Date tabled	4.11.2021			

FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

70	+
ECR	Izabela-Helena Kloc, Zdzisław Krasnodębski, Robert Roos, Beata Szydło, Grzegorz Tobiszowski
ID	Paolo Borchia, Markus Buchheit, Elena Lizzi, Thierry Mariani, Georg Mayer, Joëlle Mélin, Isabella Tovaglieri
NI	András Gyürk, Clara Ponsatí Obiols, Viktor Uspaskich
PPE	François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Cristian-Silviu Buşoi, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Adam Jarubas, Seán Kelly, Andrius Kubilius, Eva Maydell, Angelika Niebler, Aldo Patriciello, Markus Pieper, Sara Skyttedal, Maria Spyraki, Riho Terras, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Valter Flego, Claudia Gamon, Bart Groothuis, Klemen Grošelj, Christophe Grudler, Ivars Ijabs, Mauri Pekkarinen, Morten Petersen, Nils Torvalds
S&D	Marek Paweł Balt, Carlo Calenda, Josianne Cutajar, Niels Fuglsang, Lina Gálvez Muñoz, Robert Hajšel, Ivo Hristov, Romana Jerković, Eva Kaili, Łukasz Kohut, Miapetra Kumpula-Natri, Adriana Maldonado López, Dan Nica, Tsvetelina Penkova, Carlos Zorrinho
Verts/ALE	Rasmus Andresen, Michael Bloss, Ignazio Corrao, Ciarán Cuffe, Henrike Hahn, Ville Niinistö, Manuela Ripa, Bronis Ropė, Jordi Solé

3	-
The Left	Manuel Bompard, Marc Botenga, Marisa Matias

1	0
ECR	Jessica Stegrud

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