European Parliament
2019-2024

Committee on Industry, Research and Energy

2020/0359(COD)

3.6.2021

AMENDMENTS
92 - 362

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

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

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

Amendment 92
Evžen Tošenovský

Proposal for a directive
Title 1

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

Or. en

Amendment 93
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 3

Text proposed by the Commission	*Amendment*
(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence and cause major damage to the Union economy and society. Cybersecurity	(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.	preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market. ***The use of artificial intelligence in cybersecurity has the potential of improving the detection and to stop unsophisticated attacks, enabling resources to be diverted towards more sophisticated attacks. Member States should therefore encourage in their national strategies the use of automated tools in cybersecurity and the sharing of data needed to train and improve automated tools in cybersecurity.***

Or. en

Amendment 94
Evžen Tošenovský

Proposal for a directive
Recital 7

Text proposed by the Commission	*Amendment*
(7) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy in light of the considerations set out in recitals (4) to (6). The sectors covered by Directive (EU) 2016/1148 should therefore be extended to provide a comprehensive coverage of the sectors and services of vital importance for key societal and economic activities within the internal market. ***The rules should not be different according to whether the entities are operators of essential services or digital service providers. That differentiation has proven obsolete, since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market.***	(7) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy in light of the considerations set out in recitals (4) to (6). The sectors covered by Directive (EU) 2016/1148 should therefore be extended to provide a comprehensive coverage of the sectors and services of vital importance for key societal and economic activities within the internal market.

Or. en

Amendment 95
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 7

Text proposed by the Commission	*Amendment*
(7) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy in light of the considerations set out in recitals (4) to (6). The sectors covered by Directive (EU) 2016/1148 should therefore be extended to provide a comprehensive coverage of the sectors and services of vital importance for key societal and economic activities within the internal market. The ***rules*** should not be different according to whether the entities are operators of essential services or digital service providers. That differentiation has proven obsolete, since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market.	(7) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy in light of the considerations set out in recitals (4) to (6). The sectors covered by Directive (EU) 2016/1148 should therefore be extended to provide a comprehensive coverage of the sectors and services of vital importance for key societal and economic activities within the internal market. The ***risk management requirements and reporting obligations*** should not be different according to whether the entities are operators of essential services or digital service providers. That differentiation has proven obsolete, since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market.

Or. en

Justification

Consistency with text of the Directive.

Amendment 96
Marisa Matias, Sira Rego, Cornelia Ernst, Manuel Bompard

Proposal for a directive
Recital 10

Text proposed by the Commission	*Amendment*
(10) The Commission, in cooperation with the Cooperation Group, ***may*** issue	(10) ***SMEs represent, in the European context, a huge percentage of the***

guidelines on the implementation of the criteria applicable to micro and small enterprises.

industrial/business market and, given the new practices in the sector, increasingly digitised, they face specific and worrying cybersecurity challenges. Limited cyber knowledge, lack of cybersecurity, high cost of cybersecurity solutions are some of these challenges for which SMEs need increased protection. Member States should therefore, and on the basis of this Directive, plan and implement national cybersecurity strategies to make available all existing or to be created means to technically support SMEs so they will be able to detect, prevent and react to cyberattacks or cyber threats. The Commission***, directly or through ENISA***, in cooperation with the Cooperation Group, ***will*** issue guidelines on the implementation of the criteria applicable to micro and small enterprises.

Or. en

Amendment 97
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
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 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	(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 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.	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. ***The provisions of this Directive apply to entities with complex business models or operating environments, whereby an entity may simultaneously fulfil the criteria assigned to both essential and important entities. In order to enable the effective supervision and enforcement of risk management measures and reporting obligations for entities falling within the scope of this Directive, competent authorities or CSIRTs shall enforce the provisions of this Directive to a function or unit level within an entity, in order to appropriately and sufficiently address the level of criticality.***

Or. en

Justification

Entities with complex business models may at the same time fulfil the classification criteria for both essential and important entities. This addition is intended to allow competent authorities or CSIRTs to enforce the provision of the Directive to such complex environments in order to properly assess the level of criticality.

Amendment 98
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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 into account the level of criticality of the sector or of the type of service, as well as	(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 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.	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 ***cybersecurity risk management measures, reporting obligations and*** 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.

Or. en

Amendment 99
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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 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.	(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 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. Important entities should be subject to ***lighter*** reporting obligations***, and longer timelines to reflect the complexity of forensics***. 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.

Or. en

Amendment 100
Marisa Matias, Sira Rego, Cornelia Ernst, Sandra Pereira, Giorgos Georgiou, Manuel Bompard

Proposal for a directive
Recital 11 a (new)

Text proposed by the Commission	*Amendment*
	(11a) The Covid-19 pandemic has changed many pre-existing work situations, forcing many workers to work from home, and it seems that this change is here to stay for many of these situations. Therefore, it is necessary to ensure that homeworkers are also adequately protected against cybercrime threats and/or attacks. This requires such workers to be adequately trained to detect, prevent and/or react to cyber threats. These workers must as well be protected against employers' cyber surveillance systems that would not just violate their labour rights as their personal ones as the right to privacy. Trade unions and other relevant stakeholders must play a meaningful role in this protection.

Or. en

Amendment 101
Marisa Matias, Sira Rego, Cornelia Ernst, Sandra Pereira, Giorgos Georgiou, Manuel Bompard

Proposal for a directive
Recital 11 b (new)

Text proposed by the Commission	*Amendment*
	(11b) The daily lives of a large part of the population are increasingly digitalised, both personally and professionally, and in this pandemic

phase we are seeing much greater and growing use of various digital platforms for various purposes. Consumers' rights must therefore be properly protected, particularly the right to be informed of any cyberattacks on websites that they have used and/or on which they may have provided their personal data.

Or. en

Amendment 102
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission may issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.	(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors***. Sector-specific legislation and instruments that require essential or important entities to adopt cybersecurity risk management measures, or impose reporting obligations for significant incidents, shall, where possible, be consistent with the terminology, and refer to the definitions in Article 4 of this Directive***. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive***, and apply to the entirety of the security aspects of the operations and services provided by essential and important entities***, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission may issue guidelines in relation to the implementation of the lex

specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

Or. en

Justification

This Directive should remain the building block on which different sector-specific issues shall be addressed through sector-specific legislation or instruments. Sufficient alignment and coordination of future sector-specific instruments shall be foreseen in order to avoid regulatory overlaps and the risks arising therefrom.

Amendment 103
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. ***Where a*** sector–specific Union legal act ***requires*** essential or important entities to adopt cybersecurity risk management measures ***or*** to notify incidents or significant cyber threats ***of at least an equivalent effect to the obligations*** laid down in this Directive***, those*** sector-specific ***provisions, including*** on supervision and enforcement, should apply. The Commission may issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is	(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. ***As a minimum baseline*** sector–specific Union legal act ***should require*** essential or important entities to adopt cybersecurity risk management measures ***and*** to notify incidents or significant cyber threats ***in line with requirements*** laid down in ***Articles 18 (1, 2) and 20 of*** this Directive***. Where*** sector-specific ***legislations foresee specific rules*** on supervision and enforcement, ***these rules*** should apply. The Commission may issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management

without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

measures and incident notifications. ***Nevertheless, while adopting the additional sector-specific Union acts the need of a comprehensive and consistent cybersecurity framework should be duly taken into account.*** This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

Or. en

Justification

There is a need to strengthen the importance of the NIS2 Directive as the main horizontal legislation in the field of cybersecurity. Safeguards should be provided that future sectoral legislation does not change the main principles of the NIS2 framework when it comes to cybersecurity requirements and incident notification. It is also crucial that incident notifications from all sectors are sent directly to CSIRTs.

Amendment 104
Christophe Grudler, Klemen Grošelj, Nathalie Loiseau, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ***may*** issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-	(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ***should*** issue guidelines in relation to the implementation of the lex specialis***, taking relevant opinions, expertise and best practices of***

specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.	***ENISA and the Cooperation Group into account***. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

Or. en

Justification

To ensure that implementation of lex specialis is done in a way that respects the minimum security requirements defined and established by the NIS directive, best practices collected by ENISA and the NIS cooperation group should be taken into account in Commission guidelines.

Amendment 105
Tsvetelina Penkova

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ***may*** issue guidelines in relation to the implementation of ***the lex specialis. This*** Directive ***does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures***	(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, ***and where the requirements are neither conflicting nor overlapping,*** those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ***shall*** issue ***comprehensive*** guidelines in relation to the implementation of ***each sector specific legislation, including on how it impacts***

and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

the application of the directive. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

Or. en

Amendment 106
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 14

Text proposed by the Commission	*Amendment*
(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to	(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information ***on a regular basis***, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to

exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose.

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

exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose.

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

Or. en

Amendment 107
Rasmus Andresen
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

Justification

As this Directive sets a general cybersecurity framework for networks, DNS operators could fall under the category of essential or important entities, but a sectorial regulation of DNS should be introduced only if necessary and through a separate act.

Amendment 108
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez

Muñoz

Proposal for a directive
Recital 15

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

Or. en

Justification

Differentiating between the resolution sides of the DNS is essential to include in scope the necessary services and excluding the root name servers. Excluding those from the scope if essential to maintain and open internet and avoid risks of fragmentation and risks of extra-territorial application of the Directive.

Amendment 109
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Christophe Grudler

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,	(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***.	this Directive should apply to ***publicly available recursive domain name*** resolution ***services and authoritative domain name resolution services. This Directive does not apply to*** root name servers.

Or. en

Amendment 110
Evžen Tošenovský

Proposal for a directive
Recital 15

Text proposed by the Commission	*Amendment*
(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, ***including operators of root name servers,*** top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.	(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.

Or. en

Amendment 111
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 17 a (new)

Text proposed by the Commission	*Amendment*
	(17a) The edge ecosystem is an emerging vector susceptible to cyber threats and a

growing trend with attacks targeting devices — such as routers, switches, and firewalls — is having a significant impact to both enterprises and to the connected digital ecosystem in its entirety. Edge computing ecosystems delivered in a highly distributed form are essential for the development of the Internet of Things (IoT), the Industrial Internet of Things (IIoT) and the sectoral ecosystems of connected devices such as connectivity infrastructure and autonomous vehicles. IoT devices may potentially offer additional attack surfaces and allow threats and attacks to trickle from the device to the network or the cloud. Poor security of IoT devices or IoT gateways can potentially hinder the security of the entire connectivity chain and the data flows towards the edge and the cloud, consequentially affecting the overall security of the ecosystem.

Or. en

Justification

Distributed cloud computing and connected devices offer additional attack surfaces and can lead to spill over effects of risks, incidents and cybersecurity threats.

Amendment 112
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 17 b (new)

Text proposed by the Commission	*Amendment*
	(17b) The continuous increase of computing power combined with the rising levels of maturity of exponential technologies such as machine learning (ML) and artificial intelligence (AI) enable the development of advanced cybersecurity capabilities for real-time

detection, analysis, containment and response to cyber threats in a rapidly evolving threat landscape. AI tools and applications are used to develop security controls including, but not limited to, active firewalls, smart antivirus, automated CTI (cyber threat intelligence) operations, AI fuzzing, smart forensics, email scanning, adaptive sandboxing, and automated malware analysis.

Or. en

Justification

Artificial Intelligence and machine learning can enhance the capabilities of cybersecurity tools and applications, and enable the creation of new forms of collective threat intelligence and automation of cybersecurity-enhancing functions.

Amendment 113
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 17 c (new)

Text proposed by the Commission	*Amendment*
	(17c) Data-driven tools and applications powered by AI-enabled systems require the processing of large amounts of data, which may include personal data. Risks persist in the entire lifecycle of AI-enabled systems in cybersecurity-enhancing tools and applications, and in order to mitigate risks of unduly interference with the rights and freedoms of individuals, the requirements of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679 shall be applied. Integrating appropriate safeguards such as pseudonymisation, encryption, data accuracy, and data minimisation in the design and use of AI-enabled systems deployed in cybersecurity applications and

processes is essential to mitigate the risks that such systems may pose on personal data.

Or. en

Justification

AI-enabled cybersecurity tools and applications must take account of risks arising to the processing of personal data. The requirements of data protection by design and by default as laid down by Regulation (EU) 2016/679 must be respected when such tools are designed and integrated in cybersecurity.

Amendment 114
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 17 d (new)

Text proposed by the Commission	*Amendment*
	(17d) Member States should adopt policies on the promotion and integration of AI-enabled systems in the prevention and detection of cybersecurity incidents and threats as part of their national cybersecurity strategies. Such policies should emphasise the technological and operational measures including, but not limited to, workflow automation, streaming analytics, active monitoring, intelligent prediction and advanced network threat detection, in order to accelerate the analysis, validation and prioritisation of threats. ENISA's National Capabilities Assessment Framework (NCAF) can assist in the evaluation and alignment of Member States' policies building on available use cases and key performance indicators. Moreover, an assessment of Member States' capabilities and overall level of maturity as regards the integration of AI-enabled systems in cybersecurity should be factored in the methodological

construction of the cybersecurity index within the meaning of ENISA's report on the state of cybersecurity in the Union under Article 15 of this Directive.

Or. en

Justification

Member States' national cybersecurity strategies to include the promotion and integration of AI in cybersecurity-related practices to enable the development of national cybersecurity processes fit for the future.

Amendment 115
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 17 e (new)

Text proposed by the Commission	*Amendment*
	(17e) Open-source cybersecurity tools contribute to a higher degree of transparency and have a positive impact on the efficiency of industrial innovation. Open standards facilitate interoperability between security tools, benefitting the security of industrial stakeholders, enabling the diversification of reliance from a single supplier or vendor, and leading to a more comprehensive CTI framework. Semi-automation of CTI production is an important tool to reduce the number of manual steps underpinning the analysis of CTI. The use of AI and ML within CTI should be further explored to increase the value of machine learning functions within CTI activities.

Or. en

Justification

Open-source tools and applications increase interoperability and enable the diversification of reliance from single vendors for industrial stakeholders. Such tools may also allow for

increased automation.

Amendment 116
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 17 f (new)

Text proposed by the Commission	*Amendment*
	(17f) Member States should develop a policy for the integration of open-source tools in public administration, and further explore measures to incentivise the wider adoption of open-source software by developing strategies to address and minimise the legal and technical risks that entities are faced with, as regards licensing and the necessary levels of technical support. Such policies are of particular importance for small and medium-sized enterprises (SMEs) facing significant costs for implementation, which can be minimised by reducing the need for specific applications or tools.

Or. en

Justification

Member States to include policies on integrating open-source tools and applications in their national cybersecurity strategies.

Amendment 117
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 19

Text proposed by the Commission	*Amendment*
(19) Postal service providers within the meaning of Directive 97/67/EC of the	(19) Postal service providers within the meaning of Directive 97/67/EC of the

European Parliament and of the Council[18] , as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services. Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services.

[18] Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998, p. 14).

European Parliament and of the Council[18] , as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services ***while taking into account the degree of their dependence on network and information systems***. Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services.

[18] Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998, p. 14).

Or. en

Amendment 118
Evžen Tošenovský

Proposal for a directive
Recital 20

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

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.	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.

Or. en

Amendment 119
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Recital 20 a (new)

Text proposed by the Commission	*Amendment*
	(20a) Member States should ensure that the network and information systems used by their public administration entities are subject to their national cybersecurity regulation. Where appropriate, public administration entities should be subject to obligations similar to those for essential and important entities, as appropriate.

Or. en

Amendment 120
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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	(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.

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***, particularly for supervision and enforcement***. Member States should be able to assign this role to an existing authority. ***The competent authorities should have the necessary means to perform their duties, including powers to request the information necessary to assess the level of security of networks or services. They should also have the power to request comprehensive and reliable data about actual security incidents that have had a significant impact on the operation of services. They should, where necessary, be assisted by CSIRTs. In particular, CSIRTs may be required to provide competent authorities with information about risks and security incidents affecting services and recommend ways to address them.***

Or. en

Amendment 121
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova

Proposal for a directive
Recital 21 a (new)

Text proposed by the Commission	*Amendment*
	(21a) Public-Private Partnerships (PPPs) in the field of cybersecurity can provide the right framework for knowledge exchange, sharing of best practices and the establishment of a common level of understanding amongst all stakeholders. Goal-oriented and service outsourcing PPPs foster a culture of cybersecurity at the Member State level,

and leverage the exchange and transfer of expertise, thus raising cybersecurity awareness and the overall level of reciprocal support between public and private entities. Hybrid PPPs enable governments to assign either the operation, or the delivery of service-specific functions, of a CSIRT to an experienced entity facilitating the access of public administrations to private sector resources, and increasing the levels of trust between stakeholders by establishing a proactive attitude in case of incidents or crises.

Or. en

Amendment 122
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova

Proposal for a directive
Recital 21 b (new)

Text proposed by the Commission	*Amendment*
	(21b) Member States should adopt policies underpinning the establishment of cybersecurity-specific PPPs as part of their national cybersecurity strategies. These policies should clarify, among others, the scope and stakeholders involved, the governance model, the available funding options, and the interaction among participating stakeholders. PPPs can leverage the expertise of private sector entities to support Member States' competent authorities in developing state-of-the art services and processes including, but not limited to, information exchange, early warnings, cyber threat and incident exercises, crisis management, and resilience planning.

Or. en

Justification

Member States to include PPP policies in their national cybersecurity strategies, laying out specific provisions underpinning the governance model, the funding options and the interaction within the PPP framework to enable Member States with limited resources to take advantage of private sector resources in further strengthening their competent authorities and CSIRTs.

Amendment 123
Marisa Matias, Sira Rego, Cornelia Ernst, Manuel Bompard

Proposal for a directive
Recital 23 a (new)

Text proposed by the Commission	*Amendment*
	(23a) Cybercrime is a cross-border issue, in a constant changing process, so in order to achieve a common level of cybersecurity across the EU, the rules on prevention, detection and response to cyber threats and attacks need to be harmonized as far as possible. Therefore, ENISA should provide continuous technical support to Member States and national competent authorities and, in addition to its supervisory tasks, ENISA should provide regular recommendations and guidance for the implementation of cybersecurity best practices, also for support to SMEs. and to workers.

Or. en

Amendment 124
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 24

Text proposed by the Commission	*Amendment*
(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to	(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to

prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ensure that they have well-functioning CSIRTs, also known as computer emergency response teams (‘CERTs’), complying with essential requirements in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. In view of enhancing the trust relationship between the entities and the CSIRTs, in cases where a CSIRT is part of the competent authority, Member States should consider functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities.

prevent, detect, respond to and mitigate network and information system incidents and risks***. Member States should ensure that CSIRTs have at their disposal an appropriate, secure, and resilient communication and information infrastructure to exchange information between CSIRTs and with essential and important entities and other relevant parties***. Member States should therefore ensure that they have well-functioning CSIRTs, also known as computer emergency response teams (‘CERTs’), complying with essential requirements in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. In view of enhancing the trust relationship between the entities and the CSIRTs, in cases where a CSIRT is part of the competent authority, Member States should consider functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities.

Or. en

Amendment 125
Evžen Tošenovský

Proposal for a directive
Recital 24

Text proposed by the Commission	*Amendment*
(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ensure that they ***have*** well-functioning ***CSIRTs, also known as computer emergency response teams (‘CERTs’)***,	(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ***designate one or more CSIRTs under this Directive and*** ensure that they ***are*** well-functioning, complying with essential

complying with essential requirements in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. In view of enhancing the trust relationship between the entities and the CSIRTs, in cases where a CSIRT is part of the competent authority, Member States should consider functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities.

requirements in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level***. Member States may as CSIRTs designate also existing computer emergency response teams ('CERTs')***. In view of enhancing the trust relationship between the entities and the CSIRTs, in cases where a CSIRT is part of the competent authority, Member States should consider functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities.

Or. en

Amendment 126
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 25

Text proposed by the Commission	*Amendment*
(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] as regards personal data, on behalf of and upon request by an entity under this Directive, a proactive scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.	(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] as regards personal data, on behalf of and upon request by an entity under this Directive, ***or in case of a serious threat to national security,*** a proactive scanning of the network and information systems used for the provision of their services***. The knowledge whether an entity runs a privileged management interface, affects the speed of undertaking mitigating actions. It is critical that an entity or a CSIRTs upon an entity's request, have the ability to continuously discover, inventory, manage, and monitor all internet-facing assets, both on premises and in the cloud, to understand their overall organisational risk to newly discovered supply chain***

	compromises or critical vulnerabilities. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.
[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).	[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

Or. en

Amendment 127
Rasmus Andresen
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 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 ***in order to identify, mitigate or prevent specific network and information security threats. Processing of personal data by such scanning should be kept to the minimum necessary and should, in particular, respect the principles of data minimisation, purpose limitation and data protection by design and by default***. Member States should aim at ensuring an

equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.

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

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

Or. en

Justification

As a particular case, answering a targeted need, such scanning should be accompanied by legal clarity and safeguards.

Amendment 128
Marisa Matias, Sira Rego, Cornelia Ernst, Manuel Bompard

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. ***With regard to personal data, all entities, public***

	and/or private, which, due to a reported incident or a detected cybersecurity threat, wish to access or legitimately access personal data shall proceed in absolute accordance with the General Data Protection Regulation.
[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).	[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

Or. en

Amendment 129
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Nicola Danti, Christophe Grudler, Martina Dlabajová

Proposal for a directive
Recital 26

Text proposed by the Commission	*Amendment*
(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive.	(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks***, including with CSIRTs outside the Union,*** in addition to the CSIRTs network established by this Directive.

Or. en

Justification

International cooperation with likeminded partners outside the Union should be encouraged.

Amendment 130
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez

Muñoz

Proposal for a directive
Recital 26 a (new)

Text proposed by the Commission	*Amendment*
	(26a) Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application security, and business or end-user data which entities rely on. Cyber hygiene policies comprising a common baseline set of practices including, but not limited to, software and hardware updates, password changes, management of new installs, limitation of administrator-level access accounts, and backing up of data, enable a proactive framework of preparedness and overall safety and security in the event of incidents or threats.

Or. en

Justification

Cyber hygiene policies and control cam prevent security risks, enabling a proactive framework of security preparedness and safety.

Amendment 131
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 26 b (new)

Text proposed by the Commission	*Amendment*
	(26b) Member States should adopt policies to promote cyber hygiene as part of their national cybersecurity strategies. Such policies should build on cyber hygiene controls and programmes that are affordable and accreditable in order to

minimise the cost of implementation, especially for SMEs, and encourage wider compliance thereto by both public and private entities. ENISA should monitor and assess Member States' cyber hygiene policies, and explore EU wide schemes to enable cross-border checks ensuring equivalence independent of Member State requirements.

Or. en

Justification

Member States adopting cyber hygiene protocols can add value to the overall preparedness of competent authorities and raise security overall.

Amendment 132
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova

Proposal for a directive
Recital 28

Text proposed by the Commission	*Amendment*
(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC 29417 provide guidance on vulnerability handling and vulnerability disclosure respectively. As regards vulnerability	(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC 29417 provide guidance on vulnerability handling and vulnerability disclosure respectively. As regards vulnerability

disclosure, coordination between reporting entities and manufacturers or providers of ICT products or services is particularly important. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also comprise coordination between the reporting entity and the organisation as regards the timing of remediation and publication of vulnerabilities.

disclosure, coordination between reporting entities and manufacturers or providers of ICT products or services is particularly important. ***Voluntary*** coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also comprise coordination between the reporting entity and the organisation as regards the timing of remediation and publication of vulnerabilities. ***Strengthening the coordination and timely exchange of relevant information between the manufacturer or provider of ICT products or services and the reporting entities is essential to facilitate the voluntary framework of vulnerability disclosure.***

Or. en

Amendment 133
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
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	(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 ***the reporting entity, or the manufacturer or the provider of ICT products or services,***

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.

engages a third-party coordinator to assist with the disclosure process. 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.

Or. en

Amendment 134
Tsvetelina Penkova

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	(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 manufacturers or providers of ICT products or services, ***which report the vulnerability, and their customers, which are likely to be affected by the vulnerability,*** where necessary. The tasks of the CSIRT coordinator should in particular include identifying and contacting concerned entities, supporting reporting entities, ***providing guidelines on*** disclosure timelines, and managing vulnerabilities that affect multiple organisations (multi-party vulnerability disclosure). Where vulnerabilities affect multiple manufacturers or providers of ICT

Member State, the designated CSIRTs from each of the affected Member States should cooperate within the CSIRTs Network.

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 ***in providing assistance and guidance to the affected manufacturers***.

Or. en

Amendment 135
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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***, in cooperation with ENISA,*** 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.

Or. en

Amendment 136
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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. ***In general, to encourage a culture of disclosure of incidents a voluntary disclosure should be without detriment to the reporting entity. Any exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities***

Or. en

Amendment 137
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

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	(30) Access to correct and timely information on vulnerabilities affecting ICT products and services ***and industrial***

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.

control systems (ICS) 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.

Or. fr

Amendment 138
Evžen Tošenovský

Proposal for a directive
Recital 30

Text proposed by the Commission	*Amendment*
(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. In that regard, sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability ***registry*** where, essential and important entities and their suppliers, as well as entities which do not fall in the scope of application of this Directive may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures.	(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. In that regard, sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability ***database*** where, essential and important entities and their suppliers, as well as entities which do not fall in the scope of application of this Directive may, on a voluntary basis, disclose ***the patched*** vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures.

Or. en

Amendment 139
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 31

Text proposed by the Commission	*Amendment*
(31) Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A European vulnerability registry maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries in third country jurisdictions.	(31) Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A European vulnerability registry maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries in third country jurisdictions. ***ENISA could play a more central management role either by exploring the option of becoming a "Root CVE Numbering Authority" in the global Common Vulnerabilities and Exposures (CVE) registry, or setting up a database to leverage the existing CVE programme for vulnerability identification and registration to enable interoperability and reference between the European and third country jurisdiction registries.***

Or. en

Justification

ENISA can pursue becoming a root numbering authority in the global CVE efforts and thus gain a more central management role, allowing ENISA to enable interoperability and reference of the European registry with global equivalent efforts.

Amendment 140
Evžen Tošenovský

Proposal for a directive
Recital 31

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

Or. en

Amendment 141
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 32

Text proposed by the Commission	*Amendment*
(32) The Cooperation Group should establish a work programme every two years including the actions to be undertaken by the Group to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive should be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of	(32) ***The Cooperation Group set up under this Directive, should include representatives of Member States, the Commission, ENISA and, due to the link with the data protection framework, the European Data Protection Board (EDPB).*** The cooperation group should establish a work programme every two years including the actions to be undertaken by the Group to implement its

the Group.	objectives and tasks. The timeframe of the first programme adopted under this Directive should be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Group.

Or. en

Justification

As a first mention of the Group, clarity on its membership has been added, in line with changes proposed in the articles.

Amendment 142
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 35

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

Or. en

Justification

Clarity of the structure and security clearance of such exchanges is necessary to ensure the effectiveness of the exchange and cooperation among CSIRTs.

Amendment 143
Rasmus Andresen
on behalf of the Greens/EFA Group

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 ***and the European cyber crises liaison organisation network***. Such agreements should ensure adequate protection of ***Union interests and*** data. ***This shall not preclude the right of Member States to cooperate with like-minded third countries on management of vulnerabilities and cyber security risk management, facilitating reporting and general information sharing in line with Union legislation.***

Or. en

Justification

Cyber incidents are often cross border beyond the Union and it makes sense to cooperate in treating them.

Amendment 144
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 38

Text proposed by the Commission	*Amendment*

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

Or. en

Justification

Moved from recital to Article 4 (Definitions).

Amendment 145
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 39

Text proposed by the Commission	*Amendment*
(39) For the purposes of this Directive, the term 'near misses' should refer to an event which could potentially have caused harm, but was successfully prevented from fully transpiring.	***deleted***

Or. en

Justification

Moved from recital to Article 4 (Definitions).

Amendment 146
Christophe Grudler, Klemen Grošelj, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

Proposal for a directive
Recital 40

Text proposed by the Commission	*Amendment*
(40) Risk-management measures should include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data.	(40) Risk-management measures should include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data. ***It must be approached using systemic analysis that break down the various processes and the interactions between the subsystems, in order to have a complete picture of the security of the information system. The human factor should be fully taken into account in the analysis.***

Or. en

Justification

A systemic approach towards the security of information systems is necessary

Amendment 147
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 40

Text proposed by the Commission	*Amendment*
(40) Risk-management measures should include measures to identify any risks of incidents, to prevent, detect ***and handle*** incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data.	(40) Risk-management measures should include measures to identify any risks of incidents, to prevent, detect***, respond to, attribute, and recover from*** incidents***,*** and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data.

Or. en

Amendment 148

Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Recital 43

Text proposed by the Commission	*Amendment*
(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. ***Entities should be in particular encouraged to incorporate the cybersecurity safeguards into the contractual arrangements with the tier-1 suppliers and service providers, including responsibility of the tier-1 suppliers for other tiers of suppliers and service providers.***

Or. en

Amendment 149
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 43

Text proposed by the Commission	*Amendment*
(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence	(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence

of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should ***therefore*** assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should ***evaluate their own cybersecurity capabilities and pursue the integration of cybersecurity enhancing technologies driven by AI or machine learning systems to automate their capabilities and the protection of network architectures. Entities should also*** assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.

Or. en

Justification

Lesson learned from past cybersecurity incidents is the need to modernise technologies such as artificial intelligence & machine learning -based user behavioural, and technologies that effectively collect, integrate, and normalise security data across the entire network to assist with incident response.

Amendment 150
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 43

Text proposed by the Commission	*Amendment*
(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to ***cyber-attacks*** and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party	(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to ***attacks against information systems*** and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third

products and services. Entities should therefore assess and take into account the overall quality of products ***and*** cybersecurity practices of their suppliers and service providers, including their secure development procedures.	party products and services. Entities should therefore assess and take into account the overall quality of products***, the security measures embedded in them and the*** cybersecurity practices of their suppliers and service providers, including their secure development procedures ***and security features of the product***.

Or. en

Justification

In order to address efficiently the security, not only the stakeholders in a supply chain have to implement security measures for themselves, but the products need to be assessed from a cybersecurity standpoint.

Amendment 151
Tsvetelina Penkova

Proposal for a directive
Recital 43

Text proposed by the Commission	*Amendment*
(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality ***and resilience*** of products***, services*** and cybersecurity practices of their suppliers and service providers, including their secure development procedures.

Or. en

Amendment 152
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 43 a (new)

Text proposed by the Commission	*Amendment*
	(43a) In order to offer the necessary transparency to mitigate 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[1a]

Or. en

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

Justification

Supply chains are included in the Opinion 5/2021 of the European Data Protection Supervisor.

Amendment 153
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 44

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

operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP.

operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP***, not only in terms of the close operational integration but also as regards the need for such outsourced activities involving personal data by a controller to be in full compliance with Regulation (EU) 2016/679, in particular the processing by a processor on behalf of a controller***.

Or. en

Amendment 154
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 44

Text proposed by the Commission	*Amendment*
(44) Among service providers, managed security services providers (MSSPs) in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to detect and respond to incidents. Those MSSPs have however also been the targets of ***cyberattacks*** themselves and through their close integration in the operations of operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP.	(44) Among service providers, managed security services providers (MSSPs) in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to detect and respond to incidents. Those MSSPs have however also been the targets of ***attacks against information systems*** themselves and through their close integration in the operations of operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP. *(This amendment should apply across the text, replacing cyberattacks with "attacks against information systems", aligning the wording with the Cybercrime Directive 2013/40/EU)*

Or. en

Justification

The term cyberattack is not explicit by itself therefore needs to be replaced with "attacks against information systems", as in the Cybercrime Directive 2013/40/EU.

Amendment 155
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Nicola Danti, Christophe Grudler

Proposal for a directive
Recital 45

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

Or. en

Amendment 156
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 46

Text proposed by the Commission	*Amendment*
(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21] , with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.	(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA***, and in consultation with the European Data Protection Board (EDPB)***, 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. ***Particular emphasis should be placed on ICT services, systems or products subject to specific requirements, in particular in third country jurisdictions serving as the country of origin.***
[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

Justification

The EDPB can assist the Cooperation Group, the Commission and ENISA to factor in considerations regarding personal data in the risk assessments of supply chains. It is also important to emphasise ICT services, systems and products' requirements when such services, systems, and products originate form a third country.

Amendment 157
Evžen Tošenovský

Proposal for a directive
Recital 46

Text proposed by the Commission	*Amendment*
(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated ***sectoral*** supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21] , with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.	(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21] , with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities. ***Where appropriate, the Cooperation Group should monitor the supply chain risk assessment activities of other democratic countries.***
[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 158
Christophe Grudler, Klemen Grošelj, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer, Nathalie Loiseau

Proposal for a directive
Recital 47

Text proposed by the Commission	*Amendment*
(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU	(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.***	Toolbox on 5G cybersecurity agreed by the Cooperation Group.

Or. en

Justification

Moved to Article 19

Amendment 159
Evžen Tošenovský

Proposal for a directive
Recital 47

Text proposed by the Commission	*Amendment*
(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. ***To identify the supply chains that should be subject to a coordinated risk assessment, the following***	(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.

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.

Or. en

Amendment 160
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 47

Text proposed by the Commission	*Amendment*
(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical	(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.	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 ***across the entire lifecycle of the service, system or product*** and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities. ***Such risk assessments should identify best practices for managing risks associated with risks in the ICT supply chain and explore ways to further incentivise their wider adoption by entities within each sector under examination.***

Or. en

Amendment 161
Bart Groothuis, Iskra Mihaylova, Christophe Grudler, Martina Dlabajová

Proposal for a directive
Recital 48

Text proposed by the Commission	*Amendment*
(48) In order to streamline the legal obligations imposed on providers of public electronic communications networks or publicly available electronic communications services, and trust service providers related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities to benefit from the legal framework established by this Directive (including designation of CSIRT responsible for risk and incident handling, participation of competent authorities and bodies in the work of the Cooperation Group and the CSIRT network), they should be included in the scope of application of this Directive. The ***corresponding provisions laid down in Regulation (EU) No 910/2014 of the***	(48) In order to streamline the legal obligations imposed on providers of public electronic communications networks or publicly available electronic communications services, and trust service providers related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities to benefit from the legal framework established by this Directive (including designation of CSIRT responsible for risk and incident handling, participation of competent authorities and bodies in the work of the Cooperation Group and the CSIRT network), they should be included in the scope of application of this Directive. The rules on reporting obligations should be without prejudice to Regulation (EU)

European Parliament and of the Council[22] and Directive (EU) 2018/1972 of the European Parliament and of the Council[23] related to the imposition of security and notification requirement on these types of entities should therefore be repealed. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council[24] .	2016/679 and Directive 2002/58/EC of the European Parliament and of the Council[24] .
[22] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).	
[23] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).	
[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).	[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

Or. en

Justification

In order to avoid legal uncertainty, corresponding provision in Regulation No 910/2014 (eIDAS) should be repealed/amended in the revision of the Regulation itself.

Amendment 162
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 48

Text proposed by the Commission	*Amendment*
(48) In order to streamline the legal obligations imposed on providers of public electronic communications networks or publicly available electronic communications services, and trust service providers related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities to benefit from the legal framework established by this Directive (including designation of CSIRT responsible for risk and incident handling, participation of competent authorities and bodies in the work of the Cooperation Group and the CSIRT network), they should be included in the scope of application of this Directive. The corresponding provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council[22] and Directive (EU) 2018/1972 of the European Parliament and of the Council[23] related to the imposition of security and notification requirement on these types of entities should ***therefore be repealed***. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council[24] .	(48) In order to streamline the legal obligations imposed on providers of public electronic communications networks or publicly available electronic communications services, and trust service providers related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities to benefit from the legal framework established by this Directive (including designation of CSIRT responsible for risk and incident handling, participation of competent authorities and bodies in the work of the Cooperation Group and the CSIRT network), they should be included in the scope of application of this Directive. The corresponding provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council[22] and Directive (EU) 2018/1972 of the European Parliament and of the Council[23] related to the imposition of security and notification requirement on these types of entities should ***be complemented***. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council[24] .
[22] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).	[22] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).
[23] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).	[23] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).
[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July	[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July

2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).	2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

Or. en

Amendment 163
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Recital 48 a (new)

Text proposed by the Commission	*Amendment*
	(48a) The national regulatory authorities or other competent authorities responsible for public electronic communications networks or of publicly available electronic communications services pursuant to Directive (EU) 2018/1972 should be informed of significant incidents, cyber threats and near misses notified by providers of public electronic communications networks or publicly available electronic communications services and the measures taken in response to those risks and incidents.

Or. en

Amendment 164
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 50

Text proposed by the Commission	*Amendment*
(50) Given the growing importance of	(50) Given the growing importance of

number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security of network and information systems appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission.	number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security of network and information systems appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk ***to network security*** for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission. ***However, as the attack surface continues to expand, number-independent interpersonal communications services including, but not limited to, social media messengers, are becoming popular attack vectors. Malicious actors use platforms to communicate and attract victims to open compromised web pages, therefore increasing the likelihood of incidents involving the exploitation of personal data, and by extension, the security of information systems.***

Or. en

Justification

ENISA's Emerging Trends chapter of the Threat Landscape finds that malicious actors are now using other platforms to communicate and attract victims to open compromised web pages. Hence, despite the lower risk to network security from number-independent interpersonal communication services, the risk remains high for attacks to users.

Amendment 165
Tsvetelina Penkova

Proposal for a directive
Recital 50

Text proposed by the Commission	*Amendment*
(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security of network and information systems appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission.	(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements ***or used as means for meeting the requirements for risk management set under Article 18,*** in view of their specific nature***, technological pervasiveness*** and economic importance. Providers of such services should thus also ensure a level of security of network and information systems appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission.

Or. en

Amendment 166
Evžen Tošenovský

Proposal for a directive
Recital 50

Text proposed by the Commission	*Amendment*
(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic	(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic

importance. Providers of such services should thus also ensure a level of security of network and information systems appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services ***which make use of numbers and*** which do not exercise actual control over signal transmission.	importance. Providers of such services should thus also ensure a level of security of network and information systems appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to ***number-based*** interpersonal communications services which do not exercise actual control over signal transmission.
	Or. en

Amendment 167
Evžen Tošenovský

Proposal for a directive
Recital 51

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

Or. en

Amendment 168
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 51

Text proposed by the Commission	*Amendment*
(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents ***in relation thereto***.	(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report ***security*** incidents ***as in Article 2 (41) of the European Electronic Communications Code (EECC)***.

Or. en

Amendment 169
Rasmus Andresen
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	(53) ***Encryption is critical and irreplaceable for safeguarding the security of electronic communications networks and services data protection and privacy. Strong and state of the art encryption must be available to be used for mitigation of risks to network and***

communications, for instance by using specific types of software or encryption technologies.	***information security and for the rights and freedoms of individuals.*** 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 ***additional*** measures they can take to protect the security of their ***devices and*** communications, for instance by using specific types of software or encryption technologies. ***The approach to security through obscurity has its limitations, while the open cooperative models can provide relief and increase the security of hardware and software, therefore service providers and traders are encouraged to use open source and open hardware.***

Or. en

Justification

Strong and state of the art encryption is critical and irreplaceable for effective data protection and privacy.

Amendment 170
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 53

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

Or. en

Amendment 171
Rasmus Andresen
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 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 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 ***is without prejudice to*** 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. ***Such enforcement powers must always fully respect due process and other safeguards, as well as fundamental rights, in particular the right to respect for private life and communications and the right to the protection of personal data.*** Solutions for lawful access to information ***from*** end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime. ***Any actions taken have to carefully adhere to the principles of necessity, proportionality and subsidiarity and shall not lead to creating backdoors or weakening encryption, ensuring that the privacy and security of encrypted data, including in end-to-end encrypted communications is not compromised.***

Or. en

Justification

Paraphrasing the Council communication on Encryption

Amendment 172
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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 ***data-centric security techniques, such as*** encryption, ***tokenisation, segmentation, throttle access, marking, tagging, strong identity and access management, and automated access decisions***, should be promoted 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.

Or. en

Amendment 173
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
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. 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. The effectiveness of encryption in protecting ***the*** privacy and security of communications ***must not be undermined in any circumstance, as any loophole in encryption is open to be explored or exploited by actors, regardless of their legitimacy or intent***.

Or. en

Amendment 174
Evžen Tošenovský

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	(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, ***could*** be promoted and, where necessary, should be ***implemented by*** 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.	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.

Or. en

Amendment 175
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 54 a (new)

Text proposed by the Commission	*Amendment*
	(54a) Any measures 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 code, or monitoring of electronic communications outside clear legal authorities should be prohibited to ensure the effectiveness of the technology and its wider use. The cases where encryption can be used to mitigate risks related to non-compliant data transfers as presented in EDPB Recommendations 01/2020 may enable stronger encryption, whether in transit or

at rest, for providers of such services and networks for the purposes of Article 18.

Or. en

Amendment 176
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Recital 54 a (new)

Text proposed by the Commission	*Amendment*
	(54a) An incident should be typically considered significant by the competent authorities or the CSIRT if the incident has caused substantial operational disruption or financial losses for the entity concerned and the incident has affected other natural or legal persons by causing considerable material or non-material losses.

Or. en

Amendment 177
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 55

Text proposed by the Commission	*Amendment*
(55) This Directive lays down a ***two-stage*** approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual	(55) This Directive lays down a ***three-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.

companies and entire sectors. ***In this regard, the Directive should also include reporting of incidents that, based on an initial assessment performed by the entity, may be assumed to lead to substantial operational disruption or financial losses or affect other natural or legal persons by causing considerable material or non-material losses. The initial assessment should take into account amongst others, the affected network and information systems and, in particular, their importance in the provision of the entity's services, the severity and technical characteristics of the cyber threat, and any underlying vulnerabilities that are being exploited, as well as the entity's experience with similar incidents.*** Where entities become aware of an incident, they ***should provide an early warning within 24 hours, without any obligation to disclose additional information. Entities*** should be required to submit an initial notification within ***72*** hours, followed by a ***comprehensive*** report not later than one month after ***the incident has been handled. The initial incident notification timeline of 72 hours should not preclude entities from reporting incidents earlier, therefore allowing entities to seek support from competent authorities or CSIRTs swiftly, and enabling competent authorities or CSIRTs to mitigate the potential spread of the reported incident. Where an incident requires a longer period to be handled, an entity should be required to submit regular reports on the mitigation measures in place to contain, respond to, attribute and recover from the incident, and a comprehensive report not later than one month after the incident has been handled***. The initial notification should 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 ***72*** hours for the initial notification and one month for the ***comprehensive*** report.

Or. en

Justification

Aligning the notification timeline with the timeline provided in Regulation (EU) 2016/679 can harmonise the notification process and avoid double reporting in cases where the incident involves personal data. An early warning mechanism will allow entities to swiftly make competent authorities or CSIRTs aware of an incident, without that warning requiring entities to disclose additional information, hence enabling entities to invest resources in dealing with the incident and gain a better understanding of the incident in order to provide more detailed information to the competent authority of CSIRT in their initial notification.

Amendment 178
Eva Maydell, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 55

Text proposed by the Commission	*Amendment*
(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial	(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. ***In this regard, the Directive should also include reporting of incidents that, based on an***

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.

initial assessment performed by the entity, may be assumed to lead to substantial operational disruption or financial losses or affect other natural or legal persons by causing considerable material or non-material losses. The initial assessment should take into account amongst other, the affected network and information systems and in particular their importance in the provision of the entity's services, the severity and technical characteristics of the cyber threat, and any underlying vulnerabilities that are being exploited as well as the entity's experience with similar incidents. Where entities become aware of an incident, they should be required to submit an initial notification within ***72*** hours, followed by a report not later than ***three months*** 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. 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 ***72*** hours for the initial notification and ***three months*** for the report.

Or. en

Amendment 179
Evžen Tošenovský

Proposal for a directive
Recital 55

Text proposed by the Commission	*Amendment*
(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification ***within 24 hours***, followed by a final report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines ***of 24 hours for the initial notification and one month for the final report***.	(55) This Directive lays down a 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 ***significant*** incident, they should be required to submit an initial notification ***without undue delay***, 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 ***reporting*** deadlines.

Or. en

Amendment 180
Rasmus Andresen
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.	(59) Maintaining accurate and complete databases of domain names and registration data (so called 'WHOIS data') and providing lawful access to ***competent authorities for network and information security to*** such data ***may contribute to increased*** cybersecurity. Where processing includes personal data such processing shall comply with Union data protection law. ***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 with Directive 2002/58/EC on concerning the processing of personal data and the protection of privacy in the electronic communications sector, and is not modifying or adding to their provisions.***

Or. en

Justification

Clarifying the scope and extent.

Amendment 181
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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	(59) Maintaining accurate***, verified*** and complete databases of domain names and registration data (so called **"**WHOIS data**"**) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, ***so that third-***

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.

party rights could be protected and 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.

Or. en

Amendment 182
Rasmus Andresen
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.	(60) The availability and timely accessibility of data to public authorities, CERTs ***and*** CSIRTs ***can sometimes be useful*** to prevent and combat Domain Name System abuse, in particular to respond to cybersecurity incidents. Such access should comply with Union data protection law insofar as it is related to personal data.

Or. en

Justification

Change required for the scope alignment

Amendment 183
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez

Muñoz

Proposal for a directive
Recital 60

Text proposed by the Commission	*Amendment*
(60) The availability and timely accessibility of ***these*** data to ***public authorities, including*** competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs, ***(***CSIRTs, and as regards the data of their clients ***to*** providers of electronic communications networks and services and providers of cybersecurity technologies ***and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents***. Such access should comply with Union data protection law insofar as it is related to personal data.	(60) The availability and timely accessibility of ***the domain name registration*** data to ***legitimate access seekers is essential to protect the online ecosystem, prevent DNS abuse, detect and prevent crime and fraud, protect minors, protect intellectual property, and protect against hate speech. For the purposes of this Directive, legitimate access seekers are natural or legal persons making a justified request on the basis of a legitimate interest under Union or national law to access DNS data, and they may include*** 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**,** providers of electronic communications networks and services and providers of cybersecurity technologies. Such access should comply with Union data protection law insofar as it is related to personal data.

Or. en

Amendment 184
Rasmus Andresen
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	(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.

registrars) 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 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.

Or. en

Justification

Changed the language to underline that NIS2 is not a sectorial regulation for TLDs

Amendment 185
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 61

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

Or. en

Amendment 186
Rasmus Andresen
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 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.	***deleted***

[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

Justification

This recital falls outside the scope of a cybersecurity act.

Amendment 187
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 62

Text proposed by the Commission	*Amendment*
(62) TLD registries and ***the*** entities providing domain name registration services ***for them*** should make publically available domain name registration data ***that fall outside the scope of Union data protection rules, such as data that concern*** legal persons[25] . TLD registries and ***the*** entities providing domain name registration services ***for the TLD*** should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that TLD registries and ***the*** entities providing domain name registration services ***for them*** should respond ***without undue delay*** to requests from legitimate access seekers for the disclosure of domain	(62) TLD registries and entities providing domain name registration services should ***be required to*** make publically available domain name registration data ***of*** legal persons[25]. TLD registries and entities providing domain name registration services should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that TLD registries and entities providing domain name registration services should respond ***within 72 hours*** to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and entities providing domain name registration services should establish

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.

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".

[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 188
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Nicola Danti, Christophe Grudler

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	(63) All essential and important entities under this Directive should fall under the jurisdiction of the Member State where they provide their services ***or carry out their activities***. If the entity provides services in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of these

authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions.	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.

Or. en

Justification

This directive applies to both entities that provide services as to entities which manufacture or carry out activities related to any stage of production, processing and distribution of food, as indicated in the Annexes.

Amendment 189
Evžen Tošenovský

Proposal for a directive
Recital 64

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

determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment ***with the highest number of employees*** in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.

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

Or. en

Amendment 190
Evžen Tošenovský

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	(65) In cases where a DNS service provider, TLD name registry, content delivery network provider, cloud computing service provider, data centre service provider***,*** digital provider ***and provider of number-independent interpersonal communications services*** 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

address and of other contact details, or 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.

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 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 191
Rasmus Andresen
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	(65) In cases where a 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

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 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.

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 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

Justification

In line with keeping NIS2 a general framework and avoiding sectorial regulation.

Amendment 192
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Recital 68

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

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

Or. en

Amendment 193
Rasmus Andresen
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 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,***	(69) The processing of personal data, ***which should be limited to what is*** strictly necessary and proportionate for the purposes of ensuring network and information security 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.

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

Justification

Aligning the text with GDPR recital 49 without adding to and indirectly modifying it.

Amendment 194
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

Proposal for a directive
Recital 69

Text proposed by the Commission	*Amendment*
(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, ***public authorities,*** CERTs***, CSIRTs, and providers of security technologies and services*** should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, uniform resources locators (URLs), domain names,	(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, CERTs should constitute a legitimate interest of the data controller concerned, as referred to in Regulation ***(EU) 2016/679 and by public authorities, namely competent authorities, Single Points Of Contact (SPOCs), CSIRTs, NIS CG, CSIRT Network, CERTs and CYCLONe should constitute a legal obligation or the public interest or the exercise of official authority 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,

and email addresses.	tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, ***telephone numbers, bank account numbers, geolocation data, payment data,*** uniform resources locators (URLs), domain names, and email addresses.

Or. en

Amendment 195
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 69

Text proposed by the Commission	*Amendment*
(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services ***should constitute*** a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, uniform	(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by ***essential and important*** entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services ***is necessary to comply with a legal obligation under this Directive and constitutes*** a legitimate interest of the data controller concerned, as referred to in ***point (c) paragraph 1, and point (f) paragraph 1 respectively of Article 6 of*** Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures,

resources locators (URLs), domain names, and email addresses.	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

Justification

A clear legal basis is necessary for the processing of personal data for cybersecurity related purposes. The legal basis of legitimate interest as prescribed in Article 6(1)(f) of Regulation (EU) 2016/679 should underpin information-arrangements, whereas the legal basis of compliance with a legal obligation as prescribed in Article 6(1)(c) of Regulation (EU) 2016/679 should underpin the cybersecurity risk-management measures, reporting obligations and the provisions laid out in Article 23 of this Directive.

Amendment 196
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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,	(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***, identification, containment***, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and

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***.	procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of personal data.

Or. en

Amendment 197
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 70

Text proposed by the Commission	*Amendment*
(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to ensuring a fair balance of obligations for both entities and competent authorities. Thus, essential entities should be subject to a fully-fledged supervisory regime (ex-ante and ex-post), while important entities should be subject to a light supervisory regime, ex-post only. For the latter, this means that important entities should not document systematically compliance with cybersecurity risk management requirements, while competent authorities should implement a reactive ex -post approach to supervision and, hence, not have a general obligation to supervise those entities.	(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities***. The supervisory regime shall, amongst other issues, verify that essential and important entities take appropriate technical and organisational measures to manage the risks posed to the security of network and information systems by implementing basic computer hygiene practices such as software updates, device configuration, network segmentation, identity and access management or user awareness and training regarding corporate email cyber threats, phishing or social engineering techniques***. 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.

Or. en

Amendment 198
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 71

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

process.

Or. en

Amendment 199
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 71

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

Or. en

Justification

Administrative sanctions stemming from breaches of cybersecurity risk management and

reporting obligations of entities should target actual damages or losses rather than potential damages or losses that could have been triggered.

Amendment 200
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 72

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

Or. en

Amendment 201
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Recital 76

Text proposed by the Commission	*Amendment*
(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of ***the*** suspension of a certification or authorisation concerning part or all the services provided by an essential entity and the imposition of a temporary ***ban from the exercise of*** managerial functions ***by a natural person***. Given their severity and impact on the	(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of***, where applicable, the temporary*** suspension of a certification or authorisation concerning part or all the services provided by an essential entity**,** and the imposition of a temporary ***against any person discharging managerial responsibilities at chief executive officer***

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

or legal representative level in that essential entity from exercising managerial functions ***in that entity. This provision shall not apply to public administration entities as referred to in this Directive***. Given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection, due process, presumption of innocence and right of defence.

Or. en

Amendment 202
Evžen Tošenovský

Proposal for a directive
Recital 76

Text proposed by the Commission	*Amendment*
(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of	(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of

obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning ***part or all the*** services provided by an essential entity ***and the imposition of a temporary ban from the exercise of managerial functions by a natural person***. Given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection, due process, presumption of innocence and right of defence.	obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning services provided by an essential entity. Given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection, due process, presumption of innocence and right of defence.

Or. en

Amendment 203
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Recital 76

Text proposed by the Commission	*Amendment*

(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity ***and the imposition of a temporary ban from the exercise of managerial functions by a natural person***. Given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection, due process, presumption of innocence and right of defence.	(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity. Given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection, due process, presumption of innocence and right of defence.

Or. en

Amendment 204
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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.	***deleted***

Or. en

Amendment 205
Rasmus Andresen
on behalf of the Greens/EFA Group

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 ***independent*** experts designated by the Member States***,*** of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources. ***When deciding on the methodology, the Commission, supported by ENISA, should establish an objective, non-discriminatory, technology neutral, fair and transparent system for the selection of such experts.***

Or. en

Justification

In order to ensure an objective view, the procedure should be transparent and the experts independent.

Amendment 206
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez

Muñoz

Proposal for a directive
Recital 79

Text proposed by the Commission	*Amendment*
(79) A peer-review mechanism should be introduced, allowing the assessment by experts designated by the Member States of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources.	(79) A peer-review mechanism should be introduced, allowing the assessment by experts designated by the Member States ***and ENISA*** of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources***, and provide an effective path for the transfer of cybersecurity-enhancing technologies, mechanisms and processes between and among competent authorities or CSIRTs***.

Or. en

Justification

The peer-review process laid out in Article 16 of the Directive can enable mature CSIRTs to transfer cybersecurity technology and related polices, controls and practices to Member States' competent authorities and CSIRTs under review leading not only to better cooperation but also more harmonious development of capabilities and expertise from this process.

Amendment 207
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Recital 80

Text proposed by the Commission	*Amendment*
(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should also be empowered to adopt delegated acts establishing which categories of essential entities shall be	***deleted***

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

---

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

Or. en

Amendment 208
Tsvetelina Penkova

Proposal for a directive
Recital 80

Text proposed by the Commission	*Amendment*
(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should also be empowered to ***adopt delegated acts*** establishing which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. It is of particular importance that	(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should also be empowered to ***initiate legislative proposals under Article 114 TFEU*** establishing which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. It is of particular

the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[26] . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.	importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[26]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.
[26] OJ L 123, 12.5.2016, p. 1.	[26] OJ L 123, 12.5.2016, p. 1.

Or. en

Justification

The suggested amendment is necessary as to ensure that the legal coherence is preserved with the existing EU acquis. Formally requiring specific sectors or products, services or processes to undergo certification introduces a mandatory requirement, which is inconsistent with Regulation 2019/881/EC ("The Cybersecurity Act") and the provisions that govern the EU certification framework under Article 56(2) and Article 56(3). The latter unambiguously stipulates that the certification is voluntary, unless "otherwise specified by Union or Member State law".

Amendment 209
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	(aa) establishes framework for cooperation among Member States;

Or. en

Amendment 210

Evžen Tošenovský

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 ***obligation on Member States to introduce*** 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;

Or. en

Amendment 211
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(c) lays down obligations on cybersecurity information sharing**.**	(c) lays down obligations on ***Member States to facilitate the*** cybersecurity information sharing***;***

Or. en

Amendment 212
Evžen Tošenovský

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

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

Or. en

Amendment 213
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

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***, including ICT suppliers providing products and services for critical functions performed by essential or important entities. This Directive does not apply to entities regarded by Member States as non-critical***. This Directive does not apply to entities that qualify as micro and small 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. fr

Amendment 214
Rasmus Andresen
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	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]	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

Justification

Although security needs to be raised everywhere, the adding too much requirements on non-commercial free and open source projects could have a chilling effect.

Amendment 215
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Nicola Danti, Christophe Grudler

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 ***that provide their services or carry out their activities within the Union***. This Directive does not apply to entities that qualify as micro and small 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

Justification

To clarify that the directive applies to entities active within the EU.

Amendment 216
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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 ***in so far as they carry out in-scope activities within the Union***. This Directive does not apply to entities that qualify as micro and small 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

Justification

This Directive applies only to entities which are active within the EU.

Amendment 217
François-Xavier Bellamy

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***, including manufacturers and providers of ICT products***. This Directive does not apply to entities that qualify as micro and small 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 218
Evžen Tošenovský

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 in Annex I and Annex II. ***Without prejudice to paragraph 2 of this Article and Article 27,*** this Directive does not apply to entities that qualify as micro and small 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 219
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
2. ***However***, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:	2. ***By way of derogation from paragraph 1 of this Article***, regardless of their size, this Directive also applies to entities ***of a type*** referred to in Annexes I and II, where:

Or. en

Amendment 220
Rasmus Andresen
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 221
Marisa Matias, Sira Rego, Sandra Pereira, Giorgos Georgiou, Manuel Bompard

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

Text proposed by the Commission	*Amendment*
(d) a potential disruption of the service	(d) a potential disruption of the service

provided by the entity could have ***an impact on*** public ***safety, public*** security or public ***health***;	provided by the entity could have ***repercussions on the provision of*** public ***services, particularly health, education, transport*** security or public ***order***;

Or. en

Amendment 222
Rasmus Andresen
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 223
Rasmus Andresen
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 224
Marisa Matias, Sira Rego, Cornelia Ernst, Manuel Bompard

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

Text proposed by the Commission	*Amendment*
	(fa) the entity is critical for the provision of services in insular, remote or unpopulated areas;

Or. en

Amendment 225
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
	2a. Member States shall ensure that all entities falling under the scope of this Directive comply with this Directive as important entities. Member States may decide which important entities shall be designated as essential entities, taking into account particularly whether the entities had already been identified as the operators of essential services pursuant to Article 5 of NIS Directive (2016/1148) and prioritisation of the sectors and subsectors with higher level of criticality listed in Annex I.
	Member States shall by [transposition deadline] establish an initial list of essential and important entities, which should comply with this Directive and review it, on a regular basis, and, where

appropriate, update it.

Member States shall set a deadline for initial self-notification or identification by the competent authority and compliance with this Directive for the entities falling under the scope of this Directive not exceeding [6 months after the transposition deadline]. The entities which had been already identified as the operators of essential services pursuant to Article 5 of NIS Directive (2016/1148) shall comply with this Directive by [transposition deadline].

The entities shall submit at least the following information: the name of the entity, address and up-to-date contact details, including email addresses and telephone numbers, and relevant sector(s) and subsector(s) referred to in Annexes I and II. The entities shall without undue delay notify any changes to the details they submitted, and in any event, within two weeks from the date on which the change took effect.

Or. en

Amendment 226
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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

Text proposed by the Commission	*Amendment*
	2a. This Directive applies only to manufacturing facilities of important and essential entities listed in Annexes I and II that are located within the Union.

Or. en

Amendment 227
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
	2b. The entities referred to in Article 24(1) shall submit the self-notifications in the Member State in which they have their main establishment.
	Apart from information referred to in the third subparagraph of paragraph 2a of this Article, they shall notify the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 24(3) and the Member States where the entity provides services.
	Where an entity referred to in paragraph 1 has besides its main establishment in the Union further establishments or provides services in other Member States, the single contact point of the main establishment shall without undue delay forward the information to the single points of contact of those Member States.
	Where an entity fails to notify or to provide the relevant information on Member States concerned within the deadline set out by the Member State of its main establishment, any Member State where the entity provides services shall be competent to ensure that entity's compliance with the obligations laid down in this Directive.

Or. en

Amendment 228
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
	2c. By [6 months after the transposition deadline] and every 12 months thereafter, Member States shall submit to the Cooperation Group and for the purpose of the review referred to in Article 35 to the Commission the information necessary to enable to assess the consistency of Member States' approaches to the identification of essential and important services. That information shall include at least the number of all essential and important entities identified for each sector and subsector referred to in Annexes I and II, including number of small and micro enterprises in each category;

Or. en

Amendment 229
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 2 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. Member States shall ensure that the network and information systems used by their public administration entities are subject to their national cybersecurity regulation.

Or. en

Amendment 230
Rasmus Andresen
on behalf of the Greens/EFA Group

Proposal for a directive
Article 2 – paragraph 4

Text proposed by the Commission	*Amendment*
4. This Directive applies without prejudice to Council Directive 2008/114/EC[30] and Directives 2011/93/EU[31] and 2013/40/EU[32] of the European Parliament and of the Council.	4. This Directive applies without prejudice to Council Directive 2008/114/EC[30] and Directives 2011/93/EU[31] and 2013/40/EU[32] ***and 2002/58/EC[1a] and Regulation (EU) 2016/679[1b]*** of the European Parliament and of the Council.
[30] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).	[30] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).
[31] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).	[31] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).
[32] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).	[32] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

Or. en

(1a Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector1b 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)

Justification

Completing the relevant list of provisions

Amendment 231
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez

Muñoz

Proposal for a directive
Article 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 the extent 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, that processing is considered necessary for compliance with a legal obligation in accordance with paragraph1(c) of Article 6 of Regulation (EU) 2016/679.

Or. en

Justification

Clarifying 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 232
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

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

Text proposed by the Commission	*Amendment*
	5a. To fulfil the tasks set out in this Directive, competent authorities and CSIRTs shall process personal data,

including the data referred to in Article 9 of the Regulation (EU) 2016/679, and shall process information that is confidential pursuant to Union and national rules, for the purposes and to the extent strictly necessary to fulfil these tasks.

Or. en

Amendment 233
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*
	5b. For the purposes of arrangements underpinning cybersecurity information-sharing and voluntary notification of information as set out in Articles 26 and 27 of this Directive, the processing of personal data constitutes a legitimate interest of the data controller concerned in accordance with paragraph 1(f) of Article 6 of Regulation (EU) 2016/679.

Or. en

Justification

Clarifying legal basis under Regulation (EU) 2016/679 for the processing of personal data where there is a legitimate interest.

Amendment 234
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

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

Text proposed by the Commission	*Amendment*

5b. To fulfil the tasks set out in this Directive, SPOCs, the Cooperation Group, the CSIRT Network and CyCLONe shall process personal data and information that is confidential pursuant to Union and national rules, for the purposes and to the extent strictly necessary to fulfil these tasks.

Or. en

Amendment 235
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*
	5c. As regards the processing of personal data from essential entities providing services of public electronic communications networks or publicly available electronic communications referred to in point 8 of Annex I and point (a)(i) of paragraph2(1), such processing of personal data required for the purposes of ensuring network and information security shall be in compliance with the provisions set out in Directive 2002/58/EC.

Or. en

Justification

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

Amendment 236
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

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

Text proposed by the Commission	*Amendment*
	5c. When processing the personal data referred to in Article 9 of the Regulation (EU) 2016/679, competent authorities and CSIRTs shall conduct the risk analyses, introduce proper safeguards and procedures to exchange information.

Or. en

Amendment 237
Christophe Grudler, Klemen Grošelj, Nathalie Loiseau, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

Proposal for a directive
Article 2 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.	6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply. ***The Commission shall issue guidelines in relation to the implementation of the sector–specific acts of Union law in order to ensure that security requirements established by this Directive are met by those acts. When preparing those guidelines, the Commission shall take into account ENISA and the Cooperation Group best practices and expertise.***

Or. en

Justification

To ensure that implementation of lex specialis is done in a way that respects the minimum security requirements defined and established by the NIS directive, the Commission shall issue guidelines for the implementation of the sector-specific acts. Best practices collected by ENISA and the NIS cooperation group should be taken into account in the preparation of these guidelines

Amendment 238
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 2 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.	6. ***Sector-specific acts that require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, shall, where possible, refer to the definitions in Article 4 of this Directive.*** Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.

Or. en

Amendment 239
Tsvetelina Penkova

Proposal for a directive
Article 2 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.	6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, ***including with regards to the competence and obligations of the supervisory authority,*** the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.

Or. en

Amendment 240
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

Proposal for a directive
Article 2 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Where provisions of sector–specific acts of Union law require essential or important entities ***either*** to adopt cybersecurity risk management measures ***or*** to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.	6. Where provisions of sector–specific acts of Union law require essential or important entities to adopt cybersecurity risk management measures ***and*** to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.

Or. en

Amendment 241
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

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

Text proposed by the Commission	*Amendment*
	6a. Sector-specific acts of Union law referred to in paragraph 6 should at minimum include:
	(a) cybersecurity risk management measures as laid down in Article 18 (1) and (2); and
	(b) requirements to notify incidents and significant cyber threats as laid down in Article 20 (1- 4)

Or. en

Amendment 242
Evžen Tošenovský

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

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

Or. en

Amendment 243
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*

	(4a) 'near miss' means an event which could have caused harm, but was successfully prevented from fully transpiring;

Or. en

Justification

Moved from Recitals.

Amendment 244
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 4 – paragraph 1 – point 5

Text proposed by the Commission	*Amendment*
(5) 'incident' means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems;	(5) 'incident' means any ***unwanted or unexpected*** event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems;

Or. en

Amendment 245
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

Proposal for a directive
Article 4 – paragraph 1 – point 5 – point i (new)

Text proposed by the Commission	*Amendment*
	(i) by way of derogation 'security incident' as defined in Article 2(41) of Directive (EU) 2018/1972 remains applicable for interpersonal electronic communications service providers.

Or. en

Justification

The definition of security incident as in EECC has been recently transposed in national law and repealing it with this Directive may be premature. There is a need for further assessment the impact of repealing the definition.

Amendment 246
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 4 – paragraph 1 – point 5 a (new)

Text proposed by the Commission	*Amendment*
	(5a) 'near miss' means any event which could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems, but was successfully prevented from fully transpiring;

Or. en

Amendment 247
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

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

Or. en

Amendment 248
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

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

Or. en

Justification

Moved from Recitals.

Amendment 249
Rasmus Andresen
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

Justification

Aligning the text with the changes to the scope

Amendment 250
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

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

Or. en

Justification

The DNS does not allow end-users to reach services and resources on the internet. Rather, it allows end-users to look up those services and resources enabling their devices to communicate with those services and resources over the Internet. The DNS merely provides identification of services and resources; reachability of those services and resources depends on internet routing and connectivity services.

Amendment 251
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Christophe Grudler, Martina Dlabajová

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

Text proposed by the Commission	*Amendment*
(13) 'domain name system (DNS)' means a hierarchical distributed naming system which ***allows end-users to reach***	(13) 'domain name system (DNS)' means a hierarchical***,*** distributed naming system which ***is used to identify Internet***

services and resources ***on the*** internet***;***	services and resources***, allowing end user devices to make use of*** Internet ***routing and connectivity services to reach those services and resources.***

Or. en

Amendment 252
Rasmus Andresen
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

Justification

Aligning the text with the changes to the scope

Amendment 253
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 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***;	(14) 'DNS service provider' means an entity that provides***: a) open and public*** recursive ***domain name resolution services; or b)*** authoritative domain name resolution services ***as a*** service ***procurable by third-party entities***;

Or. en

Justification

Differentiating between the resolution sides of the DNS is essential to include in scope the necessary services and excluding the root name servers. Excluding those from the scope if essential to maintain and open internet and avoid risks of fragmentation and risks of extra-territorial application of the Directive.

Amendment 254
Rasmus Andresen
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 255
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*

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

Or. en

Justification

Many top-level domain name registries outsource the technical operation of their TLD. Thus, it is more appropriate to not imply such outsourcing excludes the entity from being a top-level domain name registry.

Amendment 256
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*
	(15a) ‘legitimate access seekers’ means any natural or legal person, including competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CSIRTs, CERTs, providers of electronic communications networks and services, and providers of cybersecurity technologies and services, seeking DNS data upon a justified request on the basis of Union or national law for the purposes of preventing DNS abuse, detecting and preventing crime and fraud, protecting minors, protecting intellectual property, and protecting against hate speech;

Or. en

Amendment 257
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 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***)***;	(22) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other ***via number-independent interpersonal communications services*** across multiple devices, and in particular, via chats, posts, videos and recommendations;

Or. en

Amendment 258
Tsvetelina Penkova

Proposal for a directive
Article 4 – paragraph 1 – point 22 a (new)

Text proposed by the Commission	*Amendment*
	(22a) 'compromise assessment' is an objective inspection by a qualified entity of a network and its devices to discover unknown security breaches and ongoing or past intrusions, signs of indicators of compromise, unauthorised access, malware, and to assess risks by identifying weaknesses in the security architecture, vulnerabilities, improper usage or policy violations and system security misconfigurations;

Or. en

Amendment 259
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
(23) 'public administration entity' means an entity in a Member State that complies with the following criteria:	***deleted***
(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 has legal personality;	
(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;	
(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, goods, services or capital.	
Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded.	

Or. en

Amendment 260
Marisa Matias, Sira Rego, Cornelia Ernst, Manuel Bompard

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 ***has legal personality and*** complies with ***some of*** the following criteria:

Or. en

Amendment 261
Marisa Matias, Sira Rego, Cornelia Ernst, Manuel Bompard

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 262
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

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

Or. en

Amendment 263
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

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

Or. en

Amendment 264
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
	(23c) 'number-based interpersonal communications service' means a number-based interpersonal communications service as defined in point (6) of Article 2 of Directive (EU) 2018/1972;

Or. en

Amendment 265
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
	(23d) 'number-independent interpersonal communications service' means a number-independent interpersonal communications service as defined in point (7) of Article 2 of Directive (EU) 2018/1972;

Or. en

Amendment 266
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 4 – paragraph 1 – point 25

Text proposed by the Commission	*Amendment*
(25) 'essential entity' means any entity of a type referred to as an essential entity ***in Annex I***;	(25) 'essential entity' means any entity of a type referred to ***in Annex I and II, designated by the Member State*** as an essential entity;

Or. en

Amendment 267
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 4 – paragraph 1 – point 26

Text proposed by the Commission	*Amendment*
(26) 'important entity' means any entity of a type referred to ***as an important entity*** in Annex ***II.***	(26) 'important entity' means any entity of a type referred to in Annex ***I and II, unless exempted from the scope of this Directive or designated by the Member State as an essential entity;***

Or. en

Amendment 268
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 4 – paragraph 1 – point 26 a (new)

Text proposed by the Commission	*Amendment*
	(26a) 'non-critical entity' means any entity of a type referred to in Annex I and Annex II which, regardless of its size and resources, has no critical function within

a specific sector or type of service and is not highly dependent on other sectors or types of service;

Or. fr

Amendment 269
Evžen Tošenovský

Proposal for a directive
Article 4 – paragraph 1 – point 26 a (new)

Text proposed by the Commission	*Amendment*
	(26a) 'service' means any activity referred to in Annexes I and II provided for essential, important or other public or private entities or consumers, including provision of electronic communication networks and manufacture;

Or. en

Amendment 270
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

Proposal for a directive
Article 4 – paragraph 1 – point 26 b (new)

Text proposed by the Commission	*Amendment*
	(26b) 'critical function' means a network and information system function of an essential or important entity in connection with which disruption to availability, integrity, authenticity and confidentiality will result in a significant failure or deterioration of the functionality of the services provided by the critical or important entity concerned;

Or. fr

Amendment 271
Patrizia Toia

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

Text proposed by the Commission	*Amendment*
1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:	1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity ***and taking into account each sector specificities in terms of cyber risk management and resilience***. The national cybersecurity strategy shall include, in particular, the following:

Or. en

Amendment 272
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*
1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives ***and*** appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:	1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives***, the required technical, organisational, and financial resources to achieve those objectives, and the*** appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:

Or. en

Amendment 273

Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of ***cybersecurity***. The national cybersecurity strategy shall include, in particular, the following:	1. Each Member State shall adopt a national cybersecurity strategy***, a coherent framework*** defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of ***security of network and information systems in that Member State***. The national cybersecurity strategy shall include, in particular, the following:

Or. en

Amendment 274
François-Xavier Bellamy

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

Text proposed by the Commission	*Amendment*
1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:	1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity***, and strengthening the Union's strategic autonomy***. The national cybersecurity strategy shall include, in particular, the following:

Or. en

Amendment 275
Patrizia Toia

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

Text proposed by the Commission	*Amendment*
(a) a definition of objectives and priorities of the Member States' strategy on cybersecurity;	(a) a definition of objectives and priorities of the Member States' strategy on cybersecurity ***for each sector covered by this Directive***;

Or. en

Amendment 276
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

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

Text proposed by the Commission	*Amendment*
(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of public bodies and entities as well as other relevant actors;	(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of public bodies and entities as well as other relevant actors***, in particular those with responsibility for specific support for SMEs. The governance framework shall clearly lay down the organisational arrangements for cooperation and coordination between the national competent authorities designated under this Directive, taking account of their specific national circumstances***;

Or. fr

Amendment 277
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*

(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 ***and*** the roles and responsibilities of public bodies and entities as well as other relevant actors;	(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2***, and an appropriate framework defining*** the roles and responsibilities of public bodies and entities as well as other relevant actors***, underpinning the cooperation and coordination, at the national level, between the competent authorities designated under Articles 7(1) and 8(1), the single point of contact designated under Article 8(3), and the CSIRTs designated under Article 9***;

Or. en

Amendment 278
Christophe Grudler, Klemen Grošelj, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

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

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

Or. en

Justification

Moved to Article 5, paragraph 1, point b a (new)

Amendment 279
Christophe Grudler, Klemen Grošelj, Nathalie Loiseau, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

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

Text proposed by the Commission	*Amendment*
	(ba) a framework for allocating the roles and responsibilities of public bodies and entities as well as other relevant actors, including the organisation of the cooperation at the national level, between the competent authorities designated under Article 7(1) and Article 8(1), the single point of contact designated under Article 8(3), and CSIRTs designated under Article 9;

Or. en

Justification

The organisation of the cooperation between the different actors should be clearly defined in the national cybersecurity strategy.

Amendment 280
Rasmus Andresen
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 281

Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

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

Text proposed by the Commission	*Amendment*
(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;	(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy***, taking steps to establish a single cybersecurity point of contact for SMEs in order to support them in implementing specific cybersecurity measures***;

Or. fr

Amendment 282
Marisa Matias, Sira Rego, Cornelia Ernst, Sandra Pereira, Giorgos Georgiou, Manuel Bompard

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

Text proposed by the Commission	*Amendment*
(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;	(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy***, including trade unions and other focused on workers' protection***;

Or. en

Amendment 283
Evžen Tošenovský

Proposal for a directive
Article 5 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. ***As part*** of the national cybersecurity strategy, Member States shall in particular ***adopt*** the following policies:	2. ***In the framework*** of the national cybersecurity strategy, Member States shall in particular ***address*** the following policies:

Or. en

Amendment 284
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*
	(aa) guidelines addressing cybersecurity in the supply chain for ICT products and services used by entities outside the scope of this Directive, and in particular supply chain challenges faced by SMEs;

Or. en

Amendment 285
Rasmus Andresen
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 286
Rasmus Andresen
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 287
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*
	(da) a policy on promoting the integration of open-source tools and applications;

Or. en

Amendment 288
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*

	(db) a policy to promote and support the development and integration of AI and other emerging technologies in cybersecurity-enhancing tools and applications;

Or. en

Amendment 289
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*
(e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives;	(e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives***, including targeted policies addressing issues relating to gender representation and balance in the aforementioned areas***;

Or. en

Amendment 290
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*
	(ea) a policy to promote cyber hygiene programmes comprising a baseline set of practices and controls;

Or. en

Amendment 291
Rasmus Andresen
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

Justification

Education needs special attention but also support.

Amendment 292
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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 ***and enhance*** cybersecurity tools and secure network infrastructure;

Or. en

Amendment 293
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova

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

Text proposed by the Commission	*Amendment*

(fa) a policy, including relevant procedures and governance frameworks, to support and promote the establishment of cybersecurity PPPs;

Or. en

Amendment 294
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera, Markus Pieper

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

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

Or. en

Amendment 295
Marisa Matias, Sira Rego, Cornelia Ernst, Sandra Pereira, Giorgos Georgiou, Manuel Bompard

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

Text proposed by the Commission	*Amendment*
	(ha) a policy for cyber hygiene, and protection and training of workers against these new labour risks and threats.

Or. en

Amendment 296
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera, Markus Pieper

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

Text proposed by the Commission	*Amendment*
	(ha) a policy raising awareness for cybersecurity threats and best practices among the general population.

Or. en

Amendment 297
Marisa Matias, Sira Rego, Cornelia Ernst, Sandra Pereira, Giorgos Georgiou, Manuel Bompard

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

Text proposed by the Commission	*Amendment*
	(hb) a policy for addressing awareness and security of consumers of digital services.

Or. en

Amendment 298
Marisa Matias, Sira Rego, Cornelia Ernst, Manuel Bompard

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

Text proposed by the Commission	*Amendment*
	(hc) an evaluation of the proper harmonisation between this Directive and the General Date Protection Regulation.

Or. en

Amendment 299
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Nicola Danti, Christophe Grudler,

Martina Dlabajová

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

Text proposed by the Commission	*Amendment*
	2a. A policy to help authorities build awareness and understanding of the security considerations needed to design, build, and manage connected places.

Or. en

Justification

Connected places (i.e. smart cities) and their underlying infrastructure should become more resilient against cyberattacks.

Amendment 300
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Nicola Danti, Christophe Grudler, Martina Dlabajová

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

Text proposed by the Commission	*Amendment*
	2b. A policy specifically addressing the ransomware threat and disrupting the ransomware business model.

Or. en

Justification

Member States should raise awareness and take action to combat the rapidly increasing and evolving ransomware pandemic.

Amendment 301
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive

Article 5 – paragraph 3

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

Or. en

Amendment 302
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 5 – paragraph 4

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

Or. en

Amendment 303
Patrizia Toia

Proposal for a directive
Article 5 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall ***assist*** Member States***, upon request, in*** the development of a national strategy and of key performance indicators for the assessment of the strategy.	4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) ***and the EU competent authorities for each sector*** shall ***define guidelines to*** Member States ***for*** the development of a national strategy and of key performance indicators for the assessment of the strategy.

Or. en

Amendment 304
Eva Maydell, Massimiliano Salini

Proposal for a directive
Article 5 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. While implementing this Directive, Member States shall enforce EU guidance in order to ensure harmonisation at EU level, also by defining a homogeneous set of cybersecurity rules for new players that could enter in the European market;

Or. en

Amendment 305
Evžen Tošenovský

Proposal for a directive
Article 6 – title

Text proposed by the Commission	*Amendment*

Coordinated vulnerability disclosure and a European vulnerability ***registry***	Coordinated vulnerability disclosure and a European vulnerability ***database***

Or. en

Amendment 306
Evžen Tošenovský

Proposal for a directive
Article 6 – paragraph 1

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

Or. en

Amendment 307
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

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	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***.	essential entities and their suppliers of network and information systems to disclose and register ***only those*** vulnerabilities present in ICT products or ICT services ***which can be mitigated***, 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**,** the severity of the vulnerability in terms of the circumstances under which it may be exploited, ***and*** related patches**.** In the absence of available patches, ***ENISA should not disclose the vulnerability and should set manufacturers or suppliers*** of ***ICT products or services a deadline for providing reliable mitigation. Where several actors are affected by the same vulnerability, ENISA should coordinate the mitigation patch installation schedule***.
	Or. fr

Amendment 308
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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	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 ***only those*** vulnerabilities present in ICT products or ICT services ***that have a mitigation available*** , as well as to provide access to the information on vulnerabilities contained in the registry to all interested

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.	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. ***When several users are affected by the same vulnerability, ENISA should coordinate the schedule of the installation of the mitigation patches.***

Or. en

Amendment 309
Rasmus Andresen
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 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	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.	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

Justification

Due to the need to ensure fast reaction times, automatisation needs to be favoured.

Amendment 310
François-Xavier Bellamy

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***	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, ***ENISA should not disclose the vulnerability and impose a deadline to manufacturers or providers of ICT*** products ***or ICT*** services

mitigated.	***to provide a reliable mitigation. When several players are affected by the same vulnerability, ENISA should coordinate the schedule of the installation of the mitigation patches***.

Or. en

Amendment 311
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 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***, and the necessary technical and organisational measures to ensure the security and integrity of the registry,*** with a view in particular to enabling important and essential entities and their suppliers of network and information systems***, as well as entities excluded from the scope of this Directive, and their suppliers,*** 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***, enabling all parties and in particular, the users of the ICT products or ICT services concerned to adopt appropriate mitigating measures***. 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, ***and*** the availability of related patches.

Or. en

Justification

ENISA to adopt the required policies and controls to ensure the security and integrity of the coordinated vulnerability registry.

Amendment 312
Evžen Tošenovský

Proposal for a directive
Article 6 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the ***registry*** to all interested parties. The ***registry*** shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.	2. ENISA shall develop and maintain a European vulnerability ***database leveraging the global Common Vulnerabilities and Exposures (CVE)*** 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 ***voluntarily*** 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 ***database*** to all interested parties. The ***database*** shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches 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 313
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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

Text proposed by the Commission	*Amendment*
	2a. ENISA shall establish a structured cooperation agreements with Common Vulnerability and Exposure registry or other similar registries.

Or. en

Amendment 314
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*
	1a. Where a Member State designates more than one competent authorities referred to in paragraph1, it should clearly indicate which of these competent authorities shall serve as the main point of contact for the management of large-scale incidents and crises.

Or. en

Amendment 315
Evžen Tošenovský

Proposal for a directive
Article 7 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
3. Each Member State shall adopt a national cybersecurity incident and crisis	3. Each Member State shall adopt a national cybersecurity incident and crisis

response plan where objectives and modalities in the management of large-scale cybersecurity incidents and crises are set out. The plan ***shall lay down,*** in particular***,*** the following:	response plan where objectives and modalities in the management of large-scale cybersecurity incidents and crises are set out. ***Member States shall consider inclusion in*** the plan in particular ***of*** the following ***points***:

Or. en

Amendment 316
Evžen Tošenovský

Proposal for a directive
Article 7 – paragraph 4

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

Or. en

Amendment 317
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera, Markus Pieper

Proposal for a directive
Article 8 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. Member States shall ensure that the competent authorities designated pursuant to paragraph 1 cooperate with competent authorities designated

pursuant to Article 8 of (CER Directive) for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks.

Or. en

Amendment 318
Evžen Tošenovský

Proposal for a directive
Article 8 – paragraph 3

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

Or. en

Amendment 319
Evžen Tošenovský

Proposal for a directive
Article 9 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. Each Member State shall designate one of its CSIRTs referred to in paragraph 1 as a coordinator for the purpose of coordinated vulnerability disclosure pursuant to Article 6(1) (‘CVD CSIRT coordinator’). Where a Member State designates only one CSIRT, that CSIRT shall also be the CVD CSIRT coordinator for that Member State.

Or. en

Amendment 320
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 9 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that each CSIRT has adequate resources to carry out effectively their tasks as set out in Article ***10(2)***.	2. Member States shall ensure that each CSIRT has adequate resources ***and the technical capabilities necessary*** to carry out effectively their tasks as set out in Article ***10(3)***.

Or. en

Justification

Proposed amendments in Article 10 in accordance with requirements, technical capabilities to perform tasks, and tasks for CSIRTs.

Amendment 321
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 9 – paragraph 5

Text proposed by the Commission	*Amendment*
5. CSIRTs shall participate in peer reviews organised in accordance with Article 16.	***deleted***

Or. en

Amendment 322
Seán Kelly

Proposal for a directive

Article 9 – paragraph 6 a (new)

Text proposed by the Commission	*Amendment*
	6a. The Union may 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, the CSIRTs Network and the European cyber crises liaison organisation network. Such agreements shall take into account the need to ensure adequate protection of data.

Or. en

Justification

This Article would enable continued co-operation with the UK, post-Brexit which is reliant on that article for UK's interaction with the Cooperation Group under the Cyber Security provisions of the EU-UK Trade and Cooperation Agreement.

Amendment 323
Seán Kelly

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

Text proposed by the Commission	*Amendment*
	6b. Member States may cooperate with particular third countries as a means to meeting the provisions in this Directive on management of vulnerabilities, peer reviews, cyber security risk management, reporting measures and information sharing arrangements.

Or. en

Justification

This Article would allow specific Member States to avail of long standing links with particular third countries (i.e. UK and US) as a way of complying with the obligations in the Directive.

Amendment 324
Evžen Tošenovský

Proposal for a directive
Article 9 – paragraph 7

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

Or. en

Amendment 325
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

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

Or. en

Amendment 326
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive

Article 10 – paragraph 1 – point c a (new)

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

Or. en

Justification

Codes of conduct to govern the confidentiality of CSIRT operations, underpinning the interactions and work methods of CSIRT staff to ensure the security, integrity and trustworthiness of task-related information.

Amendment 327
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

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

Or. en

Amendment 328
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*
	(ea) CSIRTs shall have appropriate descriptions of the skillsets required by staff to meet the technical capabilities necessary to perform assigned tasks;

Or. en

Justification

Appropriate descriptions of skillsets can clarify task description and refine technical requirements for the sourcing and training of staff to develop the right skills for the tasks assigned to the CSIRT.

Amendment 329
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

Text proposed by the Commission	*Amendment*
	(eb) CSIRTs shall have appropriate internal training frameworks and, where suitable, relevant policies to support external technical training of staff in order to reinforce a culture of continuous improvement;

Or. en

Amendment 330
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

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

following technical capabilities to perform their tasks:

(a) The ability to conduct real-time monitoring of networks and information systems, and anomaly detection;

(b) The ability to support penetration prevention operations including, in particular, the detection and analysis of sophisticated cyber threats;

(c) The ability to collect and conduct complex forensic data analysis, and reverse engineering of cyber threats;

(d) The ability to filter harmful communication content including, but not limited to, malicious e-mails;

(e) The ability to protect data, including personal and sensitive data, from unauthorised exfiltration;

(f) The ability to enforce strong authentication and access privileges;

(g) The ability to analyse and attribute cyber threats.

Or. en

Justification

Commission's proposal expands CSIRTs' requirements and tasks however, in order to support CSIRTs in reaching the required maturity levels to perform the assigned tasks, it is more appropriate to describe the technical capabilities that CSIRTs need to develop. This approach takes account of CSIRTs with divergent maturity levels, rather than directly assigning those tasks to them, thus avoiding any risks of failure for CSIRTs with limited resources and decreased maturity levels.

Amendment 331
Eva Maydell, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera, Markus Pieper

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

Text proposed by the Commission	*Amendment*
	(da) acquiring real time threat

intelligence and sharing the information among public and private entities based on interoperable solutions.

Or. en

Amendment 332
Rasmus Andresen
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;	(e) providing, upon ***a specific*** request of an entity, scanning of the network and information systems used for the provision of their services ***in order to identify, mitigate or prevent specific and exceptional network and information security threats, in full respect of Regulation 2016/679***;

Or. en

Justification

Clarification needed both on the target of such scans and the limitations of the activity.

Amendment 333
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

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

Text proposed by the Commission	*Amendment*
	(fa) providing practical and operational guidance for essential and important entities in connection with cybersecurity response and prevention activities, including, in particular, dedicated technical support for SMEs;

Or. fr

Amendment 334
Eva Maydell, Markus Pieper, Franc Bogovič, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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

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

Or. en

Amendment 335
Evžen Tošenovský

Proposal for a directive
Article 10 – paragraph 3

Text proposed by the Commission	*Amendment*
3. CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive.	3. CSIRTs shall establish cooperation relationships with ***relevant entities, industry and other*** relevant actors in the private sector, with a view to better achieving the objectives of the Directive.

Or. en

Amendment 336
Evžen Tošenovský

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	2. Member States shall ensure their competent authorities ***and*** their CSIRTs

CSIRTs receive notifications on incidents, ***and*** significant cyber threats and near misses submitted pursuant to this Directive***. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to*** Article 20.	receive notifications on ***significant*** incidents, significant cyber threats and ***significant*** near misses submitted pursuant to ***Articles 20 and 27 of*** this Directive ***via the single entry point referred to in*** Article 20***(3a)***.

Or. en

Amendment 337
Evžen Tošenovský

Proposal for a directive
Article 11 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Each Member State shall ensure that its competent authorities or CSIRTs inform its single point of contact of notifications on incidents, significant cyber threats and near misses ***submitted pursuant to this Directive***.	3. Each Member State shall ensure that its competent authorities or CSIRTs inform its single point of contact ***and other relevant authorities in accordance with Article 20*** of notifications on ***significant*** incidents, significant cyber threats and ***significant*** near misses.

Or. en

Amendment 338
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 11 – paragraph 4

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

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

Or. en

Amendment 339
Evžen Tošenovský

Proposal for a directive
Article 11 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. Where relevant to the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation with other relevant stakeholders, such as CSIRTs other than those referred to in Article 9(1), CERTs and SOCs.

Or. en

Amendment 340

Evžen Tošenovský

Proposal for a directive
Article 11 – paragraph 5

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

Or. en

Amendment 341
Evžen Tošenovský

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

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

stakeholders, particularly representatives of industry, to participate in its work.

Or. en

Amendment 342
Rasmus Andresen
on behalf of the Greens/EFA Group

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

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

As many of the security incidents result in consequences on personal data it is essential that EDPB is a permanent member.

Amendment 343
Eva Maydell, Franc Bogovič, Markus Pieper, Angelika Niebler, Ivan Štefanec, Pilar del Castillo Vera

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

Text proposed by the Commission	*Amendment*
Where appropriate, the Cooperation Group may invite representatives of relevant stakeholders to participate in its work.	Where appropriate, the Cooperation Group may invite representatives of relevant ***industry*** stakeholders ***covered by this***

Directive to participate in its work.

Or. en

Amendment 344
Thierry Mariani, Paolo Borchia, Isabella Tovaglieri

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

Text proposed by the Commission	*Amendment*
Where appropriate, the Cooperation Group ***may*** invite representatives of relevant stakeholders to participate in its work.	The Cooperation Group ***shall*** invite representatives of relevant ***industrial*** stakeholders***, including SMEs,*** to participate in its work.

Or. fr

Amendment 345
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

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

Or. en

Amendment 346
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
(d) exchanging advice and cooperating with the Commission on draft Commission implementing ***or delegated*** acts adopted pursuant to this Directive;	(d) exchanging advice and cooperating with the Commission on draft Commission implementing acts adopted pursuant to this Directive;

Or. en

Amendment 347
Christophe Grudler, Klemen Grošelj, Nathalie Loiseau, Sandro Gozi, Stéphanie Yon-Courtin, Valérie Hayer

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

Text proposed by the Commission	*Amendment*
	(da) provide advice on the overall consistency of sector-specific cybersecurity requirements;

Or. en

Justification

The Cooperation Group should exchange with ENISA in order to maintain coherence in the different requirements in a specific sector.

Amendment 348
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
(f) discussing reports on the peer review referred to in Article 16(7);	***deleted***

Or. en

Amendment 349
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
	(fa) carrying out coordinated security risk assessments pursuant to Article 19(1), where applicable;

Or. en

Amendment 350
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

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

Or. en

Amendment 351
Bart Groothuis, Klemen Grošelj, Iskra Mihaylova, Nicola Danti, Christophe Grudler

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

Text proposed by the Commission	*Amendment*
	(ka) providing a yearly assessment in cooperation with ENISA on which Nation States are harbouring ransomware criminals.

Or. en

Justification

Harbouring ransomware criminals should not be left unaddressed and should come with a cost. The assessment should be followed up with concrete policy.

Amendment 352
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

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

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

Or. en

Justification

CSIRTs network can be an appropriate platform not only for the exchange of information relating to cybersecurity policies, practices, and controls, but also for the transfer of technology and technical expertise from more mature to less mature CSIRTs.

Amendment 353
Eva Kaili, Dan Nica, Łukasz Kohut, Ivo Hristov, Carlos Zorrinho, Marina Kaljurand, Maria-Manuel Leitão-Marques, Romana Jerković, Tsvetelina Penkova, Lina Gálvez Muñoz

Proposal for a directive
Article 13 – paragraph 3 – point g – point v

Text proposed by the Commission	*Amendment*
(v) contribution to the national cybersecurity incident and crisis response plan referred to in Article 7 ***(3)***;	(v) contribution to the national cybersecurity incident and crisis response plan referred to in Article 7 ***(4)***;

Or. en

Justification

Consistency with amended text of the Directive.

Amendment 354
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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

Text proposed by the Commission	*Amendment*
(l) discussing the peer-review reports referred to in Article 16(7);	***deleted***

Or. en

Amendment 355
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

Proposal for a directive
Article 13 – paragraph 4

Text proposed by the Commission	*Amendment*
4. For the purpose of the review referred to in Article 35 and by □24 months after the date of entry into force of this Directive□, and every two years thereafter, the CSIRTs network shall assess the progress made with the operational cooperation and produce a report. ***The report shall, in particular, draw conclusions on the outcomes of the peer reviews referred to in Article 16 carried out in relation to national CSIRTs, including conclusions and recommendations, pursued under this Article.*** That report shall also be submitted to the Cooperation Group.	4. For the purpose of the review referred to in Article 35 and by 24 months after the date of entry into force of this Directive, and every two years thereafter, the CSIRTs network shall assess the progress made with the operational cooperation and produce a report. That report shall also be submitted to the Cooperation Group.

Or. en

Amendment 356
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

Proposal for a directive
Article 14 – paragraph 1

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

Or. en

Justification

It should be clear from the wording of Article 14 that the CyCLONe is only for cases of large – scale cybersecurity incidents and crises (as it results from the Blueprint) and that exchange of information in the framework of the CyCLONe only considers such incidents and crises. It essential that CYCLOne fits into the existing institutional framework and there is no duplication of task especially with NIS CG and CSIRT Network.

Amendment 357
Evžen Tošenovský, Zdzisław Krasnodębski, Izabela-Helena Kloc

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 and ENISA.*** Commission ***shall participate in the EU-CyCLONe as an observer***. ENISA shall provide the secretariat of the network and support the secure exchange of information.

Or. en

Amendment 358
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

Proposal for a directive
Article 14 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
3. EU-CyCLONe shall have the following tasks:	3. EU-CyCLONe***, while avoiding any duplication of tasks with the CSIRT Network,*** shall have the following tasks:

Or. en

Justification

It essential that CYCLOne fits into the existing institutional framework and there is no duplication of task especially with NIS CG and CSIRT Network.

Amendment 359
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

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

Text proposed by the Commission	*Amendment*
(b) developing a shared situational awareness of relevant cybersecurity events;	***deleted***

Or. en

Justification

It is the CSIRTs Network task to exchange information (including technical details) on incidents, near misses, cyber threats, risks, vulnerabilities and trends and the CG to facilitate the strategic cooperation and exchange of information.

Amendment 360
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

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

Text proposed by the Commission	*Amendment*
(d) discussing national cybersecurity incident and response plans referred to in Article 7(2).	***deleted***

Or. en

Amendment 361
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(d) discussing national cybersecurity incident and response plans referred to in Article 7(2).	***deleted***

Or. en

Amendment 362
Zdzisław Krasnodębski, Evžen Tošenovský, Izabela-Helena Kloc, Elżbieta Kruk

Proposal for a directive
Article 14 – paragraph 5

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

Or. en

Justification

The scope of reporting is too wide and overlaps with the tasks of CSIRTs Network and CG. Moreover, this also overlaps with tasks of ENISA. The CyCLONe should focus on large-scale

incidents and crises.