European Parliament
2019-2024

Committee on the Internal Market and Consumer Protection

2020/0359(COD)

3.6.2021

AMENDMENTS
73 - 300

Draft opinion
Morten Løkkegaard
(PE691.156v02-00)

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))

AM_Com_LegOpinion

Amendment 73
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 5

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 Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.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 Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

Or. en

Amendment 74
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) The Directive is without prejudice to existing EU legislation governing the

protection of personal data.

Or. en

Amendment 75
Deirdre Clune

Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission.	(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission. ***The Commission should provide clear guidance on the criteria establishing which SMEs would be critical or important, especially for SME's who provide services in multiple Member States.***

Or. en

Amendment 76
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should ***also*** be covered by this Directive. Member States should be responsible for establishing a list of such	(9) However, small or micro entities***, unless*** fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should ***not*** be covered by this Directive. Member States should be responsible for establishing a list

entities, and submit it to the Commission.	of such entities, and submit it to the Commission. ***In order not to jeopardise collaborative innovation, non-commercial, free and open source projects should not be covered by this Directive.***

Or. en

Amendment 77
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 10

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

Or. en

Amendment 78
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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	(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.	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. ***This balance also helps national competent authorities to focus on those operators whose cybersecurity represents the highest societal risk***.

Or. en

Amendment 79
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 12

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

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

Amendment 80
Deirdre Clune

Proposal for a directive
Recital 12 a (new)

Text proposed by the Commission	*Amendment*
	(12a) The extension of the scope of this directive will mean the inclusion of entities subject to parallel regulation which may entail additional reporting requirements. In order to ensure coherence with all regulatory requirements, the Commission should ensure that where there are sector-specific acts that require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, that they should be consistent with the definitions and requirements of this Directive so that horizontal and sectoral legal instruments are sufficiently aligned in order to avoid any regulatory duplication or burden.

Or. en

Amendment 81
Deirdre Clune

Proposal for a directive
Recital 12 b (new)

Text proposed by the Commission	*Amendment*
	(12b) The Commission should publish clear guidance accompanying this Directive to help ensure harmonisation in implementation across Member States and avoid fragmentation.

Or. en

Amendment 82
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose.	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]	[17] [insert the full title and OJ publication reference when known]

Or. en

Amendment 83
Salvatore De Meo

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, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers***, and privacy or proxy registration service providers, domain brokers or resellers, and any other services that are related to the registration of domain names***.

Or. en

Amendment 84
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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***, the internal market*** and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.

Or. en

Amendment 85
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 20

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

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

Or. en

Amendment 86
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 20 a (new)

Text proposed by the Commission	*Amendment*
	(20a) When adopting national cybersecurity strategies, Member States should ensure that policy frameworks are available in order to address cybersecurity and the lawful access to information. In particular they should make sure that lawful access to information does not directly or indirectly lead to encryption being undermined and includes oversight, independent from the government.

Or. en

Amendment 87
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 20 b (new)

Text proposed by the Commission	*Amendment*
	(20b) A policy addressing cybersecurity in the supply chain should favour open source cybersecurity products, in line with Opinion 5/2021 of the European Data Protection Supervisor[1a]
	[1a] Opinion 5/2021 of the European Data Protection Supervisor on the Cybersecurity Strategy and the NIS 2.0 Directive, 11 March 2021

Or. en

Amendment 88
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 23

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

Or. en

Amendment 89
Marcel Kolaja
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) CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council, on behalf of and upon ***specific*** request by an entity under this Directive, a 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***. 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 90
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 26 a (new)

Text proposed by the Commission	*Amendment*
	(26a) Member States should, in accordance with their national cybersecurity strategies, put in place policies directed at cybersecurity awareness, cyber literacy and cyber-hygiene of citizens, with a view of strengthening the human element of network and information systems and protecting consumers from harm.

Or. en

Amendment 91
Maria-Manuel Leitão-Marques, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 26 b (new)

Text proposed by the Commission	*Amendment*
	(26b) In order to use resources with efficiency and effectiveness, and to be able to manage the increased amount of risks and incidents, Member States should adopt policies on the promotion and integration of AI-enabled and intelligent systems in the prevention and detection of cybersecurity incidents and threats as part of their national cybersecurity strategies, as well as make full use of them within their national competent authorities.

Or. en

Amendment 92
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 27

Text proposed by the Commission	*Amendment*
(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20] , a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.	(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20] , a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it***, thus endangering the internal market***. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.
[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).	[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

Or. en

Amendment 93
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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	(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm ***to businesses and consumers***,

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.	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.

Or. en

Amendment 94
Deirdre Clune

Proposal for a directive
Recital 28 a (new)

Text proposed by the Commission	*Amendment*
	(28a) The Commission, ENISA and the Member States should continue to foster

international alignment with standards and existing industry best practices in the area of risk management, for example in the areas of supply chain security assessments, information sharing and vulnerability disclosure.

Or. en

Amendment 95
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Svenja Hahn, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

Proposal for a directive
Recital 30

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

Or. en

Amendment 96
Marcel Kolaja
on behalf of the Greens/EFA Group

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 ***ensure that*** 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. en

Amendment 97
Marcel Kolaja
on behalf of the Greens/EFA Group

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	(31) Vulnerability registries or databases are hosted and maintained by entities which are not established in the Union. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should ***enter*** into structured cooperation agreements with ***vulnerability*** registries in third country jurisdictions ***and it should ensure that reports are transmitted to appropriate registries internationally***. ***ENISA should support European companies in their use of such registries.***

cooperation agreements with ***similar*** registries in third country jurisdictions.

Or. en

Amendment 98
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 32 a (new)

Text proposed by the Commission	*Amendment*
	(32a) The Cooperation Group should be composed of representatives of Member States, the Commission and ENISA.

Or. en

Amendment 99
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 34

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

Union Agency for Space Programme (EUSPA) to participate in its work.	Union Agency for Space Programme (EUSPA) to participate in its work***, as well as other Union bodies and agencies and supervisory authorities related to the Digital Single Market***.

Or. en

Amendment 100
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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 in order to improve cooperation ***and strengthen confidence inside the networks***. 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

Amendment 101
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 35 a (new)

Text proposed by the Commission	*Amendment*
	(35a) Likewise, the competent authorities and CSIRTs should be encouraged to participate in joint training programmes at the European level

organised by ENISA, with the same effect.

Or. en

Amendment 102
Marcel Kolaja
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 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 ***and should favour open source cybersecurity products for both software and hardware, as well as open source implementation of open and state-of-the-art, strong cryptography standards***.

Or. en

Amendment 103
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 45 a (new)

Text proposed by the Commission	*Amendment*
	(45a) Additionally, entities should also ensure adequate cybersecurity education

and training of their staff at all levels of the organisation.

Or. en

Amendment 104
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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***,*** ENISA ***and the affected essential and important entities***, should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21] , with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.
[21] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).	[21] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

Or. en

Amendment 105
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

Proposal for a directive
Recital 47

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

Amendment 106
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 51

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

Or. en

Amendment 107
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 51 a (new)

Text proposed by the Commission	*Amendment*
	(51a) In order to offer the necessary transparency to mitigate 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].
	[1a] Opinion 5/2021 of the European Data Protection Supervisor on the Cybersecurity Strategy and the NIS 2.0 Directive, 11 March 2021.

Or. en

Amendment 108
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 52

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

Or. en

Amendment 109
Marcel Kolaja
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) ***Strong and state of the art encryption is critical and irreplaceable for effective consistent protection of consumer and business security in the Single Market. 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. To protect their consumers p***roviders 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.

Or. en

Justification

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

Amendment 110
Alexandra Geese

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	(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*** 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 ***from*** end-to-end encrypted

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.	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 stricly adhere to the principles of necessity, proportionality and subsidiarity and shall not lead to creating backdoors or weakening encryption, ensuring that the security of encrypted data, including in end-to-end encrypted communications is not compromised.***

Or. en

Amendment 111
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 54

Text proposed by the Commission	*Amendment*
(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, ***where necessary,*** should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The ***use*** of end-to-end encryption should ***be reconciled with the*** Member State***'*** powers ***to ensure*** the protection of their essential security interests and public security***, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law***. ***Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an***	(54) 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, 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 ***security*** of end-to-end encryption should ***not be weakened by*** Member State powers***, policies or procedures for ensuring*** the protection of their essential security interests and public security.

effective response to crime.

Or. en

Amendment 112
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 54

Text proposed by the Commission	*Amendment*
(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. ***Solutions for lawful access to information 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 privacy and security of communications ***must not be undermined in any circumstance, as any loophole in encryption is open to be explored by all actors, regardless of their legitimacy or intent***.

Or. en

Amendment 113
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba

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 ***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. ***In this regard, this Directive*** should ***also include reporting of incidents that, based on*** an initial ***assessment performed by the entity, could 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***.

Or. en

Amendment 114
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi,

Isabella Tovaglieri, Virginie Joron

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 incident, they should be required to submit an initial notification ***without undue delay and not later than 72*** hours, followed by a final report not later than ***2 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. 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 ***2 months*** for the final report.

Or. en

Amendment 115
Maria-Manuel Leitão-Marques, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba

Proposal for a directive
Recital 55 a (new)

Text proposed by the Commission	*Amendment*
	(55a) Where entities become aware of an incident, they should be required to submit an initial notification within 72 hours, followed by a comprehensive 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. The initial notification should be preceded by an early warning about an ongoing incident, without any obligation of additional information disclosures within the first 24 hours as of the moment the entity became aware of the incident. This early warning should be submitted as soon as possible, allowing entities to seek support from competent authorities or CSIRTs swiftly, and enabling competent authorities or CSIRTs to mitigate the potential spread of the reported incident, as well as serving as a situational awareness tool for CSIRTs. Member States should ensure that the requirement to submit both the initial notification and the early warning do 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 deadline of one month for the comprehensive report.

Or. en

Amendment 116
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 56

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

Or. en

Amendment 117
Marcel Kolaja

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 databases of domain names and registration data ('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.

Or. en

Amendment 118
Salvatore De Meo

Proposal for a directive
Recital 59

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

Or. en

Amendment 119
Marcel Kolaja
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

Amendment 120
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Recital 61

Text proposed by the Commission	*Amendment*
(61) In order to ensure the availability of accurate ***and complete*** domain name registration data, TLD registries and the entities providing domain name registration services for the TLD ***(so-called registrars)*** should collect ***and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing***	(61) In order to ensure the availability of accurate domain name registration data, TLD registries and the entities providing domain name registration services for the TLD should collect ***the*** domain name registration ***data necessary*** for the ***provision of their services. They*** should ***also take steps*** to prevent and correct inaccurate registration data in accordance

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.

with Union data protection rules.

Or. en

Amendment 121
Salvatore De Meo

Proposal for a directive
Recital 61

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

Or. en

Amendment 122
Marcel Kolaja
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.***	(62) TLD registries should also enable lawful access***, without undue delay, to competent national authorities, as designated by Member States under their national cybersecurity strategies,*** to specific domain name registration data concerning natural persons, in accordance with Union data protection law.

[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 123
Salvatore De Meo

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	(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 ***and in any event within 24 hours*** 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

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.	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 124
Deirdre Clune

Proposal for a directive
Recital 68

Text proposed by the Commission	*Amendment*
(68) Entities should be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection	(68) Entities should be encouraged ***and supported by Member States*** to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements ***that are based on already established internationally recognised standards***. 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

Union law rules.	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 125
Marcel Kolaja
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, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.***	(69) The processing of personal data, ***which should be limited to what is*** strictly necessary and proportionate***,*** for the purposes of ensuring network and information security by 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.

Or. en

Amendment 126
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

Proposal for a directive
Recital 70

Text proposed by the Commission	*Amendment*
(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to ensuring a fair balance of obligations for both entities and competent authorities. Thus, essential entities should be subject to a fully-fledged supervisory regime (ex-ante and ex-post), while important entities should be subject to a light supervisory regime, ex-post only. For the latter, this means that important entities should not document systematically compliance with cybersecurity risk management requirements, while competent authorities should implement a reactive ex -post approach to supervision and, hence, not have a general obligation to supervise those entities.	(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance ***and to achieve a common high level of security within the digital sector throughout the Union***, 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***, except where there is a manifest breach of obligations, in particular where such entities cause risk for users or other services included in the scope of this Directive***.

Or. en

Amendment 127
Deirdre Clune

Proposal for a directive
Recital 70

Text proposed by the Commission	*Amendment*
(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to ensuring a fair balance of obligations for both entities and competent authorities. Thus, essential entities should be subject to a fully-fledged supervisory regime (ex-ante and ex-post), while important entities should be subject to a light supervisory regime, ex-post only. For the latter, this means that important entities should not document systematically compliance with cybersecurity risk management requirements, while competent authorities should implement a reactive ex -post approach to supervision and, hence, not have a general obligation to supervise those entities.	(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance ***and to achieve a common high level of security throughout the digital sector including by preventing risks for users or other networks, information systems and services***, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to ensuring a fair balance of obligations for both entities and competent authorities. Thus, essential entities should be subject to a fully-fledged supervisory regime (ex-ante and ex-post), while important entities should be subject to a light supervisory regime, ex-post only. For the latter, this means that important entities should not document systematically compliance with cybersecurity risk management requirements, while competent authorities should implement a reactive ex -post approach to supervision and, hence, not have a general obligation to supervise those entities ***except where there is a demonstrable breach of obligations***.

Or. en

Amendment 128
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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 the ***implicated*** 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 129
Marcel Kolaja

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

Amendment 130
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Recital 79

Text proposed by the Commission	*Amendment*
(79) A peer-review mechanism should be introduced, allowing the assessment by experts designated by the Member States of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources.	(79) A peer-review mechanism should be introduced, allowing the assessment by experts designated by the Member States ***and ENISA*** of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources***, and the exchange of experiences and best practices related to procedures and instruments***.

Or. en

Amendment 131
Deirdre Clune

Proposal for a directive
Article 1 – paragraph 1

Text proposed by the Commission	*Amendment*
1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union.	1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union ***to ensure a trustworthy digital environment for consumers and business and to improve and remove barriers to the functioning of the internal market***.

Or. en

Amendment 132
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 1 – paragraph 1

Text proposed by the Commission	*Amendment*
1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union.	1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union ***and strengthening the Digital Single Market***.

Or. en

Amendment 133
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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	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]

[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).

important entities in Annex II. ***Entities and subsectors that fall within the scope of this Directive shall be provided with clear and concise definitions with respect to their designations. This Directive does not apply to entities that Member States unequivocally identify as non-critical, including where they are of types referred to in Annex I and 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]***, without prejudice to their voluntary involvement.***

[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 134
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 2 – paragraph 1

Text proposed by the Commission	*Amendment*
1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC**.**[28]	1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC[28] ***nor to non-commercial free and open source projects.***
[28] Commission Recommendation 2003/361/EC of 6 May 2003 concerning	[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).	the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Or. en

Amendment 135
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 136
Evžen Tošenovský

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 137
Marcel Kolaja
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

Amendment 138
Marcel Kolaja
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

Amendment 139
Evžen Tošenovský

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, in particular, 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 that are to comply with this Directive and shall 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 140
Evžen Tošenovský

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;
	In addition to the 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 141
Evžen Tošenovský

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 142
Evžen Tošenovský

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 143
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

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

Or. en

Amendment 144
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	(5a) 'cross-border incident' means any incident which impacts operators under at least 2 different national competent authorities;

Or. en

Amendment 145
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 4 – paragraph 1 – point 8 a (new)

Text proposed by the Commission	*Amendment*
	(8a) "early warning" means the information preceding the initial incident notification warning to third parties, without detailed information obligations, on the onset of an incident or on the discovery moment of an ongoing incident;

Or. en

Amendment 146
Deirdre Clune

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

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

Or. en

Amendment 147
Evžen Tošenovský

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 148
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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 provided and has a low level of dependency from other sectors or types of services.

Or. en

Amendment 149
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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

Text proposed by the Commission	*Amendment*
(b) a governance framework to achieve	(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;	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 entrusted with specific SMEs support. The governance framework shall clearly outline how cooperation and coordination is organised between relevant national authorities designated under this Directive***;

Or. en

Amendment 150
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

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

Or. en

Amendment 151
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
(c) an assessment to identify relevant assets and cybersecurity risks in that Member State***;***	(c) an assessment to identify relevant assets and cybersecurity risks in that Member State***, including potential shortages that may negatively impact the***

Single Market.

Or. en

Justification

Include products and skills shortages that may be cause for concern, learning the lessons from the covid-19 crisis and the semiconductor shortages.

Amendment 152
Marcel Kolaja
on behalf of the Greens/EFA Group

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

Text proposed by the Commission	*Amendment*
	(fa) a policy framework for enhanced coordination between the competent authorities under this Directive and the independent body responsible for oversight of data collection, in line with Union law.

Or. en

Amendment 153
Marcel Kolaja
on behalf of the Greens/EFA Group

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

Text proposed by the Commission	*Amendment*
(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services;	(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services***, which should favour open source cybersecurity products for both software and hardware, as well as open source implementation of open and state-of-the-***

art, strong cryptography standards;

Or. en

Amendment 154
Marcel Kolaja
on behalf of the Greens/EFA Group

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

Text proposed by the Commission	*Amendment*
	(aa) a policy framework addressing cybersecurity and the lawful access to information, which does not undermine the effectiveness of encryption in protecting privacy and security of communications and which includes independent oversight;

Or. en

Amendment 155
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	(aa) a policy addressing cybersecurity of consumers, including their awareness of cyber threats, their cyber literacy and cyber-hygiene, as well as the cybersecurity of products available for consumers;

Or. en

Amendment 156
Marcel Kolaja
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 the promotion of the use of open source cybersecurity products***;

Or. en

Amendment 157
Deirdre Clune

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

Text proposed by the Commission	*Amendment*
(c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6;	(c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6 ***including by laying down guidelines and best practices based on already established internationally recognised standards on vulnerability handling and disclosure***;

Or. en

Amendment 158
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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***	(e) a policy on promoting and ***enhancing*** cybersecurity skills ***and competence across all levels, from the***

initiatives;	***non-experts to the highly skilled professionals***;

Or. en

Amendment 159
Marcel Kolaja
on behalf of the Greens/EFA Group

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 ***technology neutral*** cybersecurity skills, awareness raising and research and development initiatives;

Or. en

Amendment 160
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
(f) a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure;	(f) a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure ***and promoting the coherent and synergic use of available funds***;

Or. en

Amendment 161
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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

Text proposed by the Commission	*Amendment*
(h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats**.**	(h) a policy addressing specific needs of SMEs ***in fulfilling the provisions laid down by this Directive***, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats ***and encouraging, through dedicated support, their proactive adoption of suitable cybersecurity measures;***

Or. en

Amendment 162
Deirdre Clune

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

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

Or. en

Amendment 163
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

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

Or. en

Amendment 164
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	(i) this policy shall include the establishment of a national single point of contact for SMEs and a framework for the most efficient use of Digital Innovation Hubs and available funds in the achievement of policy objectives;

Or. en

Amendment 165
Stelios Kouloglou

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

Text proposed by the Commission	*Amendment*
	(ha) a policy to combat online identity theft of its citizens, a policy to protect its citizens from phishing, in particular elderly and low-literate citizens;

Or. en

Justification

First and foremost, a Member State must protect its citizens, also online.

Amendment 166
Deirdre Clune

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

Text proposed by the Commission	*Amendment*
	(ha) a policy to raise awareness and increase education about cybersecurity threats among consumers in the EU;

Or. en

Amendment 167
Stelios Kouloglou

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

Text proposed by the Commission	*Amendment*
	(hb) a policy providing protection to consumers from the exploitation of vulnerabilities of the 'internet of things' or other network and information systems;

Or. en

Justification

Cybersecurity must also mean protection for consumers online.

Amendment 168
Stelios Kouloglou

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

Text proposed by the Commission	*Amendment*
	2a. Member States shall ensure that a regulatory framework is built to guarantee that connected products and associated services including supply chains are secure-by-design, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered. Member States shall introduce cybersecurity requirements for applications, software, embedded software and operating systems;

Or. en

Amendment 169
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	Key performance indicators shall be chosen taking into account recommendations from ENISA and, whenever possible, shall be comparable at the Union level;

Or. en

Amendment 170
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 6 – title

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

Or. en

Amendment 171
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Svenja Hahn, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

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 172
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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	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 process of coordinated vulnerability disclosure shall be coherent with internationally recognised standards on vulnerability handling and*** 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

network.

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.

Or. en

Amendment 173
Marcel Kolaja
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 addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.***	2. 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 ***in relevant international registries***.

Or. en

Amendment 174
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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***, as well as the necessary technical and organisational measures for the security of the registry,*** 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. ***ENISA shall clarify the terms of work and use of registry, including procedures for reporting, use and storage of the vulnerability information. The*** registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.

Or. en

Amendment 175
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip

Proposal for a directive
Article 6 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ENISA shall develop and maintain a European vulnerability ***registry***. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties***. The registry*** shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.	2. ENISA shall develop and maintain a European vulnerability ***database***. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures ***as well as the appropriate disclosure policies*** with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and ***easily*** register vulnerabilities present in ICT products or ICT services, as well as to provide access to the ***relevant*** information on vulnerabilities contained in the registry to all interested parties***, provided that such actions do not undermine the protection of confidentiality and trade secrets. The vulnerability database*** shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.

Or. en

Amendment 176
Maria-Manuel Leitão-Marques, Adriana Maldonado López, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 6 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ENISA shall develop and maintain	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.	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. ***ENISA may enter into information sharing agreements and structured cooperation with other vulnerability registries developed and maintained by trusted partners.***

Or. en

Amendment 177
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

Proposal for a directive
Article 7 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Each Member State shall designate one or more competent authorities responsible for the management of large-scale incidents and crises. Member States shall ensure that competent authorities have adequate resources to perform, in an effective and efficient manner, the tasks	1. Each Member State shall designate one or more competent authorities responsible for the management of large-scale incidents and crises***. Where a Member State designates more than one competent authority, it should clearly indicate which of these competent authorities would serve as the main point***

assigned to them.	***of contact during a large-scale incident or crisis***. Member States shall ensure that competent authorities have adequate resources to perform, in an effective and efficient manner, the tasks assigned to them.

Or. en

Amendment 178
Deirdre Clune

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

Text proposed by the Commission	*Amendment*
	1a. Where a Member State designates more than one competent authority referred to in paragraph 1, it shall clearly indicate which of these competent authorities will serve as the main point of contact during a large-scale incident or crisis.

Or. en

Amendment 179
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 7 – paragraph 3 – point f a (new)

Text proposed by the Commission	*Amendment*
	(fa) coordination with authorities responsible for cyber intelligence and cyber defence

Or. en

Amendment 180
Evžen Tošenovský

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 181
Stelios Kouloglou

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

Text proposed by the Commission	*Amendment*
	(aa) protecting all data, including from unauthorised exfiltration and network logging using all necessary safeguards and to set parameters and standards for transparency when sharing information and or data;

Or. en

Justification

Protecting the citizens data is protecting the citizens.

Amendment 182
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
(c) responding to incidents;	(c) responding to incidents ***and,***

	whenever possible and adequate, providing assistance to entities that may request it;

Or. en

Amendment 183
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
(d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;	(d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity***, namely through the analysis of early warnings and notifications as referred to in Article 20***;

Or. en

Amendment 184
Marcel Kolaja
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 compliance with Union law***;

Or. en

Amendment 185
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
(f) participating in the CSIRTs network and providing mutual assistance to other members of the network upon their request.	(f) ***actively*** participating in the CSIRTs network and providing mutual assistance to other members of the network upon their request.

Or. en

Amendment 186
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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

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

Or. en

Amendment 187
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	(fa) participating in joint cybersecurity exercises at Union level;

Or. en

Amendment 188
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 11 – paragraph 2

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

Or. en

Amendment 189
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 11 – paragraph 4

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

pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State.	pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State***, as well as with cyber defence and cyber intelligence authorities***.
[39] [insert the full title and OJ publication reference when known]	[39] [insert the full title and OJ publication reference when known]

Or. en

Amendment 190
Evžen Tošenovský

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 191
Evžen Tošenovský

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 192
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	(fa) assessing the functioning of the peer review system and drawing up recommendations for its improvement;

Or. en

Amendment 193
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	(ka) supporting ENISA in organising joint training of national competent authorities at the EU level.

Or. en

Amendment 194
Evžen Tošenovský

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 195
Evžen Tošenovský

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 196
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
(a) increasing the level of preparedness of the management of large scale incidents and crises;	(a) increasing the level of preparedness of the management of large scale incidents and crises***, including cross-border cyber threats***;

Or. en

Amendment 197
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
1. ENISA shall issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union. The report shall in particular include an assessment of the following:	1. ENISA shall issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union ***and present it to the European Parliament***. The report shall in particular include an assessment of the following:

Or. en

Amendment 198
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
(a) the development of cybersecurity capabilities across the Union;	(a) the development of cybersecurity capabilities across the Union***, including the general level of skills and competences in cybersecurity in the Digital Single Market***;

Or. en

Amendment 199
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(b) the technical, financial and human resources available to competent	(b) the technical, financial and human resources available to competent

authorities and cybersecurity policies***, and the implementation of supervisory measures and enforcement actions in light of the outcomes of peer reviews referred to in Article 16***;	authorities and cybersecurity policies;

Or. en

Amendment 200
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	(ca) an aggregated index providing an assessment of the cybersecurity of European consumers.

Or. en

Amendment 201
Evžen Tošenovský

Proposal for a directive
Article 16

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

Or. en

Amendment 202
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

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

Or. en

Amendment 203
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 16 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The methodology shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States shall designate experts eligible to carry out the peer reviews. ENISA and the Commission shall designate experts to participate as observers in the peer-reviews. The Commission, supported by ENISA, shall establish within the methodology as referred to in paragraph 1 an objective, non-discriminatory, fair and transparent system for the selection and the random allocation of experts for each peer review.	2. The methodology shall include objective, non-discriminatory***, technology-neutral***, fair and transparent criteria on the basis of which the Member States shall designate experts eligible to carry out the peer reviews. ENISA and the Commission shall designate experts to participate as observers in the peer-reviews. The Commission, supported by ENISA, shall establish within the methodology as referred to in paragraph 1 an objective, non-discriminatory, fair and transparent system for the selection and the random allocation of experts for each peer review.

Or. en

Amendment 204
Maria-Manuel Leitão-Marques, Adriana Maldonado López, Christel Schaldemose, Alex Agius Saliba

Proposal for a directive
Article 16 – paragraph 7

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

Or. en

Justification

As peer reviews are a system that also aims to build trust between Member States, reports shall not be disclosed due to the risk of undermining trust and curtailing the freedom of those writing the reports.

Amendment 205
Evžen Tošenovský

Proposal for a directive
Article 18 – paragraph 1

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

ensure a level of security of network and information systems appropriate to the risk presented***, and differentiate between the essential and important entities and between the sectors and subsectors with higher or lower level of criticality referred to in Annexes I and II***.

Or. en

Amendment 206
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

Proposal for a directive
Article 18 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.	1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. ***These measures shall be adopted following a risk-based assessment that takes the utmost account of the level of criticality of the concerned entities.*** Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented ***and shall not undermine valid security offering mechanisms already in place***.

Or. en

Amendment 207
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 18 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.	1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented. ***In particular, measures shall be taken to prevent and minimise the impact of security incidents on consumers.***

Or. en

Amendment 208
Deirdre Clune

Proposal for a directive
Article 18 – paragraph 1

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

Or. en

Justification

To reflect Article 40 (1) of the European Electronic Communications Code regarding the responsibilities of important and essential entities to prevent and mitigate risks which may have a negative impact on other networks.

Amendment 209
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

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

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

Or. en

Amendment 210
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

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

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

Or. en

Amendment 211
Evžen Tošenovský

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

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

Or. en

Amendment 212
Marcel Kolaja
on behalf of the Greens/EFA Group

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

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

Or. en

Amendment 213
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	(ga) policies to ensure adequate education and training in cybersecurity at all levels of the organisation for essential and important entities.

Or. en

Amendment 214
Marcel Kolaja
on behalf of the Greens/EFA Group

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

Text proposed by the Commission	*Amendment*
	(ga) policies that ensure reproducible-builds and code auditability.

Or. en

Amendment 215
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

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

Text proposed by the Commission	*Amendment*
	(ga) security training and awareness.

Or. en

Amendment 216
Deirdre Clune

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

Text proposed by the Commission	*Amendment*
	2a. ENISA may facilitate, in accordance with Regulation (EU) No 526/2013 of the European Parliament and of the Council, the coordination of Member States regarding the measures referred to in paragraph 1, to avoid regulatory fragmentation that may create barriers in the internal market and present additional risks.

Or. en

Justification

There may be a role for ENISA in helping to coordinate Member States operational measures in so far as this as possible to prevent any unintended fragmentation. This is also an approach consistent with the European Electronic Communications Code Article 40 (1).

Amendment 217
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
	2a. ENISA shall create and maintain an updated list of state of the art measures, as referred to in paragraph 1.

Or. en

Amendment 218
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 18 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. ***For this purpose they should also favour open source cybersecurity products for both software and hardware, as well as open source implementation of open and state-of-the-art, strong cryptography standards.***

Or. en

Amendment 219
Evžen Tošenovský

Proposal for a directive
Article 18 – paragraph 6

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

Or. en

Amendment 220
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

Proposal for a directive
Article 18 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The Commission ***is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements*** laid down in paragraph 2 ***to take account of new cyber threats, technological developments or sectorial specificities***.	6. The Commission***, in cooperation with the Cooperation Group and ENISA, shall provide guidance and best practices on the compliance by entities in a proportionate manner with the requirements,*** laid down in paragraph 2***, and in particular to the requirement in point (d) of that paragraph.*** ***In developing delegated acts, the Commission shall also consult all relevant stakeholders***.

Or. en

Amendment 221
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

Proposal for a directive
Article 19 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where ***relevant***, non-technical risk factors.	1. The Cooperation Group, in cooperation with the Commission and ENISA***, and after having consulted the affected essential and important entities***, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where ***justified by the level of criticality of the sector***, non-technical risk factors. ***Risk assessments should follow a balanced and non-discriminatory approach to ensure competitive and harmonised internal market, with coordinated Member State approaches.***

Or. en

Amendment 222
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 19 – paragraph 1

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

Or. en

Amendment 223
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

Proposal for a directive
Article 19 – paragraph 2

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

Or. en

Amendment 224
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

Proposal for a directive
Article 19 a (new)

Text proposed by the Commission	*Amendment*
	Article 19a
	When the Cooperation Group includes non-technical risk factors in its supply chain risk assessments, it shall ensure that those factors are evidence-based, clearly defined and that their interpretation is aligned across the Union to the greatest extent possible. Member States shall ensure that any affected party has clear and lawful means to raise concerns, challenge and object to the final decision taken as a result of the supply chain assessments referred to in paragraph 1 of this Article.

Or. en

Amendment 225
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.	1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident. ***Member States shall establish a single entry point for all notifications required under this Directive and under other Union law, such as Regulation (EU) 2016/679 and Directive 2002/58/EC.*** ***ENISA, in cooperation with the Cooperation Group shall develop common notification templates for the reporting information requested by Union law.***

Or. en

Amendment 226
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 20 – paragraph 1

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

Or. en

Amendment 227
Deirdre Clune

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

Text proposed by the Commission	*Amendment*
	1a. For the purpose of simplifying reporting obligations, Member States shall establish a single entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC.

Or. en

Amendment 228
Deirdre Clune

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

Text proposed by the Commission	*Amendment*
	1b. ENISA, in cooperation with the Cooperation Group shall develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burden for companies.

Or. en

Amendment 229
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.	***deleted***
Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.	

Or. en

Amendment 230
Marcel Kolaja

on behalf of the Greens/EFA Group

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

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

Or. en

Amendment 231
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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

Text proposed by the Commission	*Amendment*
Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat ***that those entities identify that could have potentially resulted in a significant incident***.	Member States shall ensure that essential and important entities ***may*** notify, without undue delay ***where feasible or through periodic threat analysis reports***, the competent authorities or the CSIRT of any significant cyber threat ***within the meaning of Article 2(8) of Regulation (EU) 2019/881***.

Or. en

Amendment 232
Evžen Tošenovský

Proposal for a directive
Article 20 – paragraph 3

Text proposed by the Commission	*Amendment*
3. An incident shall be considered significant if:	***deleted***
(a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned;	
(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.	

Or. en

Amendment 233
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
(a) the incident has caused or ***has the potential*** to cause substantial operational disruption or financial losses for the entity concerned;	(a) the incident has caused or ***it can be assumed*** to cause substantial operational disruption or financial losses for the entity concerned;

Or. en

Amendment 234
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
(b) the incident has affected or ***has the potential*** to affect other natural or legal persons by causing considerable material	(b) the incident has affected or ***it can be assumed*** to affect other natural or legal persons by causing considerable material

or non-material losses.	or non-material losses.

Or. en

Amendment 235
Evžen Tošenovský

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

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

Or. en

Amendment 236
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

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

concerned to disclose additional information regarding the incident;

Or. en

Justification

An initial notification serves as both a call for help for operators and a situational awareness tool for CSIRTs. As there is the intention of moving the initial notification to a later point in time, it is essential to design a new tool which conserves those two characteristics but does not cause an increased burden nor diverts resources away from finding a solution to the incident.

Amendment 237
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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

Text proposed by the Commission	*Amendment*
(a) without undue delay and in any event ***within 24*** hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;	(a) without undue delay and in any event ***not later than 72*** hours after having become aware of the incident, an initial notification, which, where applicable ***and possible***, shall indicate whether the incident is presumably caused by unlawful or malicious action;

Or. en

Amendment 238
Deirdre Clune

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

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

caused by unlawful or malicious action;	caused by unlawful or malicious action;

Or. en

Amendment 239
Evžen Tošenovský

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

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

Or. en

Amendment 240
Deirdre Clune

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

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

Or. en

Amendment 241
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

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

Or. en

Amendment 242
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

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

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

Or. en

Amendment 243
Deirdre Clune

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

Text proposed by the Commission	*Amendment*
	(ca) a final report should be provided one month after the incident has been mitigated

Or. en

Amendment 244
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

Text proposed by the Commission	*Amendment*
Member States shall provide that in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines laid down in points (a) ***and (c)***.	Member States shall provide that in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines laid down in points (a)***, (b) and (d)***.

Or. en

Amendment 245
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 20 – paragraph 5

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

Or. en

Amendment 246
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 20 – paragraph 7

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

Or. en

Amendment 247
Evžen Tošenovský

Proposal for a directive
Article 21 – title

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

Or. en

Amendment 248
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 21 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to demonstrate compliance with certain requirements of Article 18, Member States ***may require*** essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881**.** ***The products, services and processes subject to*** certification ***may be developed by an essential or important entity or procured from third parties***.	1. In order to demonstrate compliance with certain requirements of Article 18, ***and following guidance from ENISA, the Commission, and the Cooperation Group,*** Member States ***shall call for*** essential and important entities to certify certain ICT products, ICT services and ICT processes***, developed either by the essential and important entities or procured from third parties,*** under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881***, or under equivalent and internationally accepted*** certification ***schemes. Whenever possible, the call for certification shall be adopted by all Member States in a harmonised way***.

Or. en

Amendment 249
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

Proposal for a directive
Article 21 – paragraph 1

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

certification ***schemes***.

Or. en

Amendment 250
Evžen Tošenovský

Proposal for a directive
Article 21 – paragraph 1

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

Or. en

Amendment 251
Evžen Tošenovský

Proposal for a directive
Article 21 – paragraph 2

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

accordance with Article 36.

Or. en

Amendment 252
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

Proposal for a directive
Article 21 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission shall ***be empowered to adopt delegated acts specifying*** which categories of essential entities shall be ***required*** to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. ***The delegated acts shall be adopted in accordance with Article 36.***	2. The Commission shall ***regularly assess the efficiency and use of the adopted European cybersecurity certification schemes under Article 49 of Regulation (EU) 2019/881 and shall identify*** which categories of essential entities shall be ***encouraged*** to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1.

Or. en

Amendment 253
Evžen Tošenovský

Proposal for a directive
Article 21 – paragraph 3

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

Or. en

Amendment 254
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 22 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.	1. In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, ***and according to guidance from ENISA and the Cooperation Group,*** encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

Or. en

Amendment 255
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

Proposal for a directive
Article 23 – title

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

Or. en

Justification

Domain name registration data is stored across a variety of actors making use of different technologies, which not necessarily have to be 'dedicated' databases.

Amendment 256
Salvatore De Meo

Proposal for a directive
Article 23 – paragraph 1

Text proposed by the Commission	*Amendment*
1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and ***the*** entities providing domain name registration services ***for the TLD*** shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.	1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and entities providing domain name registration services***,*** shall collect***, verify*** and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data. ***This should take place as a pre-requisite to engaging in domain name registration services as well as at regular periods thereafter, including when changes are made to domain name registration data. Where the domain name registration data collected and maintained is inaccurate, legitimate access seekers shall have the right to request that it is reverified and corrected, failure by an operator to do so resulting in termination of the service.***

Or. en

Amendment 257
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 23 – paragraph 1

Text proposed by the Commission	*Amendment*
1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate ***and complete*** domain name registration data ***in a dedicated database facility with due***	1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain ***the*** accurate domain name registration data ***necessary for the provision of their services, in***

diligence subject to Union data protection law ***as regards data which are personal data***.	***compliance with*** Union data protection law.

Or. en

Amendment 258
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

Proposal for a directive
Article 23 – paragraph 1

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

Or. en

Amendment 259
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 23 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under	***deleted***

the TLDs.

Or. en

Amendment 260
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

Proposal for a directive
Article 23 – paragraph 2

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

Or. en

Justification

Relevant information should contain the registrants' (email) address. The ability to communicate in writing is essential for the enforcement of criminal and civil legal claims that require written records and substantiation of communication attempts for investigative purposes.

Amendment 261
Salvatore De Meo

Proposal for a directive
Article 23 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the	2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the

holders of the domain names and the points of contact administering the domain names under the TLDs.	holders of the domain names and the points of contact administering the domain names under the TLDs***, including at least the registrants' name, physical address, email address, and telephone number***.

Or. en

Amendment 262
Alexandra Geese

Proposal for a directive
Article 23 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names ***and the points of contact administering the domain names under the TLDs***.	2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant ***the*** information ***necessary*** to identify and contact the holders of the domain names.

Or. en

Amendment 263
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 23 – paragraph 3

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

Or. en

Amendment 264
Deirdre Clune

Proposal for a directive
Article 23 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases ***include*** accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.	3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases ***infrastructure includes*** accurate***, verified*** and complete information***, and that inaccurate or incomplete data should be corrected or erased by the registrant without delay***. Member States shall ensure that such policies and procedures are made publicly available.

Or. en

Amendment 265
Alexandra Geese

Proposal for a directive
Article 23 – paragraph 3

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

Or. en

Amendment 266
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip, Jordi Cañas

Proposal for a directive
Article 23 – paragraph 3

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

Or. en

Amendment 267
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 23 – paragraph 4

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

Or. en

Amendment 268
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-

Courtin, Vlad-Marius Botoş, Andrus Ansip

Proposal for a directive
Article 23 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall ensure that the TLD registries and the entities providing domain name registration services ***for the TLD publish***, without undue delay after the registration of a domain name, domain registration data ***which are not personal data***.	4. Member States shall ensure that the TLD registries and the entities providing domain name registration services ***make publicly available***, without undue delay ***and in any event within 24 hours*** after the registration of a domain name, ***all*** domain registration data ***of legal persons as registrants***.

Or. en

Justification

Legal persons domain registration data are regarded as public and commonly used.

Amendment 269
Salvatore De Meo

Proposal for a directive
Article 23 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD ***reply*** without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.	5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. ***Legitimate access seekers may include natural or legal persons making a duly justified request to access the DNS data under Union or national law, and they may include competent authorities under Union or national law, CERTs, CSIRTs, and as regards the data of their clients – providers of electronic communications networks and services and providers of cybersecurity***

	technologies and services and cybersecurity researchers. Such duly justified requests shall include requests made to prevent DNS abuse. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD ***provide such access*** without undue delay***, and in any event within 24 hours,*** to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Or. en

Amendment 270
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 23 – paragraph 5

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

Or. en

Amendment 271
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip

Proposal for a directive
Article 23 – paragraph 5

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

Or. en

Justification

In cases of justified requests, domain registration data (including personal data) should be given to legitimate access seekers (for example for cybersecurity reasons, detection and prevention of crime, protection of minors and intellectual property, fraud prevention and protection against hate speech).

Amendment 272
Deirdre Clune

Proposal for a directive
Article 24 – paragraph 2

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

establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the Union.	establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the Union. ***This shall be done in a manner that ensures that no disproportionate burden falls on the regulatory body of one, or a small number of, Member States.***

Or. en

Amendment 273
Evžen Tošenovský

Proposal for a directive
Article 25

Text proposed by the Commission	*Amendment*
Article 25	***deleted***
Registry for essential and important entities	
1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1). The entities shall submit the following information to ENISA by [12 months after entering into force of the Directive at the latest]:	
(a) the name of the entity;	
(b) the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 24(3);	
(c) up-to-date contact details, including email addresses and telephone numbers of the entities.	
2. The entities referred to in paragraph 1 shall notify ENISA about any changes to the details they submitted under paragraph 1 without delay, and in	

any event, within three months from the date on which the change took effect.

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

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

Or. en

Amendment 274
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

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

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

Or. en

Amendment 275
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 25 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The entities referred to in paragraph 1 shall notify ***ENISA*** about any changes to the details they submitted under paragraph 1 without delay, and in any event, within three months from the date on which the change took effect.	2. The entities referred to in paragraph 1 shall notify ***the national competent authority*** about any changes to the details they submitted under paragraph 1 without delay, and in any event, within three months from the date on which the change took effect.

Or. en

Amendment 276
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 25 – paragraph 3

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

Or. en

Amendment 277
Stelios Kouloglou

Proposal for a directive
Article 26 – paragraph 2

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

Or. en

Justification

Cybersecurity threats and information on how to contain them benefit from public scrutiny. The more (tech)journalists know, the better civil society can arm itself against such threats.

Amendment 278
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Andrus Ansip, Jordi Cañas

Proposal for a directive
Article 26 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall set out ***rules*** specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such ***rules*** shall also ***lay down*** the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such	3. Member States shall set out ***guidelines*** specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such ***guidelines*** shall also ***include*** the details of the involvement***, where relevant,*** of public authorities ***and independent experts*** in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States

arrangements in accordance with their policies referred to in Article 5(2) (g).	shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).

Or. en

Amendment 279
Deirdre Clune

Proposal for a directive
Article 26 – paragraph 5

Text proposed by the Commission	*Amendment*
5. In compliance with Union law, ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance.	5. In compliance with Union law, ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance***; as well as by facilitating information-sharing at Union level, with the aim of promoting the cross-border exchange of information between relevant trusted communities of essential and important entities as referred to in the second paragraph, taking into account Union law and safeguarding business-sensitive information***.

Or. en

Amendment 280
Marco Campomenosi, Alessandra Basso, Markus Buchheit, Antonio Maria Rinaldi, Isabella Tovaglieri, Virginie Joron

Proposal for a directive
Article 26 – paragraph 5

Text proposed by the Commission	*Amendment*
5. In compliance with Union law, ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by	5. In compliance with Union law, ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance ***with***

providing best practices and guidance.	***the aim of promoting the cross-border exchange of information at Union level between the relevant entities***.

Or. en

Amendment 281
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 27 – paragraph 1

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

Or. en

Amendment 282
Deirdre Clune

Proposal for a directive
Article 27 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall ensure that, without prejudice to Article 3, entities falling	Member States shall ensure that, without prejudice to Article 3, entities ***within the***

outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.	***scope and*** falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.

Or. en

Amendment 283
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 28 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in Articles 18 and 20.	1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in Articles 18 and 20***, and are provided with the adequate means to perform their function***.

Or. en

Amendment 284
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 28 – paragraph 2

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

Or. en

Amendment 285
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 28 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.	2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches***, including data protection authorities from other Member States whenever relevant***.

Or. en

Amendment 286
Marcel Kolaja
on behalf of the Greens/EFA Group

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

Text proposed by the Commission	*Amendment*
(c) ***targeted*** security audits based on risk assessments or risk-related available information;	(c) security audits based on risk assessments or risk-related available information ***, carried out by a qualified independent body or a competent authority or independent experts and***

	make the results thereof available to the competent authority; ***the cost of the audit shall be paid by the provider;***

Or. en

Amendment 287
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Andrus Ansip

Proposal for a directive
Article 29 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request ***and*** specify the information requested.	3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request***,*** specify the information requested ***and shall limit their requests to the scope of the incident or issue of concern***.

Or. en

Amendment 288
Evžen Tošenovský

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

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

Or. en

Amendment 289
Evžen Tošenovský

Proposal for a directive
Article 29 – paragraph 6

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

Or. en

Amendment 290
Marcel Kolaja
on behalf of the Greens/EFA Group

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

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

Or. en

Amendment 291
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Andrus Ansip

Proposal for a directive
Article 30 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Where exercising their powers pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request ***and*** specify the information requested.	3. Where exercising their powers pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request***,*** specify the information requested ***and shall limit their requests to the scope of the incident or issue of concern***.

Or. en

Amendment 292
Morten Løkkegaard, Dita Charanzová, Ivars Ijabs, Sandro Gozi, Stéphanie Yon-Courtin, Vlad-Marius Botoş, Andrus Ansip

Proposal for a directive
Article 31 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of ***at least*** 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.	4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.

Or. en

Amendment 293
Evžen Tošenovský

Proposal for a directive
Article 31 – paragraph 6

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

Or. en

Amendment 294
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 32 – paragraph 1

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

Or. en

Amendment 295
Marcel Kolaja
on behalf of the Greens/EFA Group

Proposal for a directive
Article 32 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation within ***a reasonable period of time***.	1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation within ***72 hours***.

Or. en

Amendment 296
Maria-Manuel Leitão-Marques, Marc Angel, Adriana Maldonado López, Evelyne Gebhardt, Christel Schaldemose, Alex Agius Saliba, Maria Grapini

Proposal for a directive
Article 32 – paragraph 3

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

Or. en

Justification

Ensure greater consumer protection and reinforce GDPR enforcement.

Amendment 297
Marcel Kolaja

on behalf of the Greens/EFA Group

Proposal for a directive
Article 32 – paragraph 3

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

Or. en

Amendment 298
Evžen Tošenovský

Proposal for a directive
Article 36

Text proposed by the Commission	*Amendment*
Article 36	***deleted***
Exercise of the delegation	
1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	
2. The power to adopt delegated acts referred to in Articles 18(6) and 21(2) shall be conferred on the Commission for a period of five years from […]	
3. The delegation of power referred to in Articles 18(6) and 21(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any	

delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.

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

6. A delegated act adopted pursuant to Articles 18(6) and 21(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Or. en

Amendment 299
Evžen Tošenovský

Proposal for a directive
Annex I – subheading 1

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

Or. en

Amendment 300
Evžen Tošenovský

Proposal for a directive
Annex II – subheading 1

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

Or. en