European Parliament
2019-2024

Committee on Civil Liberties, Justice and Home Affairs

2020/0359(COD)

2.7.2021

AMENDMENTS
85 - 247

Draft opinion

(PE693.822v01-00)

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

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

AM_Com_LegOpinion

Amendment 85
Peter Kofod

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,*** 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).

Or. en

Amendment 86
Maria Grapini

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	(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.

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. ***The expansion of online activities in the context of the COVID-19 pandemic has highlighted the importance not only of cybersecurity issues, but also of providing relevant education and training on a large scale, practically to the entire population of the planet.***

[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.

Or. ro

Amendment 87
Maria Grapini

Proposal for a directive
Recital 3

Text proposed by the Commission

(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

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.	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. ***Malicious cyber activities threaten not only our economies, but also the functioning of our democracies, our freedom and our values. Our future security depends on transforming our capacity to protect the EU against cybersecurity threats both within the civilian infrastructure, as well as the military capacity.***
	Or. ro

Amendment 88
Maria Grapini

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	(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. ***Cybersecurity must form the basis for the digital transformation of daily activities within the entire European Union and must consolidate cooperation between the***

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.

EU bodies and the authorities of the Member States that are responsible for preventing and discouraging cyber attacks. 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.

Or. ro

Amendment 89
Peter Kofod

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	(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***, but also threaten the overall security of 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

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.

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.

Or. en

Amendment 90
Peter Kofod

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 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).

Or. en

Amendment 91
Patryk Jaki

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. Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion. ***Nevertheless, taking into account the difference in composition of public administration in the Member States, the identification process provided in Directive (EU) 2016/1148 remains an appropriate mechanism to determine which public administration entities should fall under the scope of this Directive.***
[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).	[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).

Or. en

Amendment 92
Patryk Jaki

Proposal for a directive
Recital 8 a (new)

Text proposed by the Commission	*Amendment*
	(8a) Taking into consideration the differences in the national public administration frameworks, Member States retain full decision-making autonomy regarding the question of whether to identify public administration entities and if Member States decided to do so which entities are to be identified. It would also be possible to foresee in the national legislation that particular categories of public administration entities are identified as falling under the scope of this Directive. Member States should also be able to structure the obligations for public administration entities regarding security requirements, incident notification, supervision and sanctions.

Or. en

Amendment 93
Patryk Jaki

Proposal for a directive
Recital 11

Text proposed by the Commission	*Amendment*
(11) Depending on the sector in which they operate or the type of service they provide, the entities falling within the scope of this Directive should be classified into ***two*** categories: essential ***and*** important. That categorisation should take	(11) Depending on the sector in which they operate or the type of service they provide, the entities falling within the scope of this Directive should be classified into ***three*** categories: essential***,*** important***, and public administration***. That

into account the level of criticality of the sector or of the type of service, as well as the level of dependency of other sectors or types of services. ***Both*** essential and important entities should be subject to the same risk management requirements and reporting obligations. The supervisory and penalty regimes between ***these two categories of*** entities should be differentiated to ensure a fair balance between requirements and obligations on one hand, and the administrative burden stemming from the supervision of compliance on the other hand.

categorisation should take into account the level of criticality of the sector or of the type of service, as well as the level of dependency of other sectors or types of services. Essential and important ***entities and public administration*** entities should be subject to the same risk management requirements and reporting obligations. ***Member States should have right to exclude obligations for public administration entities.*** The supervisory and penalty regimes between ***essential and important*** entities should be differentiated to ensure a fair balance between requirements and obligations on one hand, and the administrative burden stemming from the supervision of compliance on the other hand. ***The supervisory and penalty regimes for public administration entities should be foreseen in line with the national legislation and legal system.***

Or. en

Amendment 94
Patrick Breyer
on behalf of the Greens/EFA Group

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.

Or. en

Amendment 95
Maria Grapini

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, 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. ***Cybersecurity must be one of the EU priorities in responding to the COVID-19 pandemic, during which cyber attacks have intensified, which will have to lead to further investment in this field.***

Or. ro

Amendment 96

Patryk Jaki

Proposal for a directive
Recital 20 a (new)

Text proposed by the Commission	*Amendment*
	(20a) It is crucial to raise the cyber awareness and resilience in public administration entities. At the same time it is also essential to take into account the specificities of the composition of national public administrations. Therefore Member States should be given a flexibility to decide if and which public administration entities should be covered by this Directive and should have right to exclude select obligations for these entities. Identification of public administration entities should be at the individual Member State's sole discretion.

Or. en

Amendment 97
Maria Grapini

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 make sure that this authority has adequate resources to fulfil its duties in an efficient and effective way***.

Or. ro

Amendment 98
Patryk Jaki

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 ***and public administration entities*** under this Directive. Member States should be able to assign this role to an existing authority.

Or. en

Amendment 99
Patrick Breyer
on behalf of the Greens/EFA Group

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	(25) 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.

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).

Or. en

Amendment 100
Maria Grapini

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, 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. ***Also, cybersecurity risks should never be used as a pretext for breaching human rights.***
_____	_____
[19] Regulation (EU) 2016/679 of the	[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).

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).

Or. ro

Amendment 101
Maria Grapini

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. 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. ***Cybersecurity is indispensable for network and global internet connectivity, therefore improving cybersecurity is essential for EU citizens to be able to trust innovation and connectivity, given the expansion of online activities in the context of the COVID-19 pandemic.***

[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).

Or. ro

Amendment 102
Maria Grapini

Proposal for a directive
Recital 29

Text proposed by the Commission	*Amendment*
(29) Member States should therefore take measures to facilitate coordinated 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.	(29) Member States should therefore take measures to facilitate coordinated 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. ***Member States should jointly 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.

Or. ro

Amendment 103
Maria Grapini

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 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. ***Member States should 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.***

Or. ro

Amendment 104
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner

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. ***When personal data is transferred to a third country or international organisation, Chapter V of Regulation (EU) 2016/679 shall apply***.

Or. en

Amendment 105
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner

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	(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.

(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, or may be, 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.

Or. en

Amendment 106
Patryk Jaki

Proposal for a directive
Recital 42

Text proposed by the Commission	*Amendment*
(42) Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those are primarily private network and information systems managed by their internal IT staff or the security of which has been outsourced. The cybersecurity risk management and reporting requirements pursuant to this Directive should apply to the relevant essential and important entities regardless of whether they perform the maintenance of their network and information systems internally or outsource it.	(42) Essential and important ***entities and public administration*** entities should ensure the security of the network and information systems which they use in their activities. Those are primarily private network and information systems managed by their internal IT staff or the security of which has been outsourced. The cybersecurity risk management and reporting requirements pursuant to this Directive should apply to the relevant essential and important entities ***and public administration entities*** regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

Or. en

Amendment 107

Maria Grapini

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***.

Or. ro

Amendment 108
Pernando Barrena Arza

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	(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.

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

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. ***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.***

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

Or. en

Amendment 109
Patryk Jaki

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	(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive ***and public administration entities*** 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

vulnerabilities.

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).

Or. en

Amendment 110
Pernando Barrena Arza

Proposal for a directive
Recital 46 a (new)

Text proposed by the Commission	*Amendment*
	(46a) 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.

Or. en

Amendment 111
Patryk Jaki

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	(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.	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 ***and public administration 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.

Or. en

Amendment 112
Patryk Jaki

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.

Or. en

Justification

SMEs will usually be excluded from the scope of this Directive. However, they are relevant

actors when it comes to increasing cybersecurity levels of societies and economies. The national strategies should therefore pay attention to their specific needs and vulnerabilities.

Amendment 113
Patryk Jaki

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 ***and public administration entities*** are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important ***entities and public administration*** 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.

Or. en

Amendment 114
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 51 a (new)

Text proposed by the Commission	*Amendment*
	(51a) In order to offer the necessary transparency to mitigate specific supply chain risks, open source cybersecurity products (software and hardware), including open source encryption, should be favoured, in line with Opinion 5/2021

of the European Data Protection Supervisor [15a]

[15a] ***Opinion 5/2021 of the European Data Protection Supervisor on the Cybersecurity Strategy and the NIS 2.0 Directive, 11 March 2021***

Or. en

Amendment 115
Patrick Breyer
on behalf of the Greens/EFA Group

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*** 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. ***In order to increase the security of hardware and software, providers should be encouraged to use open source and open hardware.***

Or. en

Amendment 116
Pernando Barrena Arza

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 Article 18. ***No provision in this Directive should be construed as an endorsement of or obligation to weakening*** end-to-end encryption***, whether through "backdoors" or other*** solutions.

Or. en

Amendment 117
Sophia in 't Veld, Moritz Körner

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***	(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption***, which is a critical and irreplaceable technology for effective data protection and privacy***, 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

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***.

Article 18. ***Nothing in this Regulation should be viewed as an effort to weaken*** end-to-end encryption ***through "backdoors" or similar*** solutions.

Or. en

Amendment 118
Patrick Breyer
on behalf of the Greens/EFA Group

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***	(54) ***Being essential*** to safeguard the security of electronic communications networks and services ***as well as the fundamental right to privacy***, the use of encryption, and in particular end-to-end encryption, should be promoted and 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. ***Any interferences with the confidentiality of private communications should not lead to creating backdoors or weakening*** encryption ***while ensuring that the privacy and*** security ***of encrypted data, including*** in end-to-end encrypted communications***, is not compromised***.

effective response to crime.

Or. en

Justification

Member States must neither legally mandate nor otherwise incentivise the weakening of encryption for any reason, as this would inevitably undermine network and information security for all users and institutions.

Amendment 119
Maria Grapini

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 within end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and the security of communications, ***whilst 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 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 within end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and the security of communications, ***and this should not be undermined under any circumstances, as any encryption shortfall is open for exploration or exploitation by actors, regardless of their legitimacy or intention***.

Or. ro

Amendment 120
Maria Grapini

Proposal for a directive
Recital 54 a (new)

Text proposed by the Commission	*Amendment*
	(54a) any measure aimed at weakening encryption or circumventing the technology's architecture may incur significant risks to the effective protection capabilities it entails, thus inevitably compromising the protection of personal data and privacy, resulting in an overall loss of trust in security controls. Any unauthorised decryption, reverse engineering of encryption codes or monitoring of electronic communications other than by legal authorities should be prohibited to ensure the effectiveness of the technology and its wider use. The cases in which encryption can be used to mitigate the risks related to non-compliant data transfers, as presented in EDPB Recommendations 01/2020, may enable a stronger encryption, whether in transit or at rest, for the providers of such services and networks for the purposes of Article 18.

Or. ro

Amendment 121
Maria Grapini

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 ***a maximum of*** 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 ***a maximum of*** 24 hours for the initial notification and one month for the final report.
	Or. ro

Amendment 122
Patryk Jaki

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 and public administration*** 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.

Or. en

Amendment 123
Patryk Jaki

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 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	(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 and public administration*** 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

that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the EC3 and ENISA.	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.

Or. en

Amendment 124
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Olivier Chastel, Moritz Körner

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 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.	(57) Where it is suspected that an incident is related to serious criminal activities under Union or national law, essential and important entities, on the basis of applicable criminal proceedings rules in 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 EC3 and ENISA.

Or. en

Amendment 125
Patrick Breyer
on behalf of the Greens/EFA Group

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.	***deleted***

Or. en

Amendment 126
Patrick Breyer
on behalf of the Greens/EFA Group

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.	***deleted***

Or. en

Amendment 127

Patrick Breyer
on behalf of the Greens/EFA Group

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***

Or. en

Amendment 128
Patrick Breyer
on behalf of the Greens/EFA Group

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	***deleted***

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.

---

[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".

Or. en

Amendment 129
Patryk Jaki

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. 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. ***Public administration entities shall fall under the jurisdiction of the Member State in which they were identified pursuant to Article 2a.***

Or. en

Amendment 130
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 65

Text proposed by the Commission	*Amendment*
(65) In cases where a ***DNS service provider,*** TLD name registry, content delivery network provider, cloud computing service provider, data centre service provider and digital provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such an entity is offering services within the Union, it should be ascertained whether it is apparent that the entity is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the entity's or an intermediary's website or of an email address and of other contact details, or the	(65) In cases where a TLD name registry, content delivery network provider, cloud computing service provider, data centre service provider and digital provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such an entity is offering services within the Union, it should be ascertained whether it is apparent that the entity is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the entity's or an intermediary's website or of an email address and of other contact details, or the use of a language generally used in the

use of a language generally used in the third country where the entity is established, is as such insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the entity is planning to offer services within the Union. The representative should act on behalf of the entity and it should be possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a written mandate of the entity to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting.

third country where the entity is established, is as such insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the entity is planning to offer services within the Union. The representative should act on behalf of the entity and it should be possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a written mandate of the entity to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting.

Or. en

Amendment 131
Patrick Breyer
on behalf of the Greens/EFA Group

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	***deleted***

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.

Or. en

Amendment 132
Maria Grapini

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	(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. ***In many cases, personal data are***

processing of the following types of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.

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 the following types of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.

Or. ro

Amendment 133
Patryk Jaki

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	(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. ***When it comes to***

supervise those entities.

public administration entities the supervisory powers should be executed in line with the national frameworks and it should be up to Member States discretion to impose suitable measures of supervision and enforcement.

Or. en

Amendment 134
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner

Proposal for a directive
Recital 78 a (new)

Text proposed by the Commission	*Amendment*
	(78a) The European Commission should support Member States to design educational programmes on cybersecurity, to enable members of the management body of entities falling within the scope of this Directive to receive or recruit cybersecurity specialists and technicians in order to comply with the obligations arising from this Directive.

Or. en

Amendment 135
Maria Grapini

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 must ensure a coordinated***

response to large-scale cyber incidents and crises and, also, must offer assistance in order to facilitate recovery following such cyber attacks.

Or. ro

Amendment 136
Pernando Barrena Arza

Proposal for a directive
Recital 82 a (new)

Text proposed by the Commission	*Amendment*
	(82a) This Directive does not apply to Union bodies, however, Union bodies could be considered essential or important entities under this Directive. By [6 months after entry into force], the Commission should evaluate the need to apply the provisions of this Directive to Union bodies and present, where appropriate, legislative proposals to this effect.

Or. en

Amendment 137
Patryk Jaki

Proposal for a directive
Article 1 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) lays down cybersecurity risk management and reporting obligations for entities of a type referred to as essential entities in Annex I ***and*** important entities in Annex II;	(b) lays down cybersecurity risk management and reporting obligations for entities of a type referred to as essential entities in Annex I**,** important entities in Annex II ***and public administration entities***;

Or. en

Amendment 138
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner

Proposal for a directive
Article 1 a (new)

Text proposed by the Commission	*Amendment*
	Article 1 a
	Protection and processing of personal data
	1. Any processing of personal data in the Member States pursuant to this Directive shall be carried out in accordance with Regulation (EU) 2016/679and Directive 2002/58/EC.2. Any processing of personal data by the Commission and ENISA pursuant to this Directive shall be carried out in accordance with Regulation (EC) No 2018/1725.

Or. en

Amendment 139
Patrick Breyer
on behalf of the Greens/EFA Group

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] ***nor to non-commercial free and open source projects. 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).

Or. en

Amendment 140
Pernando Barrena Arza

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 enterprises within the meaning of Commission Recommendation 2003/361/EC.[28]
[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).

Or. en

Amendment 141
Patryk Jaki

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

Text proposed by the Commission	*Amendment*
	1 a. This Directive also applies to public administration entities identified by

the Member States in accordance with art. 2a, notwithstanding para 1b.

Or. en

Amendment 142
Patryk Jaki

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

Text proposed by the Commission	*Amendment*
	1b. This directive does not apply to public administration entities that carry out activities in the areas of public security, defence or national security.

Or. en

Amendment 143
Patrick Breyer
on behalf of the Greens/EFA Group

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

Text proposed by the Commission	*Amendment*
(iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;	***deleted***

Or. en

Justification

A catch all, sectorial approach is not compatible with the scope of this directive.

Amendment 144
Patryk Jaki

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

Text proposed by the Commission	*Amendment*
(b) the entity is a public administration entity as defined in point 23 of Article 4;	***deleted***

Or. en

Amendment 145
Pernando Barrena Arza

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 in a Member State ***or region***;

Or. en

Amendment 146
Patrick Breyer
on behalf of the Greens/EFA Group

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;

Or. en

Justification

The text provides assessment criteria, therefore the rule will apply when a disruption could have an impact. The change eliminates a double conditionality.

Amendment 147
Patrick Breyer
on behalf of the Greens/EFA Group

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;

Or. en

Justification

The text provides assessment criteria, therefore the rule will apply when a disruption could have an impact. The change eliminates a double conditionality.

Amendment 148
Patryk Jaki

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

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.	Member States shall establish a list of entities identified pursuant to points (b) to ***(e)*** 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.

Or. en

Amendment 149
Pernando Barrena Arza

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 Directive 2013/40/EU[32] 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).	
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).

Or. en

Amendment 150
Pernando Barrena Arza

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

Text proposed by the Commission	*Amendment*
	4 a. This Directive applies without prejudice to Union legislation for the protection of personal data, in particular Regulation (EU) 2016/679, Directive(EU)

2016/680 and Directive 2002/58/EC. Where the application of this Directive requires the processing of personal data, this shall take place in accordance with those instruments.

Or. en

Amendment 151
Patryk Jaki

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 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 ***or public administration entities***.

Or. en

Amendment 152
Pernando Barrena Arza

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	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.	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 interests of essential or important entities.

Or. en

Amendment 153
Maria Grapini

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

Text proposed by the Commission	*Amendment*
	5a. As regards the processing of personal data, essential and important entities, as well as competent authorities, CERTs, and CSIRTs, shall process personal data to an extent that is strictly necessary and proportionate for the purposes of ensuring network and information security, in accordance with the obligations set out in this Directive. Where the processing of personal data is required for the purpose of cybersecurity and network and information security in accordance with the provisions set out in Article 18 and Article 20 of the Directive, including the provisions set out in Article 23, this processing shall be considered necessary in order to ensure compliance with a legal obligation in accordance with paragraph 1(c) of Article 6 of Regulation (EU) 2016/679.

Or. ro

Justification

Clarifying the legal basis, under Regulation (EU) 2016/679, for the processing of personal data where there is an obligation to comply with the requirements of the provisions laid out in this Directive.

Amendment 154
Maria Grapini

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

Text proposed by the Commission	*Amendment*
	5b. As regards the processing of personal data from essential entities providing services of public electronic communication networks or publicly available electronic communications referred to in point 8 of Annex I and point (a)(i) of paragraph (1), such processing of personal data required for the purposes of ensuring network and information security must be in compliance with the provisions set out in Directive 2002/58/EC.

Or. ro

Justification

Clarifying the legal basis, under Directive 2002/58/EC (e-Privacy Directive), for the processing of personal data from entities providing services of public communication networks or publicly available electronic communications, which are in scope of this Directive.

Amendment 155
Sophia in 't Veld, Maite Pagazaurtundúa, Moritz Körner, Fabienne Keller

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.

Or. en

Justification

EDPS opinion

Amendment 156
Patrick Breyer
on behalf of the Greens/EFA Group

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

Text proposed by the Commission	*Amendment*
	6 a. This Directive is to be applied in full compliance with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and is not modifying or adding to its provisions.

Or. en

Amendment 157
Patryk Jaki

Proposal for a directive
Article 2 a (new)

Text proposed by the Commission	*Amendment*
	Article 2 a
	Identification of Public Administration Entities
	1. By [date] Member States may identify public administration entities established

on their territory.

2. The criteria for the progressive identification of public administration entities shall be as follows:

(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities, or by other bodies governed by public law;

(c) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.

3. The public administration entities identified in line with this Article shall be reviewed and where appropriate updated by Member States when necessary.

4. Member States shall inform the Commission about the result of the process of identification of public administration entities in accordance with this Article.

Or. en

Amendment 158
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 4 – paragraph 1 – point 9

Text proposed by the Commission	*Amendment*

(9) ‘representative’ means any natural or legal person established in the Union explicitly designated to act on behalf of i) ***a DNS service provider, a top-level domain (TLD) name registry,*** a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;	(9) ‘representative’ means any natural or legal person established in the Union explicitly designated to act on behalf of i) a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;

Or. en

Amendment 159
Pernando Barrena Arza

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***

Or. en

Amendment 160
Patrick Breyer
on behalf of the Greens/EFA Group

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 DNS service providers;	***deleted***

Or. en

Amendment 161
Patrick Breyer
on behalf of the Greens/EFA Group

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;	***deleted***

Or. en

Justification

Aligning the text with the changes to the scope. The fact that there was a need to define this term shows the need for a sector specific legislation.

Amendment 162
Pernando Barrena Arza

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***

Or. en

Amendment 163
Patryk Jaki

Proposal for a directive
Article 4 – paragraph 1 – point 23 – introductory part

Text proposed by the Commission	*Amendment*
(23) 'public administration entity' means an entity in a Member State that ***complies with the following criteria:***	(23) 'public administration entity' means an entity in a Member State that ***was identified by the Member State in accordance with Article 2a.***

Or. en

Amendment 164
Patryk Jaki

Proposal for a directive
Article 4 – paragraph 1 – point 23 – point a

Text proposed by the Commission	*Amendment*
(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;	***deleted***

Or. en

Amendment 165
Patryk Jaki

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

Text proposed by the Commission	*Amendment*
(b) it has legal personality;	***deleted***

Or. en

Amendment 166
Patryk Jaki

Proposal for a directive
Article 4 – paragraph 1 – point 23 – point c

Text proposed by the Commission	*Amendment*
(c) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities, or by other bodies governed by public law;	***deleted***

Or. en

Amendment 167
Patryk Jaki

Proposal for a directive
Article 4 – paragraph 1 – point 23 – point d

Text proposed by the Commission	*Amendment*
(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons,	***deleted***

goods, services or capital.

Or. en

Amendment 168
Patryk Jaki

Proposal for a directive
Article 4 – paragraph 1 – point 23 – paragraph 1

Text proposed by the Commission	*Amendment*
Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded.	***deleted***

Or. en

Amendment 169
Patrick Breyer
on behalf of the Greens/EFA Group

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

Text proposed by the Commission	*Amendment*
	(da) an assessment of the general level of cybersecurity awareness amongst citizens as well as on the general level of security of consumer connected devices;

Or. en

Justification

The security is also a matter of user awareness and level of security of consumer connected devices. Consumer connected devices can be elements in DDoS attacks therefore the level of preparedness of the citizens and the devices commonly put on the market is an important indicator of risks. The reporting is linked to Article 5(2) e which requires awareness raising measures.

Amendment 170
Patryk Jaki

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 ***and public administration entities*** for the provision of their services;

Or. en

Amendment 171
Patrick Breyer
on behalf of the Greens/EFA Group

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***;

Or. en

Justification

While allowing MS flexibility, some level of guidance is introduced.

Amendment 172
Patrick Breyer
on behalf of the Greens/EFA Group

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;

Or. en

Justification

In order to support a diverse threat mitigation landscape.

Amendment 173
Patryk Jaki

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

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

Or. en

Justification

Cybersecurity is not only about ensuring the functionality of the network, but also about protecting the users of the network.

Amendment 174
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Olivier Chastel, Moritz Körner

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

Text proposed by the Commission	*Amendment*
	(ea) a policy on education to develop training programmes on cybersecurity to provide entities with specialists and technicians;

Or. en

Amendment 175
Maria Grapini

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 cybersecurity tools and secure network infrastructure***, including specific policies that address aspects related to representation and gender balance in the above-mentioned fields***;

Or. ro

Amendment 176
Patrick Breyer
on behalf of the Greens/EFA Group

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 ***education establishments, in particular*** academic and research institutions to develop ***and deploy*** cybersecurity tools and secure network infrastructure;

Or. en

Amendment 177
Maria Grapini

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

Text proposed by the Commission	*Amendment*
	(ga) carrying out research projects that contribute to the national cybersecurity strategy, in order to maintain the highest level of cybersecurity possible.

Or. ro

Amendment 178
Peter Kofod

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 also taking into account their capabilities to respond to such threats***.

Or. en

Amendment 179
Patrick Breyer
on behalf of the Greens/EFA Group

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	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.	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. ***For ensuring security and accessibility of information, state of the art cybersecurity measures shall be accompanied by machine-readable datasets and corresponding interfaces (APIs).***

Or. en

Amendment 180
Patryk Jaki

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	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 public administration*** 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

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.

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.

Or. en

Amendment 181
Pernando Barrena Arza

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 ***the public***. 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.

Or. en

Amendment 182
Pernando Barrena Arza

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***, regional and cross-border*** preparedness measures and activities;

Or. en

Amendment 183
Patryk Jaki

Proposal for a directive
Article 9 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure to exchange information with essential and important entities and other relevant interested parties. To this end, Member States shall ensure that the CSIRTs contribute to the deployment of secure information sharing tools.	3. Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure to exchange information with essential and important entities and ***public administration entities and*** other relevant interested parties. To this end, Member States shall ensure that the CSIRTs contribute to the deployment of secure information sharing tools.

Or. en

Amendment 184
Patryk Jaki

Proposal for a directive
Article 9 – paragraph 4

Text proposed by the Commission	*Amendment*

4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted sectorial or cross-sectorial communities of essential and important entities.	4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted sectorial or cross-sectorial communities of essential and important entities ***and public administration entities***.

Or. en

Amendment 185
Patryk Jaki

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 ***and public administration entities*** as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents;

Or. en

Amendment 186
Patrick Breyer
on behalf of the Greens/EFA Group

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;	***deleted***

Or. en

Justification

As criticised by the EDPS the proposal fails to delineate the types of proactive scanning which CSIRTs may be requested to undertake and to identify the main categories of personal data involved. There is a risk that "proactively scanning" systems could enable systematic collection and analysis of personal data and/or electronic communications data by CSIRTs.

Amendment 187
Pernando Barrena Arza

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 proactive scanning of the network and information systems used for the provision of their services; ***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.***

Or. en

Amendment 188
Patryk Jaki

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,	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 ***or public administration entities***, pursuant to

pursuant to Article 20.	Article 20.

Or. en

Amendment 189
Pernando Barrena Arza

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 and ENISA. 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.

Or. en

Amendment 190
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Olivier Chastel, Moritz Körner

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	3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service ***and the European Cybercrime Centre at Europol*** 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

activities of the Cooperation Group.	DORA Regulation] may participate in the activities of the Cooperation Group.

Or. en

Amendment 191
Sophia in 't Veld, Maite Pagazaurtundúa, Moritz Körner

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***,*** ENISA ***and the EDPB***. 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.

Or. en

Justification

A representative of the EDPB should be a member (not solely observer) of the Cooperation Group, because of the task of this group and the possible link with the data protection framework.

Amendment 192
Pernando Barrena Arza

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 appropriate, the Cooperation Group ***shall*** invite representatives of relevant stakeholders***, academia and civil society*** to participate in its work.

Or. en

Amendment 193
Pernando Barrena Arza

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 once a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ***cooperate*** and exchange information.

Or. en

Amendment 194
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Olivier Chastel, Moritz Körner

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.

Or. en

Amendment 195
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal

Šimečka, Olivier Chastel, Moritz Körner

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.

Or. en

Amendment 196
Patryk Jaki

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, focusing in particular on their impact on essential and important entities ***and public administration entities***.

Or. en

Amendment 197
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner

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***.

Or. en

Amendment 198
Patrick Breyer
on behalf of the Greens/EFA Group

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

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

Or. en

Amendment 199
Peter Kofod

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 in particular include an assessment of the following:

Or. en

Amendment 200
Patrick Breyer
on behalf of the Greens/EFA Group

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

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

Or. en

Justification

Justification: It is imperative to cover all risks and vulnerabilities.

Amendment 201
Patryk Jaki

Proposal for a directive
Article 17 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.	1. Member States shall ensure that the management bodies of essential and important ***entities and public administration*** entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.

Or. en

Amendment 202
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal

Šimečka, Moritz Körner

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 ***and cybersecurity specialists in charge,*** 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.

Or. en

Amendment 203
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner

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 continuity of these services and to manage 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.

Or. en

Amendment 204
Patryk Jaki

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 and public administration*** 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.

Or. en

Amendment 205
Patrick Breyer
on behalf of the Greens/EFA Group

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

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

Or. en

Justification

We need to support investment in state of the art technology

Amendment 206
Peter Kofod

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.

Or. en

Amendment 207
Patrick Breyer
on behalf of the Greens/EFA Group

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.

Or. en

Justification

Security by transparency

Amendment 208
Patrick Breyer

on behalf of the Greens/EFA Group

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, ***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.

Or. en

Amendment 209
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner, Olivier Chastel

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***, The European Data Protection Board*** 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.

Or. en

Amendment 210
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 19 – paragraph 2

Text proposed by the Commission	*Amendment*

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

Or. en

Amendment 211
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that 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. Those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service ***and provide information that would enable them to mitigate the adverse effects of the cyberattacks. By exception, where public disclosure could trigger further cyberattacks, essential and important entities, could delay the notification***. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any ***cross border*** impact of the incident.

Or. en

Justification

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

Amendment 212
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner

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***, and to the competent law enforcement authorities if the incident is of a suspected or known malicious nature***. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.

Or. en

Amendment 213
Patryk Jaki

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,	1. Member States shall ensure that essential and important entities ***and public administration entities*** notify, without undue delay***, but 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. Where

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.

appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.

Or. en

Justification

It is important to give a clear deadline. Member States can opt for shorter deadlines as a horizontal or sector-specific requirement, if they deem this appropriate.

Amendment 214
Peter Kofod

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 ***facilitate*** that essential and important entities ***may*** 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.

Or. en

Amendment 215

Patryk Jaki

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 cyber threat that those entities identify that could have potentially resulted in a significant incident.	2. Member States shall ensure that essential and important entities ***and public administration entities*** notify, without undue delay***, but within 24 hours***, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.

Or. en

Justification

It is important to give a clear deadline also in the case of a potential incident. The threat could still persist and affect other entities. Quick reporting could help mitigate the threat.

Amendment 216
Patrick Breyer
on behalf of the Greens/EFA Group

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.	Those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. ***By exception, where public disclosure could trigger further cyberattacks, essential and important entities, could delay the notification.*** The notification shall not make the notifying entity subject to increased liability.

Or. en

Amendment 217
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner

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, or may be, 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.

Or. en

Amendment 218
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 20 – paragraph 7

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

Or. en

Justification

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

Amendment 219
Patryk Jaki

Proposal for a directive
Article 20 a (new)

Text proposed by the Commission	*Amendment*
	Article 20 a
	Divergence for Public Administration Entities
	Member States may lay down the rules on whether and to what extent public administration entities are excluded from the obligations provided in Article 17, Article 18 and Article 20.

Or. en

Amendment 220
Patryk Jaki

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	1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important ***entities and public administration*** entities to certify certain ICT products, ICT services and ICT

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.	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 ***public administration entities or*** procured from third parties.

Or. en

Amendment 221
Patrick Breyer
on behalf of the Greens/EFA Group

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 in consultation with the EDPB***, 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.

Or. en

Amendment 222
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner

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	2. ENISA***, after having consulted the EDPB***, in collaboration with Member States, shall draw up advice and guidelines

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.	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.

Or. en

Amendment 223
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 23

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

Member States shall ensure that such policies and procedures are made publicly available.

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

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

Or. en

Justification

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

Agreements with ICANN already contain provisions requiring baseline measures (e.g. annual reminder to registrants that data must be accurate, correcting data when presented with evidence of inaccuracy, etc.) to verify the accuracy of domain registration data.

Amendment 224
Pernando Barrena Arza

Proposal for a directive
Article 23 – paragraph 1

Text proposed by the Commission	*Amendment*
1. For the purpose of contributing to	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.	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 ***in accordance*** with Union data protection law as regards data which are personal data.

Or. en

Amendment 225
Pernando Barrena Arza

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 information to identify and contact the holders of the domain names***, such as name and electronic mail address,*** and the points of contact administering the domain names under the TLDs.

Or. en

Amendment 226
Pernando Barrena Arza

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	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.	duly justified requests***, necessary within the competences of CERTs, CSIRTs and competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences***, 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 ***sufficiently substantiated*** requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Or. en

Amendment 227
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner

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 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 notified*** requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Or. en

Amendment 228
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 24 – paragraph 1

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

Or. en

Amendment 229
Patrick Breyer
on behalf of the Greens/EFA Group

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

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

Or. en

Amendment 230

Peter Kofod

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

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

Or. en

Amendment 231
Patryk Jaki

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

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

Or. en

Amendment 232

Patryk Jaki

Proposal for a directive
Article 26 – paragraph 2

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

Or. en

Amendment 233
Patryk Jaki

Proposal for a directive
Article 26 – paragraph 4

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

Or. en

Amendment 234
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 28 – paragraph 2

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

Or. en

Justification

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

Amendment 235
Patryk Jaki

Proposal for a directive
Article 30 a (new)

Text proposed by the Commission	*Amendment*
	Article 30 a
	Supervision and enforcement for public administration entities
	1. Member States shall ensure that the measures of supervision or enforcement imposed on public administration entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.
	2. Member States shall ensure that competent authorities, where exercising their supervisory tasks and enforcement powers in relation to public administration entities have the appropriate powers in accordance with national legislation.

Or. en

Amendment 236
Patryk Jaki

Proposal for a directive
Article 31 – title

Text proposed by the Commission	*Amendment*
General conditions for imposing administrative fines on essential and important entities	General conditions for imposing administrative fines on essential and important entities ***and public administration entities***

Or. en

Amendment 237
Patryk Jaki

Proposal for a directive
Article 31 – paragraph 1

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

Or. en

Amendment 238
Patryk Jaki

Proposal for a directive
Article 31 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Without prejudice to the powers of competent authorities pursuant to Articles	6. Without prejudice to the powers of competent authorities pursuant to Articles

29 and 30, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities ***referred to in*** Article ***4(23)*** subject to the obligations provided for by this Directive.	29 and 30, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities ***identified in accordance with*** Article ***2a*** subject to the obligations provided for by this Directive.

Or. en

Amendment 239
Patryk Jaki

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 or public administration*** 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.

Or. en

Amendment 240
Sophia in 't Veld, Maite Pagazaurtundúa, Moritz Körner, Fabienne Keller

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	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***.	entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ***without undue delay***.

Or. en

Amendment 241
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 32 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities 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 within ***72 hours***.

Or. en

Justification

To align with Art. 33 (1) GDPR

Amendment 242
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 32 – paragraph 3

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

Or. en

Justification

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

Amendment 243
Patrick Breyer
on behalf of the Greens/EFA Group

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.

Or. en

Justification

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

Amendment 244
Maite Pagazaurtundúa, Hilde Vautmans, Sophia in 't Veld, Fabienne Keller, Michal Šimečka, Moritz Körner

Proposal for a directive
Article 35 – paragraph 1

Text proposed by the Commission	*Amendment*
The Commission shall ***periodically*** review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The first report shall be submitted by… 54 months after the date of entry into force of this Directive.	The Commission shall review the functioning of this Directive ***every 3 years***, and report to the European Parliament and to the Council. The report shall in particular assess ***to what extent the Directive has contributed to achieve the highest level of security and integrity of networks and information, 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… ***[***54 months after the date of entry into force of this Directive***]***.

Or. en

Amendment 245
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 35 – paragraph 1

Text proposed by the Commission	*Amendment*
The Commission shall periodically review the functioning of this Directive, and report to the European Parliament and to the	The Commission shall periodically review the functioning of this Directive, and report to the European Parliament and to the

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

Or. en

Amendment 246
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 40 – paragraph 1

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

Or. en

Justification

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

Amendment 247
Patrick Breyer
on behalf of the Greens/EFA Group

Proposal for a directive
Article 40 a (new)

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

Or. en

Justification

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