European Parliament
2019-2024

Committee on the Internal Market and Consumer Protection

2020/0359(COD)

14.7.2021

OPINION

of the Committee on the Internal Market and Consumer Protection

for the Committee on Industry, Research and Energy

on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Rapporteur for opinion: Morten Løkkegaard

PA_Legam

SHORT JUSTIFICATION

In general, the Rapporteur welcomes the legislative proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS 2). The Rapporteur believes that in an increasingly digitalised world, security online is key to guarantee a safe digital environment as well as the functioning of the single market, where consumers and economic operators can act freely.

The NIS 2 proposal is a significant improvement compared to the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS 1). It enumerates the key deficiencies by the NIS 1, such as the low level of cyber resilience of businesses and sectors, as well as the inconsistent resilience and low levels of joint situation awareness and crisis response in and between Member States. The Rapporteur welcomes the ambitions to correct this with the NIS 2.

Scope

The Rapporteur appreciates the extended scope of the NIS 2 proposal, in particular, the inclusion of new sectors such as the public administration. The explicit list of sectors and services included will surely reduce the discretion of Member States in defining the concrete entities subject to the Directive and will consequently reduce fragmentation in the single market.

Within the sectors and services covered, the Commission proposed the size-cap rule as a uniform criterion to determine the entities falling within the scope of application of the Directive. This criterion undoubtedly presents the advantage of ensuring legal certainty, while reducing divergences among Member States.

However, while welcoming the extended sector-based scope, the Rapporteur is of the opinion that this general criterion should be combined with an assessment of the criticality of entities within each sector. This would allow for medium and large entities which, following a risk assessment, are considered to be of a low level of criticality and dependency on otherwise critical entities, to be left outside the scope of the Directive.

The Rapporteur stresses that this should not be considered an open door for discrepant interpretation between Member States. To ensure that this does not add to fragmented implementation between Member States, the Commission is encouraged to issue clear guidance on this.

Finally, while welcoming the exclusion of micro and small companies from the scope, the Rapporteur is of the view that there is a need to encourage their voluntary inclusion, as micro and small entities are also subject to, and affected by, cyberattacks.

Coordinated cybersecurity regulatory frameworks

The Rapporteur welcomes the chapter defining different elements of the national cybersecurity strategies and their crisis management tools. As part of their national cybersecurity strategy, it is proposed that Member States adopt a policy promoting the use of cryptography and encryption, especially by SMEs.

The Rapporteur welcomes the development of a European vulnerability registry by ENISA, however, believes that it is important that the registration respects business confidentiality and trade secrets and does not burden entities unnecessarily.

Cooperation among Member States

The more structured cooperation among Member States within the Cooperation Group, the CSIRTs network and the newly created group for large-scale incidents in the NIS 2 are particularly welcomed. However, there is a need to ensure that the level of confidence and willingness to exchange information among Member States is increased, as the effectiveness of this cooperation plays a key role in ensuring a high level of cybersecurity in the EU.

In light of this position, a number of amendments have been drafted to strengthen the role of the networks. In particular, the Rapporteur considers peer review a fruitful way to increase Member States´ shared confidence, and supports that they should play a crucial role in assessing the effectiveness of individual Member States´ cybersecurity policies.

Cybersecurity risk management

The extension of the risk assessment to the whole supply chain (Article 18 and Article 19) is appreciated, however, the Rapporteur stresses that the point needs clarifications to provide clear guidance to entities subject to this requirement and to Member States when carrying out a coordinated security risk evaluation of specifically critical sectors or supply chains.

Reporting obligations

The Rapporteur believes that more clarity should be provided on specific points of the reviewed Directive, mainly concerning some of the obligations imposed on companies in the scope of the NIS 2. The Rapporteur has sought to reduce the bureaucracy and make it easier for businesses to comply with the new rules having in mind the final objective of an effective implementation of the Directive.

The Rapporteur´s proposal is to extend the suggested deadline of 24 hours in the reporting obligations for the first notifications to 72 hours, to allow companies to effectively address the ongoing cybersecurity attack prior to notification. Furthermore, it is proposed to delete any reference to the mandatory notification of so-called ‘potential incidents’.

AMENDMENTS

The Committee on the Internal Market and Consumer Protection calls on the Committee on Industry, Research and Energy, as the committee responsible, to take into account the following amendments:

Amendment 1
Proposal for a directive
Recital 5

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

Amendment 2
Proposal for a directive
Recital 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) The Directive is without prejudice to the rules laid down by Union law on the protection of personal data.

Amendment 3
Proposal for a directive
Recital 9

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

Amendment 4
Proposal for a directive
Recital 10

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

Amendment 5
Proposal for a directive
Recital 12 a (new)

Text proposed by the Commission	*Amendment*
	(12a) The extension of the scope of this Directive entails the inclusion of entities subject to sector-specific regulation. To avoid any regulatory duplication or burden, the Commission should ensure that sector-specific acts that require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, are consistent with this Directive.

Amendment 6
Proposal for a directive
Recital 12 b (new)

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

Amendment 7
Proposal for a directive
Recital 12 c (new)

Text proposed by the Commission	*Amendment*
	(12c) The Commission should also issue guidelines to support Member States in correctly implementing the provisions on the scope, and to evaluate the proportionality of the obligations set out by this Directive in consideration of the criticality of entities falling in the scope, especially when applying to entities with complex business models or operating environments, whereby an entity may simultaneously fulfil the criteria assigned to both essential and important entities, or may simultaneously conduct activities that are some within and some outside the scope of this Directive. In cases where entities have their main activity outside the scope of this Directive, but some other secondary activity inside the scope, the provisions should only apply to the function or unit level within an entity, which falls within the scope of this Directive.

Amendment 8
Proposal for a directive
Recital 14

Text proposed by the Commission	*Amendment*
(14) In view of the interlinkages between cybersecurity and the physical	(14) In view of the interlinkages between cybersecurity and the physical

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

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

Amendment 9
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	(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 is essential for its continuous and stable operation, on which the digital economy***, the internal market*** and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers***, and privacy or proxy registration service providers, domain brokers or resellers, and any other services that are related to the registration of domain names***.

Amendment 10
Proposal for a directive
Recital 20

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

through joint strategies and actions at Union level.

Amendment 11
Proposal for a directive
Recital 23

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

Amendment 12
Proposal for a directive
Recital 25

Text proposed by the Commission	*Amendment*
(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] as regards personal data, on behalf of and upon request by an entity under this Directive, a ***proactive*** scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may	(25) ***To identify, mitigate and prevent specific threats*** as regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] as regards personal data, on behalf of and upon request by an entity under this Directive, a scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all

request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.

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

---

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

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

Amendment 13
Proposal for a directive
Recital 26 a (new)

Text proposed by the Commission	*Amendment*
	(26a) As a part of their national cybersecurity strategies, Member States should adopt policies on the promotion and integration of intelligent systems in the prevention and detection of cybersecurity incidents and threats. Member States should, in accordance with their national cybersecurity strategies, put in place policies directed at cybersecurity awareness and literacy, with a view of protecting consumers. When adopting national cybersecurity strategies, Member States should ensure policy frameworks to address lawful access to information.

Amendment 14
Proposal for a directive
Recital 27

Text proposed by the Commission	*Amendment*
(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to	(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to

Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20] , a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.

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

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).

Amendment 15
Proposal for a directive
Recital 28

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

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

Amendment 16
Proposal for a directive
Recital 28 a (new)

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

Amendment 17
Proposal for a directive
Recital 30

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

Amendment 18
Proposal for a directive
Recital 31

Text proposed by the Commission	*Amendment*
(31) Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A European vulnerability ***registry*** maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with ***similar*** registries in third country jurisdictions.	(31) Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A European vulnerability ***database*** maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with ***vulnerability databases or*** registries in third country jurisdictions ***and transmitting reports to appropriate registries provided that any such actions do not undermine the protection of confidentiality and trade secrets***.

Amendment 19
Proposal for a directive
Recital 32

Text proposed by the Commission	*Amendment*
(32) The Cooperation Group should establish a work programme every two years including the actions to be undertaken by the Group to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive should be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Group.	(32) The Cooperation Group should ***discuss political priorities and key challenges on cybersecurity and*** establish a work programme every two years including the actions to be undertaken by the Group to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive should be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Group.

Amendment 20
Proposal for a directive
Recital 32 a (new)

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

Amendment 21
Proposal for a directive
Recital 34

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

Amendment 22
Proposal for a directive
Recital 35

Text proposed by the Commission	*Amendment*
(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes for officials from other Member States in order to improve cooperation. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the activities of the host competent authority.	(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes ***and joint training programmes*** for officials from other Member States in order to improve cooperation ***and strengthen trust among Member States***. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the activities of the host competent authority ***or CSIRT***.

Amendment 23
Proposal for a directive
Recital 39

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

Amendment 24
Proposal for a directive
Recital 45 a (new)

Text proposed by the Commission	*Amendment*
	(45a) Additionally, entities should also ensure adequate cybersecurity education and training of their staff at all levels of the organisation.

Amendment 25
Proposal for a directive
Recital 46

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

Amendment 26
Proposal for a directive
Recital 47

Text proposed by the Commission	*Amendment*
(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-	(47) The supply chain risk assessments, in light of the features of the sector concerned ***and its criticality***, should take into account both technical and, where

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.

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

Amendment 27
Proposal for a directive
Recital 51

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

Amendment 28
Proposal for a directive
Recital 52

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

Amendment 29
Proposal for a directive
Recital 53

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

Amendment 30
Proposal for a directive
Recital 54

Text proposed by the Commission	*Amendment*
(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of ***Article 18***. The use of end-to-end encryption ***should be reconciled with*** the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime.	(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of ***cybersecurity risk management measures***. The use of end-to-end encryption ***is without prejudice to*** the Member State' powers***, policies and procedures*** to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime. ***Any action taken has to strictly adhere to the principles of proportionality and subsidiarity.***

Amendment 31
Proposal for a directive
Recital 55

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

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***.

near miss, they should be required to submit an initial notification within ***72*** hours, followed by a ***comprehensive report not later than three months after submitting the initial notification and a*** final report not later than one month after ***the incident has been mitigated***. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. ***The initial notification should be preceded by an early warning within the first 24 hours without any obligation of additional information disclosures. This early warning should be submitted as soon as possible, allowing entities to seek support from competent authorities or CSIRTs swiftly, and enabling competent authorities or CSIRTs to mitigate the potential spread of the reported incident, as well as serving as a situational awareness tool for CSIRTs.*** To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines ***foreseen***.

Amendment 32
Proposal for a directive
Recital 56

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

Amendment 33
Proposal for a directive
Recital 59

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

Amendment 34
Proposal for a directive
Recital 61

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

Amendment 35
Proposal for a directive
Recital 68

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

the Union as well as the data protection Union law rules.	compliance with the competition rules of the Union as well as the data protection Union law rules.

Amendment 36
Proposal for a directive
Recital 69

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

Amendment 37
Proposal for a directive
Recital 70

Text proposed by the Commission	*Amendment*
(70) In order to strengthen the	(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.

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

Amendment 38
Proposal for a directive
Recital 76

Text proposed by the Commission	*Amendment*
(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning ***part or all the*** services provided by an essential entity ***and the imposition of a***	(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning ***relevant*** services provided by an essential entity. Given their severity and impact on

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

Amendment 39
Proposal for a directive
Recital 79

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

Amendment 40
Proposal for a directive
Recital 80

Text proposed by the Commission	*Amendment*
(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should ***also*** be empowered to adopt delegated acts establishing ***which categories of*** essential entities ***shall*** be ***required to obtain a certificate and under which specific European cybersecurity certification schemes***. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[26] . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.	(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should be empowered to adopt delegated acts establishing ***the technical elements related to risk management measures. The Commission should also be empowered to adopt delegated acts by specifying the type of information submitted by*** essential ***and important*** entities ***of any incident having a significant impact on the provision of their services or of any near miss and by specifying the cases in which an incident should*** be ***considered to be significant***. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[26]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.
[26] OJ L 123, 12.5.2016, p. 1.	[26] OJ L 123, 12.5.2016, p. 1.

Amendment 41
Proposal for a directive
Recital 81

Text proposed by the Commission	*Amendment*
(81) In order to ensure uniform conditions for the implementation of the relevant provisions of this Directive concerning the procedural arrangements necessary for the functioning of the Cooperation Group***, the technical elements related to risk management measures or the type of information***, the format and the procedure of incident notifications, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.[27]	(81) In order to ensure uniform conditions for the implementation of the relevant provisions of this Directive concerning the procedural arrangements necessary for the functioning of the Cooperation Group, the format and the procedure of incident notifications, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.[27]
[27] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).	[27] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

Amendment 42
Proposal for a directive
Article 1 – paragraph 1

Text proposed by the Commission	*Amendment*
1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union.	1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union***, in order to achieve a trusted digital environment for consumers and economic operators, and to improve and remove barriers to the functioning of the internal market***.

Amendment 43
Proposal for a directive
Article 2 – paragraph 2 – subparagraph 1 – introductory part

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

Amendment 44
Proposal for a directive
Article 2 – paragraph 2 – subparagraph 2 a (new)

Text proposed by the Commission	*Amendment*
	The Commission shall issue guidelines in order to support Member States in correctly implementing the provisions on the scope as well as in order to grant possible derogations for specific important entities from the scope of the Directive or from some of its provisions, in consideration of their low level of criticality in their specific sector and/or their low level of dependency from other sectors or types of services. Member States, taking fully into account the Commission's guidelines, shall notify their motivated decisions in this regard to the Commission.

Amendment 45
Proposal for a directive
Article 4 – paragraph 1 – point 4

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

Amendment 46
Proposal for a directive
Article 4 – paragraph 1 – point 5 a (new)

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

Amendment 47
Proposal for a directive
Article 4 – paragraph 1 – point 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) ´near miss´ means an event which could potentially have caused harm, but was successfully prevented from fully transpiring;

Amendment 48
Proposal for a directive
Article 4 – paragraph 1 – point 15 a (new)

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

Amendment 49
Proposal for a directive
Article 5 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of	1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures***, including appropriate human and financial***

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

Amendment 50
Proposal for a directive
Article 5 – paragraph 1 – point b

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

Amendment 51
Proposal for a directive
Article 5 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) an assessment to identify relevant assets and cybersecurity risks in that 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***;

Amendment 52
Proposal for a directive
Article 5 – paragraph 1 – point e

Text proposed by the Commission	*Amendment*
(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;	(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy***, including a one-stop-shop for SMEs***;

Amendment 53
Proposal for a directive
Article 5 – paragraph 2 – point b

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

Amendment 54
Proposal for a directive
Article 5 – paragraph 2 – point c

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

Amendment 55
Proposal for a directive
Article 5 – paragraph 2 – point e

Text proposed by the Commission	*Amendment*
(e) a policy on promoting ***and developing*** cybersecurity skills***, awareness raising*** and research and development initiatives;	(e) a policy on promoting ***cybersecurity for consumers, raising their awareness about cyber threats, increasing cyber literacy, enhancing trust of users, technology neutral*** cybersecurity skills and ***education as well as promoting*** research and development initiatives ***and the cybersecurity of connected products***;

Amendment 56
Proposal for a directive
Article 5 – paragraph 2 – point e a (new)

Text proposed by the Commission	*Amendment*
	(ea) a policy on promoting the use of cryptography and encryption, in particular by SMEs;

Amendment 57
Proposal for a directive
Article 5 – paragraph 2 – point h

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

Amendment 58
Proposal for a directive
Article 5 – paragraph 2 – point h a (new)

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

Amendment 59
Proposal for a directive
Article 5 – paragraph 2 – point h b (new)

Text proposed by the Commission	*Amendment*
	(hb) a policy promoting the coherent and synergic use of available funds;

Amendment 60
Proposal for a directive
Article 5 – paragraph 4

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

Amendment 61
Proposal for a directive
Article 6 – title

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

Amendment 62
Proposal for a directive
Article 6 – paragraph 2

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

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.

network and information systems to disclose and ***easily*** register vulnerabilities present in ICT products or ICT services, as well as to provide access to the ***relevant*** information on vulnerabilities contained in the registry to all interested parties***, provided that such actions do not undermine the protection of confidentiality and trade secrets. The vulnerability database*** shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated. ***To avoid duplication of efforts, ENISA shall enter into information sharing agreement and structured cooperation agreement with the Common Vulnerabilities and Exposures (CVE) registry, and, where relevant, with other databases globally developed and maintained by trusted partners.***

Amendment 63
Proposal for a directive
Article 7 – paragraph 1 a (new)

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

Amendment 64
Proposal for a directive
Article 7 – paragraph 3 – point f

Text proposed by the Commission	*Amendment*
(f) national procedures and ***arrangements*** between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.	(f) national procedures and ***coordination*** between relevant national authorities and bodies***, including those responsible for cyber intelligence and cyber defence,*** to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.

Amendment 65
Proposal for a directive
Article 10 – paragraph 2 – point d

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

Amendment 66
Proposal for a directive
Article 10 – paragraph 2 – point e

Text proposed by the Commission	*Amendment*
(e) providing, upon request of an entity, a ***proactive*** scanning of the network and information systems used for the provision of their services;	(e) providing, upon request of an entity, a scanning of the network and information systems used for the provision of their services ***to identify, mitigate or prevent specific threats***;

Amendment 67
Proposal for a directive
Article 10 – paragraph 2 – point f

Text proposed by the Commission	*Amendment*
(f) participating in the CSIRTs	(f) ***actively*** participating in the CSIRTs

network and providing mutual assistance to other members of the network upon their request**.**	network and providing mutual assistance to other members of the network upon their request***;***

Amendment 68
Proposal for a directive
Article 10 – paragraph 2 – point f a (new)

Text proposed by the Commission	*Amendment*
	(fa) providing operational assistance and guidance to entities referred to in Annex I and II, and especially to SMEs;

Amendment 69
Proposal for a directive
Article 10 – paragraph 2 – point f b (new)

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

Amendment 70
Proposal for a directive
Article 11 – paragraph 2

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

Amendment 71
Proposal for a directive
Article 11 – paragraph 4

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

Amendment 72
Proposal for a directive
Article 12 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.	2. The Cooperation Group shall ***meet regularly and*** carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.

Amendment 73
Proposal for a directive
Article 12 – paragraph 3 – subparagraph 2

Text proposed by the Commission	*Amendment*
Where appropriate, the Cooperation Group	Where appropriate, the Cooperation Group

may invite representatives of relevant stakeholders to participate in its work.	may invite representatives of relevant ***Union bodies and agencies as well as*** stakeholders to participate in its work.

Amendment 74
Proposal for a directive
Article 12 – paragraph 4 – point a

Text proposed by the Commission	*Amendment*
(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive;	(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive ***and promoting its uniform implementation in the Member States***;

Amendment 75
Proposal for a directive
Article 12 – paragraph 4 – point a a (new)

Text proposed by the Commission	*Amendment*
	(aa) exchanging information on political priorities and key challenges on cybersecurity and defining the main objectives of the cybersecurity;

Amendment 76
Proposal for a directive
Article 12 – paragraph 4 – point a b (new)

Text proposed by the Commission	*Amendment*
	(ab) discussing national strategies of Member States and their preparedness;

Amendment 77
Proposal for a directive
Article 12 – paragraph 4 – point c

Text proposed by the Commission	*Amendment*
(c) exchanging advice and cooperating with the Commission on emerging	(c) exchanging advice and cooperating with the Commission on emerging

cybersecurity policy initiatives;	cybersecurity policy initiatives***, and with the European External Action Service on geopolitical aspects of the cybersecurity in the Union***;

Amendment 78
Proposal for a directive
Article 12 – paragraph 4 – point f

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

Amendment 79
Proposal for a directive
Article 12 – paragraph 4 – point k a (new)

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

Amendment 80
Proposal for a directive
Article 12 – paragraph 6

Text proposed by the Commission	*Amendment*
6. By … [***24*** months after the date of entry into force of this Directive] and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148.	6. By … [***12*** months after the date of entry into force of this Directive] and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148.

Amendment 81
Proposal for a directive
Article 12 – paragraph 8 a (new)

Text proposed by the Commission	*Amendment*
	8a. The Cooperation Group shall regularly publish a summary report of its activities, without prejudice of the confidentiality of information shared during its meetings.

Amendment 82
Proposal for a directive
Article 13 – paragraph 3 – point a

Text proposed by the Commission	*Amendment*
(a) exchanging information on CSIRTs' capabilities;	(a) exchanging information on CSIRTs' capabilities ***and preparedness***;

Amendment 83
Proposal for a directive
Article 13 – paragraph 3 – point b

Text proposed by the Commission	*Amendment*
(b) exchanging relevant information on incidents, near misses, cyber threats, risks and vulnerabilities;	(b) exchanging relevant information on incidents, near misses, cyber threats, risks and vulnerabilities ***and supporting Member States operational capabilities***;

Amendment 84
Proposal for a directive
Article 13 – paragraph 3 – point d a (new)

Text proposed by the Commission	*Amendment*
	(da) exchanging and discussing information in relation to cross-border incidents;

Amendment 85
Proposal for a directive
Article 13 – paragraph 3 – point g – point i a (new)

Text proposed by the Commission	*Amendment*
	(i a) information sharing;

Amendment 86
Proposal for a directive
Article 13 – paragraph 3 – point j

Text proposed by the Commission	*Amendment*
(j) ***at the request of an individual CSIRT,*** discussing the capabilities and preparedness of ***that CSIRT***;	(j) discussing the capabilities and preparedness of ***CSIRTs***;

Amendment 87
Proposal for a directive
Article 13 – paragraph 4

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

Amendment 88
Proposal for a directive
Article 14 – paragraph 3 – point a

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

Amendment 89
Proposal for a directive
Article 14 – paragraph 5

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

Amendment 90
Proposal for a directive
Article 14 – paragraph 6

Text proposed by the Commission	*Amendment*
6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements.	6. EU-CyCLONe shall ***closely*** cooperate with the CSIRTs network on the basis of agreed procedural arrangements.

Amendment 91
Proposal for a directive
Article 15 – paragraph 1 – introductory part

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

Amendment 92
Proposal for a directive
Article 15 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) the development of cybersecurity capabilities across the Union;	(a) the development of cybersecurity capabilities across the Union***, including the general level of skills and competences in cybersecurity, the overall degree of resilience of the internal market towards cyber threats and the level of implementation of the Directive across the Member States***;

Amendment 93
Proposal for a directive
Article 15 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) a cybersecurity index providing for an aggregated assessment of the maturity level of cybersecurity capabilities**.**	(c) a cybersecurity index providing for an aggregated assessment of the maturity level of cybersecurity capabilities ***including an overall assessment of cybersecurity for consumers;***

Amendment 94
Proposal for a directive
Article 15 – paragraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) the geopolitical aspects having a direct or indirect impact on the state of cybersecurity in the Union.

Amendment 95
Proposal for a directive
Article 16 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. The Commission shall establish, after consulting the Cooperation Group and	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:	ENISA, and at the latest by ***12*** months following the entry into force of this Directive, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The reviews shall be conducted by cybersecurity technical experts drawn from ***at least two*** Member States ***and of ENISA*** different than the one reviewed and shall cover at least the following:

Amendment 96
Proposal for a directive
Article 16 – paragraph 2

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

Amendment 97
Proposal for a directive
Article 18 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities shall take ***appropriate and proportionate*** technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services.	1. Member States shall ensure that essential and important entities shall take technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. ***Those measures shall be***

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.	***appropriate and proportionate to the level of criticality of the sector or of the type of service, as well as the level of dependency of the entity from other sectors or types of services, and shall be adopted following a risk-based assessment.*** Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented. ***In particular, measures shall be taken to prevent and minimise the impact of security incidents on recipients of their services.***

Amendment 98
Proposal for a directive
Article 18 – paragraph 2 – point d

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

Amendment 99
Proposal for a directive
Article 18 – paragraph 2 – point f

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

Amendment 100
Proposal for a directive
Article 18 – paragraph 2 – point g

Text proposed by the Commission	*Amendment*
(g) the use of cryptography ***and*** encryption***.***	(g) the use of cryptography***,*** encryption ***and in particular end-to-end-encryption;***

Amendment 101
Proposal for a directive
Article 18 – paragraph 2 – point g a (new)

Text proposed by the Commission	*Amendment*
	(ga) policies to ensure adequate cybersecurity training and awareness.

Amendment 102
Proposal for a directive
Article 18 – paragraph 3

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

Amendment 103
Proposal for a directive
Article 18 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission ***may*** adopt ***implementing*** acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2***. Where preparing those acts***, ***the Commission shall proceed in***	5. The Commission ***is empowered to*** adopt ***delegated*** acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2, and follow, to the greatest extent possible, international and European

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

standards, as well as relevant technical specifications. ***In developing delegated acts, the Commission shall also consult all relevant stakeholders.***

Amendment 104
Proposal for a directive
Article 18 – paragraph 6

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

Amendment 105
Proposal for a directive
Article 19 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.	1. ***In view to increase the overall level of cybersecurity,*** 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***, such as geopolitical risks***.

Amendment 106
Proposal for a directive
Article 20 – paragraph 1

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

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

Amendment 107
Proposal for a directive
Article 20 – paragraph 1 a (new)

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

Amendment 108
Proposal for a directive
Article 20 – paragraph 1 b (new)

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

Amendment 109
Proposal for a directive
Article 20 – paragraph 2 – subparagraph 1

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

Amendment 110
Proposal for a directive
Article 20 – paragraph 2 – subparagraph 2

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

Amendment 111
Proposal for a directive
Article 20 – paragraph 3 – point a

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

Amendment 112
Proposal for a directive
Article 20 – paragraph 3 – point b

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

Amendment 113
Proposal for a directive
Article 20 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. The Commission is empowered to adopt delegated acts, in accordance with Article 36, to supplement this Directive by specifying the type of information submitted pursuant to paragraph 1 of this Article and by further specifying the cases in which an incident shall be considered to be significant as referred to in paragraph 3 of this Article.

Amendment 114
Proposal for a directive
Article 20 – paragraph 4 – point -a (new)

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

Amendment 115
Proposal for a directive
Article 20 – paragraph 4 – point a

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

Amendment 116
Proposal for a directive
Article 20 – paragraph 4 – point c – introductory part

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

Amendment 117
Proposal for a directive
Article 20 – paragraph 4 – point c – point i

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

Amendment 118
Proposal for a directive
Article 20 – paragraph 4 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) in case of a still ongoing incident at time of submission of the comprehensive report under letter (c), a final report shall be provided one month after the incident has been mitigated;

Amendment 119
Proposal for a directive
Article 20 – paragraph 7

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

Amendment 120
Proposal for a directive
Article 20 – paragraph 8

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

Amendment 121
Proposal for a directive
Article 20 – paragraph 9

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

information included in the summary report.	information included in the summary report.

Amendment 122
Proposal for a directive
Article 20 – paragraph 10

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

Amendment 123
Proposal for a directive
Article 20 – paragraph 11

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

Amendment 124
Proposal for a directive
Article 21 – paragraph 1

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

Amendment 125
Proposal for a directive
Article 21 – paragraph 2

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

Amendment 126
Proposal for a directive
Article 22 – paragraph -1 (new)

Text proposed by the Commission	*Amendment*
	-1. The Commission, in collaboration

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

Amendment 127
Proposal for a directive
Article 22 – paragraph 1

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

Amendment 128
Proposal for a directive
Article 23 – title

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

Amendment 129
Proposal for a directive
Article 23 – paragraph 1

Text proposed by the Commission	*Amendment*
1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD	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.

registries and the entities providing domain name registration services for the TLD***,*** shall collect***, verify*** and maintain accurate and complete domain name registration data ***necessary for the provisions of their services*** in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.

Amendment 130
Proposal for a directive
Article 23 – paragraph 2

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

Amendment 131
Proposal for a directive
Article 23 – paragraph 3

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

policies and procedures are made publicly available.

Amendment 132
Proposal for a directive
Article 23 – paragraph 4

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

Amendment 133
Proposal for a directive
Article 23 – paragraph 5

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

Amendment 134
Proposal for a directive
Article 24 – paragraph 2

Text proposed by the Commission	*Amendment*
2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the Union.	2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the Union. ***This shall be done in a manner that ensures that no disproportionate burden falls on national regulatory bodies.***

Amendment 135
Proposal for a directive
Article 25 – paragraph 1 – introductory part

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

Amendment 136
Proposal for a directive
Article 26 – paragraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques,	(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection ***and prevention***

mitigation strategies, or response and recovery stages.	techniques, mitigation strategies, or response and recovery stages.

Amendment 137
Proposal for a directive
Article 26 – paragraph 3

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

Amendment 138
Proposal for a directive
Article 26 – paragraph 5

Text proposed by the Commission	*Amendment*
5. In compliance with Union law, ENISA shall support the establishment of 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, while safeguarding business-sensitive information. At the request of essential and important entities, the Cooperation Group shall be invited to provide best practices and guidance.***

Amendment 139
Proposal for a directive
Article 27 – paragraph -1 (new)

Text proposed by the Commission	*Amendment*
	-1. Member States shall ensure that essential and important entities may submit notifications, on a voluntary basis, of cyber threats that those entities identify that could have potentially resulted in a significant incident. Member States shall ensure that, for the purpose of these notifications, entities shall act in accordance with the procedure laid down in Article 20. Voluntary notifications shall not result in the imposition of any additional obligations upon the reporting entity.

Amendment 140
Proposal for a directive
Article 27 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall ensure that, without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States ***may*** prioritise the processing of mandatory notifications over voluntary notifications. Voluntary 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.	***1.*** Member States shall ensure that, without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States ***shall*** prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification***, but the Member State may grant it assistance from CSIRTs***.

Amendment 141
Proposal for a directive
Article 28 – paragraph 1

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

Amendment 142
Proposal for a directive
Article 28 – paragraph 2

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

Amendment 143
Proposal for a directive
Article 29 – paragraph 2 – point c

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

Amendment 144
Proposal for a directive
Article 29 – paragraph 2 – point f

Text proposed by the Commission	*Amendment*
(f) requests to access data, documents or ***any*** information necessary for the performance of their supervisory tasks;	(f) requests to access ***relevant*** data, documents or information necessary for the performance of their supervisory tasks;

Amendment 145
Proposal for a directive
Article 29 – paragraph 3

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

Amendment 146
Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning ***part or all the*** services or activities provided by an essential entity;	(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning ***relevant*** services or activities provided by an essential entity;

Amendment 147
Proposal for a directive
Article 29 – paragraph 5 – subparagraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) impose or request the imposition 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***

Amendment 148
Proposal for a directive
Article 30 – paragraph 1

Text proposed by the Commission	*Amendment*
1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through ex post supervisory measures.	1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary ***and taking into account a risk based approach***, through ex post supervisory measures.

Amendment 149
Proposal for a directive
Article 30 – paragraph 2 – point b

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

Amendment 150
Proposal for a directive
Article 30 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Where exercising their powers 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***.

Amendment 151
Proposal for a directive
Article 31 – paragraph 4

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

Amendment 152
Proposal for a directive
Article 32 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation within ***a reasonable period of time***.	1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ***without undue delay and in any event*** within ***72 hours***.

Amendment 153
Proposal for a directive
Article 32 – paragraph 3

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

Amendment 154
Proposal for a directive
Article 36 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The power to adopt delegated acts referred to in Articles ***18(6) and 21(2)*** shall be conferred on the Commission for a period of five years from […]	2. The power to adopt delegated acts referred to in Articles ***18(5) and 20(3)*** shall be conferred on the Commission for a period of five years from […]

Amendment 155
Proposal for a directive
Article 36 – paragraph 3

Text proposed by the Commission	*Amendment*
3. ***The delegation of power referred to in*** Articles ***18(6) and 21(2) may be revoked at any time*** by the European Parliament or by the Council***. A decision to revoke shall put an end*** to the ***delegation of the power specified in that decision. It*** shall ***take effect the day following the publication of the decision in the Official Journal*** of the European ***Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force***.	3. ***A delegated act adopted pursuant to*** Articles ***18(5) and 20(3) shall enter into force only if no objection has been expressed either*** by the European Parliament or by the Council ***within a period of three months of notification of that act*** to the ***European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period*** shall ***be extended by three months at the initiative*** of the European ***Parliament or of the Council***.

Amendment 156
Proposal for a directive
Article 36 – paragraph 6

Text proposed by the Commission	*Amendment*
6. A delegated act adopted pursuant to Articles ***18(6) and 21(2)*** shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a	6. A delegated act adopted pursuant to Articles ***18(5) and 20(3)*** shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a

period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

ANNEX: LIST OF ENTITIES OR PERSONS FROM WHOM THE RAPPORTEUR HAS RECEIVED INPUT

The following list is drawn up on a purely voluntary basis under the exclusive responsibility of the rapporteur. The rapporteur has received input from the following entities or persons in the preparation of the opinion, until the adoption thereof in committee:

Person	Entity
	BSA (The Software Alliance)
	BusinessEurope
	Confederation of Danish Industries
	Danish Permanent Representation
	Deutsche Telekom
	Digital Europe
	DOT Europe
	ETNO (European Telecommunications Network Operators)
	French Permanent Representation
	German Permanent Representation
	HUAWEI
	IFPI
	INTEL
	ITI (The Information Technology Industry Council)
	Kaspersky
	MÆRSK
	Microsoft
	ICANN
	MOTION PICTURE ASSOCIATION
	Orgalim
	Palo Alto Networks

	Rettighedsalliancen

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
References	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Committee responsible Date announced in plenary	ITRE 21.1.2021
Opinion by Date announced in plenary	IMCO 21.1.2021
Rapporteur for the opinion Date appointed	Morten Løkkegaard 9.2.2021
Discussed in committee	26.5.2021 21.6.2021
Date adopted	12.7.2021
Result of final vote	+: 42 –: 1 0: 2
Members present for the final vote	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Andrea Caroppo, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Carlo Fidanza, Evelyne Gebhardt, Alexandra Geese, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Antonius Manders, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Marco Zullo
Substitutes present for the final vote	Clara Aguilera, Maria da Graça Carvalho, Christian Doleschal, Claude Gruffat, Jiří Pospíšil, Kosma Złotowski

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

42	+
ECR	Adam Bielan, Carlo Fidanza, Kosma Złotowski
ID	Alessandra Basso, Hynek Blaško, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle
PPE	Pablo Arias Echeverría, Andrea Caroppo, Maria da Graça Carvalho, Deirdre Clune, Christian Doleschal, Andrey Kovatchev, Antonius Manders, Jiří Pospíšil, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Sandro Gozi, Morten Løkkegaard, Marco Zullo
S&D	Alex Agius Saliba, Clara Aguilera, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Claude Gruffat, Marcel Kolaja

1	-
NI	Miroslav Radačovský

2	0
ECR	Eugen Jurzyca
Renew	Svenja Hahn

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