European Parliament
2019-2024

Committee on the Internal Market and Consumer Protection

2020/0359(COD)

4.5.2021

DRAFT 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 8

Text proposed by the Commission	*Amendment*
(8) In accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services ('identification process'). In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[15] , that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion.	(8) In accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services ('identification process'). In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[15] , that operate within the sectors or provide the type of services covered by this Directive, fall within its scope ***except for those specific entities which are identified as non-critical by Member States***. Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion.
[15] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	[15] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Or. en

Amendment 2

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, may issue guidelines on the implementation of the criteria applicable to micro and small enterprises ***and for non-critical entities***.

Or. en

Amendment 3

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.

Or. en

Amendment 4

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***	(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. ***This*** should not discharge

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.

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.

Or. en

Amendment 5

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 should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime.

Or. en

Amendment 6

Proposal for a directive
Recital 55

Text proposed by the Commission	*Amendment*
(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within ***24*** hours, followed by a final report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of ***24*** hours for the initial notification and one month for the final report.	(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within ***72*** 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 ***72*** hours for the initial notification and one month for the final report.

Or. en

Amendment 7

Proposal for a directive
Recital 69

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

Or. en

Amendment 8

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, 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.

Or. en

Amendment 9

Proposal for a directive
Recital 76

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

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.

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

Or. en

Amendment 10

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	(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.	establishing which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes***. The Commission should also be empowered to adopt delegated acts establishing the technical elements related to risk management measures or the type of information***. 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.

Or. en

Amendment 11

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	(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

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).

(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).

Or. en

Amendment 12

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 citizens and economic operators, and to improve the functioning of the internal market***.

Or. en

Amendment 13

Proposal for a directive
Article 2 – paragraph 1

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

Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.[28]	Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC[28]***, without prejudice to their active and voluntary inclusion in the scope. This Directive does not apply to the entities that Member States identify as non-critical, including where they are of a type referred to in Annex I and Annex II.***
[28] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	[28] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Or. en

Justification

The extended scope of the NIS2 proposal with a sector-based approach is welcomed. A minor window for the exclusion of clearly non-critical entities, otherwise covered by the scope, is suggested, to not blindly expose entities with obligations and burdens that do not match their current, or future, threat-level.

Amendment 14

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

Text proposed by the Commission	*Amendment*
	(26a) 'non critical entity' means any entity of a type referred to in Annex I and II which has no critical function in that specific sector or type of service provided and has a low level of dependency from other sectors or types of services.

Or. en

Amendment 15

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

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

Or. en

Amendment 16

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***;

Or. en

Amendment 17

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

Text proposed by the Commission	*Amendment*
(e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives;	(e) a policy on promoting and developing ***trust of users and*** cybersecurity skills, awareness raising and research and development initiatives;

Or. en

Justification

The amendment has been added to be more consumer end and user focused.

Amendment 18

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;

Or. en

Amendment 19

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

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

Or. en

Amendment 20

Proposal for a directive
Article 6 – paragraph 2

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

Or. en

Justification

The amendment has been adjusted to include a stronger degree of respect for company sensitive information.

Amendment 21

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.

Or. en

Amendment 22

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.

Or. en

Amendment 23

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

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

Or. en

Justification

In strengthening the cybersecurity of the Union, a simultaneous strengthening of our mutual tool in handling the relationship between the Union and third countries (EEAS) is considered

beneficial to ensure continued strong cybersecurity understanding and defence.

Amendment 24

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

Text proposed by the Commission	*Amendment*
Where appropriate, the Cooperation Group may invite representatives of relevant stakeholders to participate in its work.	Where appropriate, the Cooperation Group may invite representatives of relevant ***Union bodies and agencies as well as*** stakeholders to participate in its work.

Or. en

Amendment 25

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***;

Or. en

Justification

In order to live up to the ambitions set out by NIS2 and address the differential implementation of NIS1, this amendment is added to ensure uniform implementation of the NIS2 in the Member States.

Amendment 26

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;

Or. en

Amendment 27

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;

Or. en

Amendment 28

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

Text proposed by the Commission	*Amendment*
(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives;	(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives***, and with the European External Action Service on geopolitical aspects of the cybersecurity in the Union***;

Or. en

Justification

In strengthening the cybersecurity of the Union, a simultaneous strengthening of our mutual tool in handling the relationship between the Union and third countries (EEAS) is considered beneficial to ensure continued strong cybersecurity understanding and defence.

Amendment 29

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

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

Or. en

Justification

In order to live up to the ambitions set out by NIS2 and address the differential implementation of NIS1, this amendment is added to ensure transparent implementation of the NIS2 in the Member States.

Amendment 30

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.

Or. en

Amendment 31

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.

Or. en

Amendment 32

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***;

Or. en

Amendment 33

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***;

Or. en

Amendment 34

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 an incident having a cross-border nature;

Or. en

Amendment 35

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

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

Or. en

Amendment 36

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***;

Or. en

Justification

The amendment is suggested in order to ensure that no Member State CSIRT may avoid being scrutinised.

Amendment 37

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	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

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.	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.

Or. en

Amendment 38

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***.

Or. en

Amendment 39

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.

Or. en

Amendment 40

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

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

Or. en

Justification

This amendment is proposed to ensure parliamentary scrutiny and oversight with the state of cybersecurity in the Union.

Amendment 41

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***, the overall degree of resilience of the internal market towards cyber threats and the level of implementation of the Directive across the Member States***;

Or. en

Justification

To have a better picture of the overall level of cybersecurity in the internal market, the proposal is amended to include an analysis of degree of resilience and of the level of implementation of the Directive.

Amendment 42

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 cybersecurity in the Union.

Or. en

Justification

The amendment is suggested to take into account the fact that increasing cybersecurity threats today are stemming from geopolitical actors outside the Union. Considering the geopolitical aspects may help to increase the overall awareness and ability to resist cyber threats with external roots.

Amendment 43

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

Text proposed by the Commission	*Amendment*
1. The Commission shall establish, after consulting the Cooperation Group and ENISA, and at the latest by ***18*** months following the entry into force of this Directive, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The reviews shall be conducted by cybersecurity technical experts drawn from Member States different than the one reviewed and shall cover at least the following:	1. The Commission shall establish, after consulting the Cooperation Group and ENISA, and at the latest by ***12*** months following the entry into force of this Directive, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The reviews shall be conducted by cybersecurity technical experts drawn from ***at least two*** Member States different than the one reviewed and shall cover at least the following:

Or. en

Amendment 44

Proposal for a directive
Article 18 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities shall take ***appropriate and proportionate*** technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.	1. Member States shall ensure that essential and important entities shall take technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. ***Those measures shall be appropriate and proportionate to the level of criticality of the sector or of the type of service, as well as the level of dependency of the entity from other sectors or types of services, and shall be adopted following a risk-based assessment.*** Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.

Or. en

Amendment 45

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

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

Or. en

Justification

This amendment is added to clarify what is expected of the essential and important entities in addressing their supply chain security.

Amendment 46

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 and an evaluation of the possible mandatory use of these tools;***

Or. en

Amendment 47

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.

Or. en

Justification

In order not to overburden entities, a minor adjustment is suggested providing some limit to the extend of responsibility of the entities.

Amendment 48

Proposal for a directive
Article 18 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission ***may*** adopt ***implementing*** acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2***. Where preparing those acts***, ***the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2)*** and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.	5. The Commission ***is empowered to*** adopt ***delegated*** acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2, and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.

Or. en

Amendment 49

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

Text proposed by the Commission	*Amendment*
	6a. The Commission in cooperation with the Cooperation Group and ENISA, shall provide guidance and best practices on the compliance by entities in a proportionate manner with the requirements, laid down in paragraph 2, and in particular to the requirement in point (d) of that paragraph.

Or. en

Amendment 50

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	1. ***In view to increase the overall level of cybersecurity,*** the Cooperation Group, in cooperation with the

risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.	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***.

Or. en

Amendment 51

Proposal for a directive
Article 20 – paragraph 2

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

Or. en

Justification

The phrase "could have potentially resulted in a significant incident" appears too ambiguous to be given legal effect.

Amendment 52

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;

Or. en

Justification

The phrase "or has the potential to cause" appears too ambiguous to be given legal effect.

Amendment 53

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.

Or. en

Justification

The phrase "or has the potential to affect" appears too ambiguous to be given legal effect.

Amendment 54

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	(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;	notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;

Or. en

Justification

The proposed 24 hour notification deadline risks distracting companies from addressing an on-going cyber attack in their systems at a most crucial time. The rapporteur proposes to extend this deadline to 72 hours for companies to be able to firstly address the on-going attack and then to comply with the notification obligation.

Amendment 55

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;

Or. en

Amendment 56

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 paragraphs 1 to the single points of contact of other affected Member States.

Or. en

Amendment 57

Proposal for a directive
Article 20 – paragraph 9

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

Or. en

Amendment 58

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 paragraphs 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].

Or. en

Amendment 59

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 paragraphs 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).

Or. en

Amendment 60

Proposal for a directive
Article 21 – paragraph 1

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

Or. en

Amendment 61

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.

Or. en

Justification

The amendment is added to promote the development of harmonised standards of cybersecurity in the Union.

Amendment 62

Proposal for a directive
Article 23 – paragraph 1

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

Or. en

Amendment 63

Proposal for a directive
Article 23 – paragraph 4

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

Or. en

Amendment 64

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

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

Or. en

Amendment 65

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. ***At the request of essential and important entities, the Cooperation Group shall be invited to provide best practices and guidance.***

Or. en

Amendment 66

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 cyberthreats 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.

Or. en

Justification

This amendment is added, in order to allow essential and important entities to share information, on a voluntary basis, regarding so-called potential incidents, if and when it might prove relevant, without thereby being subject to further obligations.

Amendment 67

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;

Or. en

Amendment 68

Proposal for a directive
Article 29 – paragraph 5 – 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;

Or. en

Amendment 69

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

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

Or. en

Amendment 70

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.

Or. en

Amendment 71

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

Text proposed by the Commission	*Amendment*
(e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks.	(e) requests to access ***relevant*** data, documents and/or information necessary for the performance of the supervisory tasks.

Or. en

Amendment 72

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	6. A delegated act adopted pursuant to Articles ***18 (5) and (6),*** and 21(2) shall

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.	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.

Or. en