EUROPEAN PARLIAMENT 2009 - 2014

Committee on Industry, Research and Energy

2013/0027(COD)

19.11.2013

AMENDMENTS
128 - 362

Draft opinion
Pilar del Castillo Vera
(PE519.596v01-00)

Measures to ensure a high common level of network and information security across the Union

Proposal for a directive
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

AM_Com_LegOpinion

Amendment 128
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 1

Text proposed by the Commission	*Amendment*
(1) Network and information systems and services play a vital role in the society. Their reliability and security are essential to economic activities and social welfare, and in particular to the functioning of the internal market.	(1) Network and information systems and services play a vital role in the society. Their reliability and security are essential to ***the freedom and overall security for the citizens of the EU as well as to*** economic activities and social welfare, and in particular to the functioning of the internal market.

Or. en

Amendment 129
Krišjānis Kariņš

Proposal for a directive
Recital 2

Text proposed by the Commission	*Amendment*
(2) The magnitude and frequency of ***deliberate or accidental*** security incidents is increasing and represents a major threat to the functioning of networks and information systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.	(2) The magnitude and frequency of security incidents is increasing and represents a major threat to the functioning of networks and information systems. ***These systems may also become an easy target for deliberate harmful actions intended to damage or interrupt the operation of the systems.*** Such incidents can ***threaten the health and safety of the population,*** impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

Or. lv

Amendment 130
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 2

Text proposed by the Commission	*Amendment*
(2) The magnitude and frequency of deliberate or accidental security incidents is increasing and represents a major threat to the functioning of networks and information systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.	(2) The magnitude and frequency of deliberate or accidental security incidents is increasing and represents a major threat to the functioning of networks and information systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user ***and investor*** confidence and cause major damage to the economy of the Union.

Or. en

Justification

Cyber attacks on stock listed companies are widespread and include theft of financial assets, intellectual property, or the disruption of operations of their customers or their business partners and could have an impact on shareholder relations as well as on the decision of potential investors.

Amendment 131
Ioannis A. Tsoukalas

Proposal for a directive
Recital 2

Text proposed by the Commission	*Amendment*
(2) The magnitude ***and frequency*** of deliberate or accidental security incidents is increasing and represents a major threat to the functioning of networks and information systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the	(2) The magnitude***, frequency and impact*** of deliberate or accidental security incidents is increasing and represents a major threat to the functioning of networks and information systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the

Union.	Union.

Or. en

Amendment 132
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 3

Text proposed by the Commission	*Amendment*
(3) As a communication instrument without frontiers, digital information systems, and primarily the Internet play an essential role in facilitating the cross-border movement of goods, services and people. Due to that transnational nature, substantial disruption of those systems in one Member State can also affect other Member States and the Union as a whole. The resilience and stability of network and information systems is therefore essential to the smooth functioning of the internal market.	(3) As a communication instrument without ***traditional*** frontiers, digital information systems, and primarily the Internet play an essential role in facilitating the cross-border movement of goods, services***, ideas*** and people. Due to that transnational nature, substantial disruption of those systems in one Member State can also affect other Member States and the Union as a whole. The resilience and stability of network and information systems is therefore essential to the smooth functioning of the internal market ***and moreover to the functioning of external markets, too***.

Or. en

Justification

The resilience and stability of network and information systems of the internal market are also vital for the interaction with global and regional markets such as North America or Asia etc.

Amendment 133
Gunnar Hökmark

Proposal for a directive
Recital 4

Text proposed by the Commission	*Amendment*
(4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated detection and response regarding network and information security ('NIS'). For that mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS in their territory. Minimum security requirements should also apply to public administrations and operators of critical information infrastructure to promote a culture of risk management and ensure that the most serious incidents are reported.	(4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated detection and response regarding network and information security ('NIS'). For that mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS in their territory. Minimum security requirements should also apply to public administrations and operators of critical information infrastructure to promote a culture of risk management and ensure that the most serious incidents are reported. ***The legal framework must be based upon the need to safeguard the privacy and integrity of citizens***

Or. en

Amendment 134
Ivailo Kalfin

Proposal for a directive
Recital 4

Text proposed by the Commission	*Amendment*
(4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated detection and response regarding network and information security ('NIS'). For that mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS in their territory. Minimum security requirements should also apply to public administrations and operators of critical information infrastructure to promote a culture of risk management and ensure that the most	(4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated detection and response regarding network and information security ('NIS'). For that mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS in their territory. Minimum security requirements should also apply to public administrations and ***public and private*** operators of critical information infrastructure to promote a culture of risk management and ensure that

serious incidents are reported.	the most serious incidents are reported. ***The Critical Infrastructure Warning Information Network (CIWIN) should be expanded to these particular operators.***

Or. en

Amendment 135
Ioannis A. Tsoukalas

Proposal for a directive
Recital 4

Text proposed by the Commission	*Amendment*
(4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated detection and response regarding network and information security ('NIS'). For that mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS in their territory. Minimum security requirements should also apply to public administrations and operators of critical information infrastructure to promote a culture of risk management and ensure that the most serious incidents are reported.	(4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated ***prevention,*** detection and response regarding network and information security ('NIS'). For that mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS in their territory. Minimum security requirements should also apply to public administrations and operators of critical information infrastructure to promote a culture of risk management and ensure that the most serious incidents are reported.

Or. en

Amendment 136
Christian Ehler, Manfred Weber, Maria Da Graça Carvalho

Proposal for a directive
Recital 4

Text proposed by the Commission	*Amendment*
(4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated	(4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated

detection and response regarding network and information security ('NIS'). For that mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS in their territory. Minimum security requirements should also apply to public administrations ***and*** operators of critical information infrastructure to promote a culture of risk management and ensure that the most serious incidents are reported.	detection and response regarding network and information security ('NIS'). For that mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS in their territory. Minimum security requirements should also apply to public administrations**,** operators of critical information infrastructure ***and stock listed companies*** to promote a culture of risk management and ensure that the most serious incidents are reported.

Or. en

Justification

Security breaches of stock listed companies could materially affect the company's products, services, relationships with customers or suppliers, and overall competitive conditions and therefore could have major impacts on the functioning of the internal (and external) market. Therefore stock listed companies should be covered by this Directive as well.

Amendment 137
Amelia Andersdotter

Proposal for a directive
Recital 4

Text proposed by the Commission	*Amendment*
(4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated detection and response regarding network and information security ('NIS'). For that mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS in their territory. Minimum security requirements should also apply to public administrations and operators ***of critical information infrastructure*** to promote a culture of risk management and ensure that ***the most***	(4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated detection and response regarding network and information security ('NIS'). For that mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS in their territory. Minimum security requirements should also apply to public administrations and ***market*** operators to promote a culture of risk management and ensure that incidents are reported.

serious incidents are reported.

Or. en

Amendment 138
Gunnar Hökmark

Proposal for a directive
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4a) To secure that governments do not exceed or misuse their powers, it is of vital importance that information and security systems of public authorities are transparent, legitimate, well-defined and adopted in a transparent manner through a democratic process.

Or. en

Amendment 139
Amelia Andersdotter

Proposal for a directive
Recital 5

Text proposed by the Commission	*Amendment*
(5) To cover all relevant incidents and risks, this Directive should apply to all network and information systems. ***The obligations on public administrations and market operators should however not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)[25] , which***	(5) To cover all relevant incidents and risks, this Directive should apply to all network and information systems.

are subject to the specific security and integrity requirements laid down in Article 13a of that Directive nor should they apply to trust service providers.

[25] OJ L 108, 24.4.2002, p. 33.

[25] OJ L 108, 24.4.2002, p. 33.

Or. en

Amendment 140
Ivailo Kalfin

Proposal for a directive
Recital 5

Text proposed by the Commission	*Amendment*
(5) To cover all relevant incidents and risks, this Directive should apply to ***all*** network and information systems***. The obligations on public administrations and market operators*** should however not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)[25] , which are subject to the specific security and integrity requirements laid down in Article 13a of that Directive nor should they apply to trust service providers.	(5) To cover all relevant incidents and risks, this Directive should apply to network and information systems***, providing and/ or operating services, as listed in Article (3(8) b) of this Directive. The obligations*** should however not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)25, which are subject to the specific security and integrity requirements laid down in Article 13a of that Directive nor should they apply to trust service providers.

[25] OJ L 108, 24.4.2002, p. 33.

[25] OJ L 108, 24.4.2002, p. 33.

Or. en

Amendment 141
Jürgen Creutzmann

Proposal for a directive
Recital 5

Text proposed by the Commission	*Amendment*
(5) ***To cover all relevant incidents and risks,*** this Directive should apply to all network and information systems. The obligations on public administrations and market operators should however not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)[25] , which are subject to the specific security and integrity requirements laid down in Article 13a of that Directive nor should they apply to trust service providers.	(5) This Directive should apply to all network and information systems. The obligations on public administrations and market operators should however not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)[25] , which are subject to the specific security and integrity requirements laid down in Article 13a of that Directive nor should they apply to trust service providers.
[25] OJ L 108, 24.4.2002, p. 33.	[25] OJ L 108, 24.4.2002, p. 33.

Or. en

Justification

There will always be incidents and risk that cannot be covered due to the sheer endless number of possibilities of incidents and the fast technological development in the ICT area. The deleted part could give the wrong impression that all risks could be completely mitigated, which is, at least with a reasonable effort and resources, not possible.

Amendment 142
Christian Ehler, Manfred Weber

Proposal for a directive
Recital 5

Text proposed by the Commission	*Amendment*
(5) To cover all relevant incidents and risks, this Directive should apply to all network and information systems. The obligations on public administrations and market operators should however not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)[25] , which are subject to the specific security and integrity requirements laid down in Article 13a of that Directive ***nor should they apply to trust service providers***.	(5) To cover all relevant incidents and risks, this Directive should apply to all network and information systems. The obligations on public administrations and market operators should however not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)[25] , which are subject to the specific security and integrity requirements laid down in Article 13a of that Directive.
[25] OJ L 108, 24.4.2002, p. 33.	[25] OJ L 108, 24.4.2002, p. 33.

Or. en

Justification

Trust Service Providers have a vital role in securing economic, financial and other transactions in the field of eCommerce, eGovernment, eBanking etc. Therefore they should not be excluded per se.

Amendment 143
Ioannis A. Tsoukalas

Proposal for a directive
Recital 6

Text proposed by the Commission	*Amendment*
(6) The existing capabilities are not sufficient enough to ensure a high level of NIS within the Union. Member States have very different levels of preparedness leading to fragmented approaches across	(6) The existing capabilities are not sufficient enough to ensure a high level of NIS within the Union. Member States have very different levels of preparedness leading to fragmented approaches across

the Union. This leads to an unequal level of protection of consumers and businesses, and undermines the overall level of NIS within the Union. Lack of common minimum requirements on public administrations and market operators in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level.	the Union. This leads to an unequal level of protection of consumers and businesses, and undermines the overall level of NIS within the Union. Lack of common minimum requirements on public administrations and market operators in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level ***and undermines the Union's leading position internationally in safeguarding and promoting a free, efficient and secure internet***.

Or. en

Amendment 144
Amelia Andersdotter

Proposal for a directive
Recital 7

Text proposed by the Commission	*Amendment*
(7) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information and coordination of actions, and common minimum security requirements for all market operators ***concerned*** and public administrations.	(7) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information and coordination of actions, and common minimum security requirements for all market operators and public administrations.

Or. en

Amendment 145
Ioannis A. Tsoukalas

Proposal for a directive
Recital 7

Text proposed by the Commission	*Amendment*
(7) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information and coordination of actions, and common minimum security requirements for all market operators concerned and public administrations.	(7) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, ***developing sufficient cybersecurity skills,*** exchange of information and coordination of actions, and common minimum security requirements for all market operators concerned and public administrations.

Or. en

Amendment 146
Ivailo Kalfin

Proposal for a directive
Recital 7

Text proposed by the Commission	*Amendment*
(7) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information and coordination of actions, and common minimum security requirements ***for all market operators concerned and public administrations***.	(7) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information and coordination of actions, and common minimum security requirements.

Or. en

Amendment 147
Christian Ehler, Manfred Weber

Proposal for a directive
Recital 7

Text proposed by the Commission	*Amendment*
(7) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information and coordination of actions, and common minimum security requirements for all market operators concerned and public administrations.	(7) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information and coordination of actions, and common minimum security requirements for all market operators concerned and public administrations. ***Minimal common standards should be applied in accordance with appropriate recommendations by the Cyber Security Co-Ordination Groups (CSGC).***

Or. en

Amendment 148
Amelia Andersdotter

Proposal for a directive
Recital 8

Text proposed by the Commission	*Amendment*
(8) The provisions of this Directive should be without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of its essential security interests, to safeguard public policy and public security, and to permit the investigation, detection and prosecution of criminal offences. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security.	***deleted***

Or. en

Amendment 149
Ioannis A. Tsoukalas

Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(9) To achieve and maintain a common high level of security of network and information systems, each Member State should have a national NIS strategy defining the strategic objectives and concrete policy actions to be implemented. NIS cooperation plans complying with essential requirements need to be developed at national level in order to reach capacity response levels allowing for effective and efficient cooperation at national and Union level in case of incidents.	(9) To achieve and maintain a common high level of security of network and information systems, each Member State should have a national NIS strategy defining the strategic objectives and concrete policy actions to be implemented. NIS cooperation plans complying with essential requirements need to be developed at national level in order to reach capacity response levels allowing for effective and efficient cooperation at national and Union level in case of incidents. ***Member States may ask for the assistance of the European Network and Information Security Agency ('ENISA') in developing their national NIS strategies, based on a common minimum NIS strategy blueprint.***

Or. en

Justification

ENISA is already acknowledged by relevant stakeholders as a highly competent centre of excellence and a trustworthy tool for promoting cybersecurity in the EU. Therefore the EU should avoid duplication of efforts and structures by building upon ENISA's know-how and require ENISA to offer counselling services to those Member States that lack NIS institutions and expertise and make a request for this kind of support.

Amendment 150
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(9) To achieve and maintain a common high level of security of network and information systems, each Member State should have a national NIS strategy defining the strategic objectives and concrete policy actions to be implemented. NIS cooperation plans complying with essential requirements need to be developed at national level in order to reach capacity response levels allowing for effective and efficient cooperation at national and Union level in case of incidents.	(9) To achieve and maintain a common high level of security of network and information systems, each Member State should have a national NIS strategy defining the strategic objectives and concrete policy actions to be implemented. NIS cooperation plans complying with essential requirements need to be developed at national level in order to reach capacity response levels allowing for effective and efficient cooperation at national and Union level in case of incidents. ***Each Member State should therefore be obliged to meet common standards regarding data format and the exchangeability of data to be shared and evaluated.***

Or. en

Justification

Interoperability has to be ensured.

Amendment 151
Amelia Andersdotter

Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(9) To achieve and maintain a common high level of security of network and information systems, each Member State should have a national NIS strategy defining the strategic objectives and concrete policy actions to be implemented. NIS cooperation plans complying with essential requirements need to be developed at national level in order to reach capacity response levels allowing for	(9) To achieve and maintain a common high level of security of network and information systems, each Member State should have a national NIS strategy defining the strategic objectives and concrete policy actions to be implemented. NIS cooperation plans complying with essential requirements need to be developed at national level***, on the basis of minimum requirements set in this***

effective and efficient cooperation at national and Union level in case of incidents.

Directive, in order to reach capacity response levels allowing for effective and efficient cooperation at national and Union level in case of incidents.

Or. en

Amendment 152
Ivailo Kalfin

Proposal for a directive
Recital 10

Text proposed by the Commission	*Amendment*
(10) To allow for the effective implementation of the provisions adopted pursuant to this Directive, a body responsible for coordinating NIS issues and acting as a focal point for cross-border cooperation at Union level should be established or identified in each Member State. These bodies should be given the adequate technical, financial and human resources to ensure that they can carry out in an effective and efficient manner the tasks assigned to them and thus achieve the objectives of this Directive.	(10) To allow for the effective implementation of the provisions adopted pursuant to this Directive, a body responsible for coordinating NIS issues and acting as a ***single*** focal point for ***both internal coordination and*** cross-border cooperation at Union level should be established or identified in each Member State. These ***single national points of contact should be designated without prejudice for each Member State to designate more than one national competent authority in charge of network information security, according to their constitutional, jurisdictional or administrative requirements, but should nonetheless be assigned with a coordinating mandate at national and Union level. These*** bodies should be given the adequate technical, financial and human resources to ensure that they can carry out in a ***continuous,*** effective and efficient manner the tasks assigned to them and thus achieve the objectives of this Directive.

Or. en

Amendment 153
Amelia Andersdotter

Proposal for a directive
Recital 10

Text proposed by the Commission	*Amendment*
(10) To allow for the effective implementation of the provisions adopted pursuant to this Directive, a body responsible for coordinating NIS issues and acting as a focal point for cross-border cooperation at Union level should be established or identified in each Member State. These bodies should be given the adequate technical, financial and human resources to ensure that they can carry out in an effective and efficient manner the tasks assigned to them and thus achieve the objectives of this Directive.	(10) To allow for the effective implementation of the provisions adopted pursuant to this Directive, a ***civilian*** body responsible for coordinating NIS issues and acting as a focal point for cross-border cooperation at Union level should be established or identified in each Member State ***in the form of an Industrial Control System Computer Emergency Response Team (ICS-CERT)***. These bodies should be given the adequate technical, financial and human resources to ensure that they can carry out in an effective and efficient manner the tasks assigned to them and thus achieve the objectives of this Directive.

Or. en

Amendment 154
Ivailo Kalfin

Proposal for a directive
Recital 11

Text proposed by the Commission	*Amendment*
(11) All Member States should be adequately equipped, both in terms of technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information systems' incidents and risks. Well-functioning Computer Emergency Response Teams complying with essential requirements should therefore be established in all Member States to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient	(11) All Member States should be adequately equipped, both in terms of technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information systems' incidents and risks. Well-functioning Computer Emergency Response Teams complying with essential requirements ***and continuous (24/7) mitigation and response capabilities*** should therefore be established in all Member States to guarantee effective and compatible capabilities to deal with

cooperation at Union level.

incidents and risks and ensure efficient cooperation at Union level. ***In view of the above, Member States should guarantee that each sectorial service, listed in Annex II of the present Directive, is covered by at least one CERT. Regarding cross border cooperation, Member States should assure that CERTs have sufficient means to participate in the respective international and European cooperation networks. The European Network Information Security Agency should provide the necessary assistance and advice for capacity building in case of need.***

Or. en

Amendment 155
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 11

Text proposed by the Commission	*Amendment*
(11) All Member States should be adequately equipped, both in terms of technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information systems' incidents and risks. Well-functioning Computer Emergency Response Teams complying with essential requirements should therefore be established in all Member States to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level.	(11) All Member States ***and market operators*** should be adequately equipped both in terms of technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information systems' incidents and risks. ***Commonly required equipment and capabilities ought to comply with commonly agreed technical standards as well as standards procedures of operation (SPO).*** Well-functioning Computer Emergency Response Teams complying with essential requirements should therefore be established in all Member States to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level. ***These CERTs should be enabled to interact on the basis of common technical standards and SPO.***

Or. en

Justification

Interoperability has to be ensured.

Amendment 156
Gunnar Hökmark

Proposal for a directive
Recital 11

Text proposed by the Commission	*Amendment*
(11) All Member States should be adequately equipped, both in terms of technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information systems' incidents and risks. Well-functioning Computer Emergency Response Teams complying with essential requirements should therefore be established in all Member States to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level.	(11) All Member States should be adequately equipped, both in terms of technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information systems' incidents and risks. Well-functioning Computer Emergency Response Teams complying with essential requirements should therefore be established in all Member States to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level. ***Security systems of public administrations must be safe and subject to democratic control and scrutiny.***

Or. en

Amendment 157
Amelia Andersdotter

Proposal for a directive
Recital 11

Text proposed by the Commission	*Amendment*
(11) All Member States should be adequately equipped, both in terms of technical and organisational capabilities, to	(11) All Member States should be adequately equipped, both in terms of technical and organisational capabilities, to

prevent, detect, respond to and mitigate network and information systems' incidents and risks. Well-functioning ***Computer Emergency Response Teams*** complying with essential requirements should therefore be established in all Member States to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level.	prevent, detect, respond to and mitigate network and information systems' incidents and risks. Well-functioning ***ICS-CERTs*** complying with essential requirements should therefore be established in all Member States to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level.

Or. en

Amendment 158
Amelia Andersdotter

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) Building upon the significant progress within the European Forum of Member States ('EFMS') in fostering discussions and exchanges on good policy practices including the development of principles for European ***cyber crisis*** cooperation, the Member States and the Commission should form a network to bring them into permanent communication and support their cooperation. ***This secure and effective cooperation mechanism should enable structured and coordinated information exchange, detection and response at Union level.***	(12) Building upon the significant progress within the European Forum of Member States ('EFMS') in fostering discussions and exchanges on good policy practices including the development of principles for European ***e-crisis*** cooperation, the Member States and the Commission should form an ***institutional*** network to bring them into permanent communication and support their cooperation.

Or. en

Amendment 159
Ioannis A. Tsoukalas

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) Building upon the significant progress within the European Forum of Member States ('EFMS') in fostering discussions and exchanges on good policy practices including the development of principles for European cyber crisis cooperation, the Member States and the Commission should form a network to bring them into permanent communication and support their cooperation. This secure and effective cooperation mechanism should enable structured and coordinated information exchange, detection and response at Union level.	(12) Building upon the significant progress within the European Forum of Member States ('EFMS') in fostering discussions and exchanges on good policy practices including the development of principles for European cyber crisis cooperation, the Member States and the Commission should form a network***, under the coordination of ENISA,*** to bring them into permanent communication and support their cooperation. This secure and effective cooperation mechanism should enable structured and coordinated information exchange, detection and response at Union level.

Or. en

Amendment 160
Ivailo Kalfin

Proposal for a directive
Recital 13

Text proposed by the Commission	*Amendment*
(13) The European Network and Information Security Agency ('ENISA') should assist the Member States and the Commission by providing its expertise and advice and by facilitating exchange of best practices. In particular, in the application of this Directive, the Commission should consult ENISA. To ensure effective and timely information to the Member States and the Commission, early warnings on incidents and risks should be notified within the cooperation network. To build capacity and knowledge among Member States, the cooperation network should also serve as an instrument for the exchange of best practices, assisting its members in building capacity, steering the organisation	(13) The European Network and Information Security Agency ('ENISA') should assist the Member States and the Commission by providing its expertise and advice and by facilitating exchange of best practices. In particular, in the application of this Directive, the Commission ***and Member States*** should consult ENISA. To ensure effective and timely information to the Member States and the Commission, early warnings on incidents and risks should be notified within the cooperation network. To build capacity and knowledge among Member States, the cooperation network should also serve as an instrument for the exchange of best practices, assisting its members in building capacity, steering

of peer reviews and NIS exercises.	the organisation of peer reviews and NIS exercises.

Or. en

Amendment 161
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 13

Text proposed by the Commission	*Amendment*
(13) The European Network and Information Security Agency ('ENISA') should assist the Member States and the Commission by providing its expertise and advice and by facilitating exchange of best practices. In particular, in the application of this Directive, the Commission should consult ENISA. To ensure effective and timely information to the Member States and the Commission, early warnings on incidents and risks should be notified within the cooperation network. To build capacity and knowledge among Member States, the cooperation network should also serve as an instrument for the exchange of best practices, assisting its members in building capacity, steering the organisation of peer reviews and NIS exercises.	(13) The European Network and Information Security Agency ('ENISA') should assist the Member States and the Commission by providing its expertise and advice and by facilitating exchange of best practices. In particular, in the application of this Directive, the Commission should consult ENISA. To ensure effective and timely information to the Member States and the Commission, early warnings on incidents and risks should be notified within the cooperation network. To build capacity and knowledge among Member States, the cooperation network should also serve as an instrument for the exchange of best practices, assisting its members in building capacity, steering the organisation of peer reviews and NIS exercises.

Or. en

Amendment 162
Amelia Andersdotter

Proposal for a directive
Recital 14

Text proposed by the Commission	*Amendment*
(14) A secure information-sharing infrastructure should be put in place to	***deleted***

allow for the exchange of sensitive and confidential information within the cooperation network. Without prejudice to their obligation to notify incidents and risks of Union dimension to the cooperation network, access to confidential information from other Member States should only be granted to Members States upon demonstration that their technical, financial and human resources and processes, as well as their communication infrastructure, guarantee their effective, efficient and secure participation in the network.

Or. en

Amendment 163
Silvia-Adriana Ţicău
Proposal for a directive
Recital 14

Text proposed by the Commission	*Amendment*
(14) A secure information-sharing infrastructure should be put in place to allow for the exchange of sensitive and confidential information within the cooperation network. ***Without prejudice to their obligation to notify incidents and risks of Union dimension to the cooperation network, access to confidential information from other Member States should only be granted to Members States upon demonstration that their technical, financial and human resources and processes, as well as their communication infrastructure, guarantee their effective, efficient and secure participation in the network.***	(14) A secure information-sharing infrastructure should be put in place to allow for the exchange of sensitive and confidential information within the cooperation network, ***to which all Member States have access.***

Or. ro

Amendment 164
Ioannis A. Tsoukalas

Proposal for a directive
Recital 14

Text proposed by the Commission	*Amendment*
(14) A secure information-sharing infrastructure should be put in place to allow for the exchange of sensitive and confidential information within the cooperation network. Without prejudice to their obligation to notify incidents and risks of Union dimension to the cooperation network, access to confidential information from other Member States should only be granted to Members States upon demonstration that their technical, financial and human resources and processes, as well as their communication infrastructure, guarantee their effective, efficient and secure participation in the network.	(14) A secure information-sharing infrastructure should be put in place***, under the supervision of ENISA,*** to allow for the exchange of sensitive and confidential information within the cooperation network. Without prejudice to their obligation to notify incidents and risks of Union dimension to the cooperation network, access to confidential information from other Member States should only be granted to Members States upon demonstration that their technical, financial and human resources and processes, as well as their communication infrastructure, guarantee their effective, efficient and secure participation in the network.

Or. en

Amendment 165
Ivailo Kalfin

Proposal for a directive
Recital 15

Text proposed by the Commission	*Amendment*
(15) As most network and information systems are privately operated, cooperation between the public and private sector is essential. Market operators should be encouraged to pursue their own informal cooperation mechanisms to ensure NIS. They should also cooperate with the public sector and share information and best practices in exchange of operational support in case of incidents.	(15) As most network and information systems are privately operated, cooperation between the public and private sector is essential. Market operators should be encouraged to pursue their own informal cooperation mechanisms to ensure NIS. They should also cooperate with the public sector and ***mutually*** share information and best practices***, including the reciprocal*** in exchange of ***relevant information and*** operational support in case of incidents. ***To effectively encourage the sharing of information and of best practices, it is***

essential to ensure that market operators and critical public administrations, referred to in Article (3(8) b), who participate in such exchanges, are not disadvantaged as a result of their cooperation. Adequate safeguards are needed to ensure that such cooperation will not expose these operators to higher compliance risk or new liabilities under, inter alia, competition, intellectual property, data protection or cybercrime law, nor expose them to increase operational or security risks.

Or. en

Amendment 166
Jürgen Creutzmann

Proposal for a directive
Recital 15

Text proposed by the Commission	*Amendment*
(15) As most network and information systems are privately operated, cooperation between the public and private sector is essential. Market operators should be encouraged to pursue their own informal cooperation mechanisms to ensure NIS. They should also cooperate with the public sector and share information and best practices in exchange of operational support in case of incidents.	(15) As most network and information systems are privately operated, cooperation between the public and private sector is essential. Market operators should be encouraged to pursue their own informal cooperation mechanisms to ensure NIS. They should also cooperate with the public sector and share information and best practices in exchange of operational support ***and relevant information*** in case of incidents.

Or. en

Amendment 167
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 15

Text proposed by the Commission	*Amendment*
(15) As most network and information systems are privately operated, cooperation between the public and private sector is essential. Market operators should be encouraged to pursue their own informal cooperation mechanisms to ensure NIS. They should also cooperate with the public sector and share information and best practices in exchange of operational support in case of incidents.	(15) As most network and information systems are privately operated, cooperation between the public and private sector is essential. Market operators should be encouraged to pursue their own informal cooperation mechanisms to ensure NIS. They should also cooperate with the public sector and share information and best practices in exchange of operational support ***and information*** in case of incidents.

Or. en

Amendment 168
Ioannis A. Tsoukalas

Proposal for a directive
Recital 16

Text proposed by the Commission	*Amendment*
(16) To ensure transparency and properly inform EU citizens and market operators, ***the competent authorities*** should ***set up a common website to publish*** non confidential information on the incidents and risks.	(16) To ensure transparency and properly inform EU citizens and market operators, ***a common website*** should ***be setup by ENISA and the competent authorities where*** non confidential information on the incidents and risks ***is to be published***.

Or. en

Amendment 169
Ivailo Kalfin

Proposal for a directive
Recital 16

Text proposed by the Commission	*Amendment*
(16) To ensure transparency and properly inform EU citizens and market operators,	(16) To ensure transparency and properly inform EU citizens and market operators,

the competent authorities should set up a common website to publish non confidential information on the incidents and risks.	the ***national*** competent authorities***, functioning as single points of contact,*** should set up a common website ***at EU level*** to publish non confidential information on the incidents and risks.

Or. en

Amendment 170
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 16

Text proposed by the Commission	*Amendment*
(16) To ensure transparency and properly inform EU citizens and market operators, the competent authorities should set up a common website to publish non confidential information on the incidents and risks.	(16) To ensure transparency and properly inform EU citizens and market operators, the competent authorities should set up a common website to publish non confidential information on the incidents and risks ***and to eventually advise on appropriate maintenance measures***.

Or. en

Amendment 171
Amelia Andersdotter

Proposal for a directive
Recital 16

Text proposed by the Commission	*Amendment*
(16) To ensure transparency and properly inform EU citizens and market operators, the competent authorities should set up a common website to publish non confidential information on the incidents ***and risks***.	(16) To ensure transparency and properly inform EU citizens and market operators, the competent authorities should set up a common website to publish non confidential information on the incidents***, risks and ways of risk mitigation***.

Or. en

Amendment 172
Ivailo Kalfin

Proposal for a directive
Recital 17

Text proposed by the Commission	*Amendment*
(17) Where information is considered confidential in accordance with Union and national rules on business confidentiality, such confidentiality shall be ensured when carrying out the activities and fulfilling the objectives set by this Directive.	(17) ***The information classification policy referred to in Recital 14 should follow the ENISA recommended Information Sharing Traffic Light Protocol. Any information exchanged shall be classified and handled according to its level of sensitivity as determined by the source of the information.*** Where information is considered confidential in accordance with Union and national rules on business confidentiality, such confidentiality shall be ensured when carrying out the activities and fulfilling the objectives set by this Directive.

Or. en

Amendment 173
Christian Ehler, Manfred Weber

Proposal for a directive
Recital 18

Text proposed by the Commission	*Amendment*
(18) On the basis in particular of national crisis management experiences and in cooperation with ENISA, the Commission and the Member States should develop a Union NIS cooperation plan defining cooperation mechanisms to counter risks and incidents. That plan should be duly taken into account in the operation of early warnings within the cooperation network.	(18) On the basis in particular of national crisis management experiences and in cooperation with ENISA, the Commission and the Member States should develop a Union NIS cooperation plan defining cooperation mechanisms to ***prevent, detect, report, and*** counter risks and incidents. That plan should be duly taken into account in the operation of early warnings within the cooperation network.

Or. en

Amendment 174
Ioannis A. Tsoukalas

Proposal for a directive
Recital 18

Text proposed by the Commission	*Amendment*
(18) On the basis in particular of national crisis management experiences and in cooperation with ENISA, the Commission and the Member States should develop a Union NIS cooperation plan defining cooperation mechanisms to counter risks and incidents. That plan should be duly taken into account in the operation of early warnings within the cooperation network.	(18) On the basis in particular of national crisis management experiences and in cooperation with ENISA, the Commission and the Member States should develop a Union NIS cooperation plan defining cooperation mechanisms***, best practices and operation patterns*** to counter risks and incidents. That plan should be duly taken into account in the operation of early warnings within the cooperation network.

Or. en

Amendment 175
Amelia Andersdotter

Proposal for a directive
Recital 19

Text proposed by the Commission	*Amendment*
(19) Notification of an early warning within the network should be required only where the scale and severity of the incident or risk concerned are or may become so significant that information or coordination of the response at Union level is necessary. Early warnings should therefore be limited to actual or potential incidents or risks that grow rapidly, exceed national response capacity or affect more than one Member State. To allow for a proper evaluation, all information relevant for the assessment of the risk or incident should be communicated to the cooperation	***deleted***

network.

Or. en

Amendment 176
Amelia Andersdotter

Proposal for a directive
Recital 20

Text proposed by the Commission	*Amendment*
(20) Upon receipt of an early warning and its assessment, the competent authorities should agree on a coordinated response under the Union NIS cooperation plan. Competent authorities as well as the Commission should be informed about the measures adopted at national level as a result of the coordinated response.	***deleted***

Or. en

Amendment 177
Ioannis A. Tsoukalas

Proposal for a directive
Recital 20

Text proposed by the Commission	*Amendment*
(20) Upon receipt of an early warning and its assessment, the competent authorities should agree on a coordinated response under the Union NIS cooperation plan. Competent authorities as well as the Commission should be informed about the measures adopted at national level as a result of the coordinated response.	(20) Upon receipt of an early warning and its assessment, the competent authorities should agree on a coordinated response under the Union NIS cooperation plan. Competent authorities***, ENISA,*** as well as the Commission should be informed about the measures adopted at national level as a result of the coordinated response.

Or. en

Amendment 178
Ioannis A. Tsoukalas

Proposal for a directive
Recital 22

Text proposed by the Commission	*Amendment*
(22) Responsibilities in ensuring NIS lie to a great extent on public administrations and market operators. A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced should be promoted and developed through appropriate regulatory requirements and voluntary industry practices. Establishing a level playing field is also essential to the effective functioning of the cooperation network to ensure effective cooperation from all Member States.	(22) Responsibilities in ensuring NIS lie to a great extent on public administrations and market operators. A culture of risk management ***and close cooperation***, involving risk assessment***,*** and the implementation of security measures appropriate to the risks faced should be promoted and developed through appropriate regulatory requirements and voluntary industry practices. Establishing a level playing field is also essential to the effective functioning of the cooperation network to ensure effective cooperation from all Member States.

Or. en

Amendment 179
Amelia Andersdotter

Proposal for a directive
Recital 24

Text proposed by the Commission	*Amendment*
(24) Those obligations should be extended beyond the electronic communications sector to key providers of information society services, as defined in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services[27] , which underpin downstream information society services or on-line activities, such as e-commerce platforms, Internet payment	(24) Those obligations should be extended beyond the electronic communications sector to key providers of information society services, as defined in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services[27] , which underpin downstream information society services or on-line activities, such as e-commerce platforms, Internet payment

gateways, social networks, search engines, cloud computing services, application stores. ***Disruption of these enabling information society services prevents the provision of other information society services which rely on them as key inputs. Software developers and hardware manufacturers are not providers of information society services and are therefore excluded. Those obligations should also be extended to public administrations, and operators of critical infrastructure which rely heavily on information and communications technology and are essential to the maintenance of vital economical or societal functions such as electricity and gas, transport, credit institutions, stock exchange and health. Disruption of those network and information systems would affect the internal market.***

[27] OJ L 204, 21.7.1998, p. 37.

gateways, social networks, search engines, cloud computing services, application stores.

[27] OJ L 204, 21.7.1998, p. 37.

Or. en

Amendment 180
Ivailo Kalfin

Proposal for a directive
Recital 24

Text proposed by the Commission	*Amendment*
(24) Those obligations should be extended beyond the electronic communications sector to key providers ***of information society services, as defined in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of*** information ***in the field of technical standards and regulations and of rules on Information Society*** services[27] ***, which underpin*** downstream information society	(24) Those obligations should be extended beyond the electronic communications sector to ***public and private*** key providers ***and operators of critical infrastructure which rely heavily on information and communications technology and are essential to the maintenance of vital economical or societal functions such as electricity and gas, transport, financial institutions, stock exchange and health. Disruption of those network and***

services or on-line activities, such as e-commerce platforms, ***Internet payment gateways,*** social networks, search engines, ***cloud computing services,*** application stores***. Disruption of these enabling information society services prevents the provision of other information society services which rely on them as key inputs.*** Software developers and hardware manufacturers are not ***providers of information society services and are therefore excluded. Those obligations should also be extended to public administrations, and operators of critical infrastructure which rely heavily on information and communications technology and are essential to the maintenance of vital economical or societal functions such as electricity and gas, transport, credit institutions, stock exchange and health. Disruption of those network and information systems would affect the internal market***.

information ***systems would affect the internal market and the physical or financial integrity of the beneficiaries of the*** services ***they provide.*** Downstream information society services or on-line activities, such as e-commerce platforms, social networks, search engines, application stores***, as well as*** software developers and hardware manufacturers***,*** are not ***to be bound to any of the compulsory reporting within this Directive. Nonetheless, their voluntary reporting and information sharing with the competent authorities following the mechanisms, laid down in this Directive, is strongly recommended, particularly in the advent of severe incidents or disruptions***.

---

[27] OJ L 204, 21.7.1998, p. 37.

---

[27] OJ L 204, 21.7.1998, p. 37.

Or. en

Amendment 181
Christian Ehler, Manfred Weber

Proposal for a directive
Recital 24

Text proposed by the Commission	*Amendment*
(24) Those obligations should be extended beyond the electronic communications sector to key providers of information society services, as defined in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on	(24) Those obligations should be extended beyond the electronic communications sector to key providers of information society services, as defined in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on

Information Society services[27] , which underpin downstream information society services or on-line activities, such as e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services, application stores. Disruption of these enabling information society services prevents the provision of other information society services which rely on them as key inputs. ***Software developers and hardware manufacturers are not providers of information society services and are therefore excluded.*** Those obligations should also be extended to public administrations, and operators of critical infrastructure which rely heavily on information and communications technology and are essential to the maintenance of vital economical or societal functions such as electricity and gas, transport, credit institutions, stock exchange and health. Disruption of those network and information systems would affect the internal market.	Information Society services[27] , which underpin downstream information society services or on-line activities, such as e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services, application stores. Disruption of these enabling information society services prevents the provision of other information society services which rely on them as key inputs. Those obligations should also be extended to public administrations, and operators of critical infrastructure which rely heavily on information and communications technology and are essential to the maintenance of vital economical or societal functions such as electricity and gas, transport, credit institutions, stock exchange and health. Disruption of those network and information systems would affect ***the internal market. The obligations should also apply for stock listed companies due to their vital role for the functioning of*** the internal market.
[27] OJ L 204, 21.7.1998, p. 37.	[27] OJ L 204, 21.7.1998, p. 37.

Or. en

Justification

The Security chain begins and ends with solutions of hard-and software producers. Therefore they should not be excluded. Security breaches of stock listed companies could materially affect the company's products, services, relationships with customers or suppliers, and overall competitive conditions and therefore could have major impacts on the functioning of the internal (and external) market. Therefore stock listed companies should be covered by this Directive as well.

Amendment 182
Christian Ehler, Manfred Weber

Proposal for a directive
Recital 25

Text proposed by the Commission	*Amendment*
(25) Technical and organisational measures imposed to public administrations and market operators should not require that a particular commercial information and communications technology product be designed, developed or manufactured in a particular manner.	***deleted***

Or. en

Justification

This could exclude the possibility to create a European solution when needed, in particular in the field of common European standards therefore the paragraph should be deleted.

Amendment 183
Ioannis A. Tsoukalas

Proposal for a directive
Recital 25

Text proposed by the Commission	*Amendment*
(25) Technical and organisational measures imposed to public administrations and market operators should not require that a particular commercial information and communications technology product be designed, developed or manufactured in a particular manner.	(25) Technical and organisational measures imposed to public administrations and market operators should not require that a particular commercial information and communications technology product be designed, developed or manufactured in a particular manner. ***On the other hand, the use of international standards pertaining to cybersecurity should be required.***

Or. en

Amendment 184
Amelia Andersdotter

Proposal for a directive
Recital 27

Text proposed by the Commission	*Amendment*
(27) To avoid imposing a disproportionate financial and administrative burden on small operators and users, the requirements should be proportionate to the risk presented by the network or information system concerned, taking into account the state of the art of such measures. These requirements should not apply to micro enterprises.	***deleted***

Or. en

Amendment 185
Christian Ehler, Maria Da Graça Carvalho

Proposal for a directive
Recital 27

Text proposed by the Commission	*Amendment*
(27) To avoid imposing a disproportionate financial and administrative burden on small operators and users, the requirements should be proportionate to the risk presented by the network or information system concerned, taking into account the state of the art of such measures. ***These requirements should not apply to micro enterprises.***	(27) To avoid imposing a disproportionate financial and administrative burden on small operators and users, the requirements should be proportionate to the risk presented by the network or information system concerned, taking into account the state of the art of such measures.

Or. en

Justification

The size of the company is not always equal to the size of the safety relevance of their product.

Amendment 186
Amelia Andersdotter

Proposal for a directive
Recital 28

Text proposed by the Commission	*Amendment*
(28) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors. ***Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the public administrations and market operators reporting incidents.*** In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes.	(28) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors. In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes.

Or. en

Amendment 187
Ivailo Kalfin

Proposal for a directive
Recital 28

Text proposed by the Commission	*Amendment*
(28) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the public administrations and market operators	(28) Competent authorities***, including the single points of contact,*** should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors ***and should handle all information exchanged in accordance with the security classification, as indicated by its source***. Publicity of incidents reported to the competent authorities should duly balance the interest

reporting incidents. In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes.

of the public in being informed about threats with possible reputational and commercial damages for the public administrations and market operators reporting incidents. In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes.

Or. en

Amendment 188
Jürgen Creutzmann

Proposal for a directive
Recital 28

Text proposed by the Commission	*Amendment*
(28) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the public administrations and market operators reporting incidents. In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes.	(28) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors. ***Previously unknown vulnerabilities or incidents reported to competent authorities should be notified to the manufacturers and service providers of affected ICT products and services.*** Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the public administrations and market operators reporting incidents. In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes.

Or. en

Justification

In case authorities are aware of vulnerabilities of certain ICT products or services, they should notify the manufacturers and service providers in order to allow them to adapt their products and services in a timely manner.

Amendment 189
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 28

Text proposed by the Commission	*Amendment*
(28) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the public administrations and market operators reporting incidents. In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes.	(28) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the public administrations and market operators reporting incidents. In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes ***though not delay any notification more than compulsorily required***.

Or. en

Amendment 190
Ioannis A. Tsoukalas

Proposal for a directive
Recital 29

Text proposed by the Commission	*Amendment*
(29) Competent authorities should have the necessary means to perform their duties, including powers to obtain sufficient information from market operators and public administrations in order to assess the level of security of network and information systems as well as reliable and comprehensive data about actual incidents that have had an impact on the operation of network and information systems.	(29) Competent authorities should have the necessary means to perform their duties, including powers to obtain sufficient information from market operators and public administrations in order to assess the level of security of network and information systems***, measure the number, scale and scope of incidents,*** as well as reliable and comprehensive data about actual incidents that have had an impact on the operation of network and information systems.

Or. en

Amendment 191
Amelia Andersdotter

Proposal for a directive
Recital 30

Text proposed by the Commission	*Amendment*
(30) Criminal activities are in many cases underlying an incident. The criminal nature of incidents can be suspected even if the evidence to support it may not be sufficiently clear from the start. In this context, appropriate co-operation between competent authorities and law enforcement authorities should form part of an effective and comprehensive response to the threat of security incidents. In particular, promoting a safe, secure and more resilient environment requires a systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities. The serious criminal nature of incidents should be assessed in the light of EU laws on cybercrime.	***deleted***

Or. en

Amendment 192
Francisco Sosa Wagner
Proposal for a directive
Recital 30

Text proposed by the Commission	*Amendment*
(30) Criminal activities ***are*** in many cases ***underlying*** an incident. ***The criminal nature of incidents can be suspected even if the evidence to support it may not be sufficiently clear from the start.*** In this context, appropriate co-operation between competent authorities and law enforcement authorities should form part of an effective and comprehensive response to the threat of security incidents. In particular, promoting a safe, secure and more resilient environment requires a systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities. The serious criminal nature of incidents should be assessed in the light of EU laws on cybercrime.	(30) Criminal activities ***may*** in many cases ***underlie*** an incident. In this context, appropriate co-operation between competent authorities and law enforcement authorities should form part of an effective and comprehensive response to the threat of security incidents. In particular, promoting a safe, secure and more resilient environment requires a systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities. The serious criminal nature of incidents should be assessed in the light of EU laws on cybercrime.

Or. es

Justification

The default assumption that any incident affecting security on a section of the network is of a criminal nature is unjustified and is the upshot of an out-of-proportion approach which, in being overly focused on security, threatens to undermine civil rights.

Amendment 193
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 30

Text proposed by the Commission	*Amendment*
(30) Criminal activities are in many cases underlying an incident. The criminal nature of incidents can be suspected even if the	(30) Criminal activities are in many cases underlying an incident. The criminal nature of incidents can be suspected even if the

evidence to support it may not be sufficiently clear from the start. In this context, appropriate co-operation between competent authorities and law enforcement authorities should form part of an effective and comprehensive response to the threat of security incidents. In particular, promoting a safe, secure and more resilient environment requires a systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities. The serious criminal nature of incidents should be assessed in the light of EU laws on cybercrime.	evidence to support it may not be sufficiently clear from the start. In this context, appropriate co-operation between competent authorities and law enforcement authorities ***as well as cooperation with the EC3 (Europol Cybercrime Centre) and ENISA*** should form part of an effective and comprehensive response to the threat of security incidents. In particular, promoting a safe, secure and more resilient environment requires a systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities. The serious criminal nature of incidents should be assessed in the light of EU laws on cybercrime.

Or. en

Amendment 194
Ioannis A. Tsoukalas

Proposal for a directive
Recital 30

Text proposed by the Commission	*Amendment*
(30) Criminal activities are in many cases underlying an incident. The criminal nature of incidents can be suspected even if the evidence to support it may not be sufficiently clear from the start. In this context, appropriate co-operation between competent authorities ***and*** law enforcement authorities should form part of an effective and comprehensive response to the threat of security incidents. In particular, promoting a safe, secure and more resilient environment requires a systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities. The serious criminal nature of incidents should be assessed in the light of EU laws on cybercrime.	(30) Criminal ***or cyberwar*** activities are in many cases underlying an incident. The criminal nature of incidents can be suspected even if the evidence to support it may not be sufficiently clear from the start. In this context, appropriate co-operation between competent authorities***,*** law enforcement authorities ***and defence institutions*** should form part of an effective and comprehensive response to the threat of security incidents. In particular, promoting a safe, secure and more resilient environment requires a systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities ***and of possible cyberwar incidents to defence institutions***. The serious criminal nature of incidents should be assessed in the light of EU laws

on cybercrime.

Or. en

Amendment 195
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 31

Text proposed by the Commission	*Amendment*
(31) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle the personal data breaches resulting from incidents. Member states shall implement the obligation to notify security incidents in a way that minimises the administrative burden in case the security incident is also a personal data breach in line with the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data[28] . Liaising with the competent authorities and the data protection authorities, ENISA could assist by developing information exchange mechanisms and templates avoiding the need for two notification templates. This single notification template would facilitate the reporting of incidents compromising personal data thereby easing the administrative burden on businesses and public administrations.	(31) Personal data are in many cases compromised as a result of incidents. ***Member States and market operators should protect personal data stored, processed or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, access or disclosure, dissemination, or access; and ensure the implementation of a security policy with respect to the processing of personal data.*** In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle the personal data breaches resulting from incidents. Member states shall implement the obligation to notify security incidents in a way that minimises the administrative burden in case the security incident is also a personal data breach in line with the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data[28] . Liaising with the competent authorities and the data protection authorities, ENISA could assist by developing information exchange mechanisms and templates avoiding the need for two notification templates. This single notification template would facilitate the reporting of incidents compromising personal data thereby easing the

administrative burden on businesses and public administrations.

[28] SEC(2012) 72 final

[28] SEC(2012) 72 final

Or. en

Justification

Aligned to the draft Data Protection Directive.

Amendment 196
Ioannis A. Tsoukalas

Proposal for a directive
Recital 32

Text proposed by the Commission	*Amendment*
(32) Standardisation of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards to ensure a high level of security at Union level. To this end, it might be necessary to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council[29] .	(32) Standardisation of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards to ensure a high level of security at Union level. To this end, it might be necessary to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council[29] . ***International standards pertaining to cybersecurity should be carefully vetted in order to ensure that they have not been***

compromised and that they provide adequate levels of security, thus safeguarding that the mandated compliance with cybersecurity standards enhances the overall level of cybersecurity of the Union and not the contrary.

[29] OJ L 316, 14.11.2012, p. 12.

[29] OJ L 316, 14.11.2012, p. 12.

Or. en

Amendment 197
Ivailo Kalfin

Proposal for a directive
Recital 32

Text proposed by the Commission	*Amendment*
(32) Standardisation of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards to ensure a high level of security at Union level. To this end, ***it*** might be necessary to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the ***Council***[29] .	(32) Standardisation of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards to ensure a high level of security at Union level. To this end, ***the application of open international standards on network information security or the design of such tools need to be considered. Another step forward*** might be necessary to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the ***Council29. In particular, ETSI,***

	CEN and CENELEC should be mandated to suggest effective and efficient EU open security standards, where technological preferences are avoided as much as possible, and which should be made easily manageable by small and medium-size market operators and smaller public administrations.
[29] OJ L 316, 14.11.2012, p. 12.	[29] OJ L 316, 14.11.2012, p. 12.

Or. en

Amendment 198
Ivailo Kalfin

Proposal for a directive
Recital 33

Text proposed by the Commission	*Amendment*
(33) The Commission should periodically review this Directive, in particular with a view to determining the need for modification in the light of changing technological or market conditions**.**	(33) The Commission should periodically review this Directive, in ***consultation with all interested stakeholders, in*** particular with a view to determining the need for modification in the light of changing technological or market conditions

Or. en

Amendment 199
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Recital 33

Text proposed by the Commission	*Amendment*
(33) The Commission should periodically review this Directive, in particular with a view to determining the need for modification in the light of changing technological or market conditions.	(33) The Commission should periodically review this Directive, in particular with a view to determining the need for modification in the light of changing ***societal, political,*** technological or market

conditions.

Or. en

Amendment 200
Amelia Andersdotter

Proposal for a directive
Recital 36

Text proposed by the Commission	*Amendment*
(36) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission as regards the cooperation between competent authorities and the Commission within the cooperation network, the ***access to the secure information-sharing infrastructure, the*** Union NIS cooperation plan, the formats and procedures applicable to informing the public about incidents, and the standards and/or technical specifications relevant to NIS. Those powers should be exercised in accordance with 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 Member States of the Commission's exercise of implementing powers[30] .	(36) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission as regards the cooperation between competent authorities and the Commission within the cooperation network, the Union NIS cooperation plan, the formats and procedures applicable to informing the public about incidents, and the standards and/or technical specifications relevant to NIS. Those powers should be exercised in accordance with 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 Member States of the Commission's exercise of implementing powers[30].
[30] OJ L 55, 28.2.2011, p.13.	[30] OJ L 55, 28.2.2011, p.13.

Or. en

Amendment 201
Ioannis A. Tsoukalas

Proposal for a directive
Recital 37

Text proposed by the Commission	*Amendment*
(37) In the application of this Directive, the Commission should liaise as appropriate with relevant sectoral committees and relevant bodies set up at EU level in particular in the field of energy, transport and health.	(37) In the application of this Directive, the Commission should liaise as appropriate with relevant sectorial committees and relevant bodies set up at EU level in particular in the field of ***e-Government,*** energy, transport and health.

Or. en

Amendment 202
Ivailo Kalfin

Proposal for a directive
Recital 38

Text proposed by the Commission	*Amendment*
(38) Information that is considered confidential by a competent authority**,** in accordance with Union and national rules on business confidentiality, should be exchanged with the Commission ***and*** other competent authorities only where such exchange is strictly necessary for the application of this Directive. The information exchanged should be limited to that which is relevant and proportionate to the purpose of such exchange.	(38) Information that is considered confidential by a competent authority in accordance with Union and national rules on business confidentiality, should be exchanged with the Commission***, its relevant agencies and/ or*** other ***national*** competent authorities only where such exchange is strictly necessary for the application of this Directive. The information exchanged should be limited to that which is relevant and proportionate to the purpose of such exchange***, while respecting pre-defined criteria for confidentiality and security and classification protocols, governing the information sharing procedure***.

Or. en

Amendment 203
Amelia Andersdotter

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

Text proposed by the Commission	*Amendment*
(b) creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems;	(b) creates an ***institutional*** cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems;

Or. en

Amendment 204
Amelia Andersdotter

Proposal for a directive
Article 1 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The security requirements provided for in Article 14 shall apply neither to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC, which shall comply with the specific security and integrity requirements laid down in Articles 13a and 13b of that Directive, nor to trust service providers.	***deleted***

Or. en

Amendment 205
Ivailo Kalfin

Proposal for a directive
Article 1 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The security requirements provided for in Article 14 shall apply neither to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC, which shall comply with the specific security and integrity requirements laid down in Articles 13a and 13b of that Directive, ***nor to*** trust service providers.	3. The security requirements provided for in Article 14 shall apply neither to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC, which shall comply with the specific security and integrity requirements laid down in Articles 13a and 13b of that Directive, ***neither to*** trust service providers ***nor to information society services whose confidentiality, integrity, availability and authenticity are not essential to the maintenance of vital economical or societal functions***.

Or. en

Amendment 206
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 1 – paragraph 4

Text proposed by the Commission	*Amendment*
4. This Directive shall be without prejudice to EU laws on cybercrime and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[32]	4. This Directive shall be without prejudice to EU laws on cybercrime and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[32]***. However, that Directive shall be reviewed without further delay in particular regarding the inclusion of ICT as a European Infrastructure.***
[32] OJ L 345, 23.12.2008, p. 75.	[32] OJ L 345, 23.12.2008, p. 75.

Or. en

Justification

Initially ICT has not been listed as a European Critical Infrastructure. The Member States agreed to reflect on this issue and review the Directive in due time. As this has not been done so far and regarding the relevance of ICT for critical infrastructures we call on the Member States to resume this discussion as soon as possible.

Amendment 207
Amelia Andersdotter

Proposal for a directive
Article 1 – paragraph 4

Text proposed by the Commission	*Amendment*
4. This Directive shall be without prejudice to ***EU laws on cybercrime*** and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[32]	4. This Directive shall be without prejudice to ***Directive 2013/40/EU on unauthorised access to computer systems*** and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[32]
[32] OJ L 345, 23.12.2008, p. 75.	[32] OJ L 345, 23.12.2008, p. 75.

Or. en

Amendment 208
Ivailo Kalfin

Proposal for a directive
Article 1 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require the processing of personal data. Such processing, which is necessary to meet the objectives of public interest pursued by this Directive, shall be authorised by the Member State pursuant	6. The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require the ***communication to trusted third parties and the*** processing of personal data. Such processing, which is necessary to meet the objectives of public interest pursued by this Directive, shall be

to Article 7 of Directive 95/46/EC and Directive 2002/58/EC, as implemented in national law.	authorised by the Member State pursuant to Article 7 of Directive 95/46/EC and Directive 2002/58/EC, as implemented in national law. ***Member States shall adopt legislative measures in accordance with Article 13 of Directive 95/46/EC to ensure that public administrations, market operators and competent authorities are not held liable for processing personal data, necessary for the sharing of information within the cooperation network and incident notification.***

Or. en

Amendment 209
Amelia Andersdotter

Proposal for a directive
Article 1 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require the processing of personal data. Such processing, which is necessary to meet the objectives of public interest pursued by this Directive, shall be authorised by the Member State pursuant to Article 7 of Directive 95/46/EC and Directive 2002/58/EC, as implemented in national law.	6. The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require the processing of personal data. Such processing, which is necessary to meet the objectives of public interest pursued by this Directive, shall be authorised by the Member State pursuant to Article 7 of Directive 95/46/EC and Directive 2002/58/EC, as implemented in national law***, after taking all measures to ensure that the data is anonymised***.

Or. en

Amendment 210
Francisco Sosa Wagner
Proposal for a directive
Article 2 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall not be prevented from adopting or maintaining provisions ensuring a higher level of security, without prejudice to their obligations under Union law.	Member States shall not be prevented from adopting or maintaining provisions ensuring a higher level of security ***that conform to the Charter of Fundamental Rights of the European Union***, without prejudice to their obligations under Union law.

Or. es

Justification

The leeway that Member States enjoy on matters of security must be conditional on respect for the principles set out in the Charter of Fundamental Rights of the European Union, including for example the right to respect for private life and communications, to protection of personal data, to freedom to conduct a business and to effective remedy before a court.

Amendment 211
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 3 – paragraph 1 – point 1 – point b

Text proposed by the Commission	*Amendment*
(b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of ***computer*** data, as well as	(b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of ***digital*** data, as well as

Or. en

Amendment 212
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 3 – paragraph 1 – point 1 – point c

Text proposed by the Commission	*Amendment*
(c) ***computer*** data stored, processed,	(c) ***digital*** data stored, processed, retrieved

retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.	or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.

Or. en

Amendment 213
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 3 – paragraph 1 – point 2

Text proposed by the Commission	*Amendment*
(2) 'security' means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system;	(2) 'security' means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system; ***"security" as defined here includes appropriate technical devices, solutions and operating procedures ensuring the security requirements set forth in this Directive.***

Or. en

Amendment 214
Amelia Andersdotter

Proposal for a directive
Article 3 – paragraph 1 – point 2 a (new)

Text proposed by the Commission	*Amendment*
	(2a) "high common level of network information security" means a network and information system across the Union where incidents are corrected and unrepeated.

Or. en

Amendment 215
Jürgen Creutzmann

Proposal for a directive
Article 3 – paragraph 1 – point 4

Text proposed by the Commission	*Amendment*
(4) 'incident' means any circumstance or event having an actual adverse effect on security;	(4) 'incident' means any ***reasonably identifiable*** circumstance or event having an actual adverse effect on security;

Or. en

Justification

The original wording was too broad and would have complicated application of the definition.

Amendment 216
Jürgen Creutzmann

Proposal for a directive
Article 3 – paragraph 1 – point 5

Text proposed by the Commission	*Amendment*
(5) 'information society service' mean service within the meaning of point (2) of Article 1 of Directive 98/34/EC;	***deleted***

Or. en

Amendment 217
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 3 – paragraph 1 – point 7

Text proposed by the Commission	*Amendment*
(7) 'incident handling' means all procedures supporting the analysis, containment and response to an incident;	(7) 'incident handling' means all procedures supporting the ***detection, prevention,*** analysis, containment and response to an incident;

Or. en

Amendment 218
Ivailo Kalfin

Proposal for a directive
Article 3 – paragraph 1 – point 8 – introductory part

Text proposed by the Commission	*Amendment*
(8) '***market*** operator' means:	(8) 'operator' means:

Or. en

Amendment 219
Jürgen Creutzmann

Proposal for a directive
Article 3 – paragraph 1 – point 8 – point a

Text proposed by the Commission	*Amendment*
(a) provider of information society services which enable the provision of other information society services, a non-exhaustive list of which is set out in Annex II;	***deleted***

Or. en

Amendment 220
Francisco Sosa Wagner
Proposal for a directive
Article 3 – paragraph 1 – point 8 – point a

Text proposed by the Commission	*Amendment*
a) provider of information society services which enable the provision of other information society services, a ***non exhaustive*** list of which is set out in Annex II;	a) provider of information society services which enable the provision of other information society services, a list of which is set out in Annex II;

Or. es

Justification

The list should be exhaustive so as to guarantee transparency.

Amendment 221
Ivailo Kalfin

Proposal for a directive
Article 3 – paragraph 1 – point 8 – point b

Text proposed by the Commission	*Amendment*
(b) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a non-exhaustive list of which is set out in Annex II.	(b) ***public or private*** operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking ***and financial services***, stock exchanges***, information and communication technologies*** and health, a non-exhaustive list of which is set out in Annex II.

Or. en

Amendment 222
Jürgen Creutzmann

Proposal for a directive
Article 3 – paragraph 1 – point 8 – point b

Text proposed by the Commission	*Amendment*
(b) operator of ***critical*** infrastructure that	(b) operator of infrastructure that are

are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a ***non-exhaustive*** list of which is set out in Annex II.	essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a list of which is set out in Annex II.

Or. en

Amendment 223
Amelia Andersdotter

Proposal for a directive
Article 3 – paragraph 1 – point 8 – point b

Text proposed by the Commission	*Amendment*
(b) operator of ***critical*** infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a non-exhaustive list of which is set out in Annex II.	(b) operator of infrastructure that are essential for the maintenance of vital economic and societal activities ***such as*** in the fields of energy, transport, banking, stock exchanges and health, a non-exhaustive list of which is set out in Annex II.

Or. en

Amendment 224
Ivailo Kalfin

Proposal for a directive
Article 3 – paragraph 1 – point 8 a (new)

Text proposed by the Commission	*Amendment*
	(8a) "incident having a significant impact" means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions;

Or. en

Amendment 225
Ivailo Kalfin

Proposal for a directive
Article 3 – paragraph 1 – point 8 b (new)

Text proposed by the Commission	*Amendment*
	(8b) "service" means the service provided by a public administration or market operator, to the exclusion of any other services of the same entity.

Or. en

Amendment 226
Jürgen Creutzmann

Proposal for a directive
Article 4

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

Or. en

Justification

The added value and the legal effect of this provision are unclear.

Amendment 227
Amelia Andersdotter

Proposal for a directive
Article 4 – title

Text proposed by the Commission	*Amendment*
Principle	***General obligation***

Or. en

Amendment 228
Vicky Ford

Proposal for a directive
Article 4 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive.	***deleted***

Or. en

Amendment 229
Amelia Andersdotter

Proposal for a directive
Article 4 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall ensure a high level of security of the network and information systems ***in their territories in accordance with this Directive***.	***The European Union and its*** Member States***, public administrations and market operators*** shall ensure a high level of security of the network and information systems ***they either develop, operate or have under their control***.

Or. en

Amendment 230
Francisco Sosa Wagner
Proposal for a directive
Article 4 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall ensure a high level of security of the network and information systems in their territories in accordance	Member States shall ensure a high level of security of the network and information systems in their territories in accordance

with this Directive.	with ***the Charter of Fundamental Rights of the European Union and*** this Directive.

Or. es

Justification

The leeway that Member States enjoy on matters of security must be conditional on respect for the principles set out in the Charter of Fundamental Rights of the European Union, including for example the right to respect for private life and communications, to protection of personal data, to freedom to conduct a business and to effective remedy before a court.

Amendment 231
Christian Ehler, Manfred Weber

Proposal for a directive
Article 4 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall ensure a ***high*** level of security of the network and information systems in their territories in accordance with this Directive.	Member States shall ensure a ***sustained continuous high*** level of security of the network and information systems in their territories in accordance with this Directive.

Or. en

Amendment 232
Amelia Andersdotter

Proposal for a directive
Article 4 a (new)

Text proposed by the Commission	*Amendment*
	Article 4 a
	Liability of market operators
	A market operator under Article 3 shall be liable for any direct damage caused to any natural or legal person due to failure to comply with the obligations of this Directive if that damage is due to fault or

neglect on its part.

Or. en

Amendment 233
Ioannis A. Tsoukalas

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

Text proposed by the Commission	*Amendment*
	(ea) Member States may ask for the assistance of the European Network and Information Security Agency ('ENISA') in developing their national NIS strategies and national NIS cooperation plans, based on a common minimum NIS strategy and cooperation blueprint.

Or. en

Amendment 234
Hans-Peter Martin

Proposal for a directive
Article 6 – paragraph 1

Text proposed by the Commission	*Amendment*
1) Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority").	1) Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority")***, which is not part of a secret service and not fully or partially identical with a secret service in terms of staffing or infrastructure.***

Or. de

Amendment 235
Amelia Andersdotter

Proposal for a directive
Article 6 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Each Member State shall designate a national competent authority on the security of network and information ***systems*** (the 'competent authority').	1. Each Member State shall designate a national competent authority on the security of network and information ***systems used on the internal market*** (the 'competent authority').

Or. en

Amendment 236
Francisco Sosa Wagner
Proposal for a directive
Article 6 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The competent authorities shall consult and cooperate, whenever appropriate, with the relevant law enforcement ***national authorities and data protection*** authorities.	5. The competent authorities shall consult ***with the data protection authorities as a matter of course*** and cooperate, whenever appropriate, with the relevant ***national*** law enforcement authorities.

Or. es

Justification

The balance between ensuring security and safeguarding freedoms would be upset were just a single authority to exercise monitoring power at national level without the cooperation of another, compensating body.

Amendment 237
Ivailo Kalfin

Proposal for a directive
Article 7 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Each Member State shall set up a Computer Emergency Response Team (hereinafter: 'CERT') responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within ***the*** competent authority.	1. Each Member State shall set up a Computer Emergency Response Team (hereinafter: 'CERT') responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within ***a*** competent authority ***on network information security or could be designated as the national single point of contact***.

Or. en

Amendment 238
Vicky Ford

Proposal for a directive
Article 7 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Each Member State shall set up ***a*** Computer Emergency Response Team (hereinafter: 'CERT') responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority.	1. Each Member State shall set up ***at least one*** Computer Emergency Response Team (hereinafter: 'CERT') ***or system of multiple CERTs, covering the sectors in Annex II,*** responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority.

Or. en

Amendment 239
Jürgen Creutzmann

Proposal for a directive
Article 7 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Each Member State shall set up ***a*** Computer Emergency Response ***Team*** (hereinafter: 'CERT') responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority.	1. Each Member State shall set up ***one or more*** Computer Emergency Response ***Teams*** (hereinafter: 'CERT') responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority.

Or. en

Justification

Member States should be free to set up more than one CERT, e.g. on a per sector basis.

Amendment 240
Amelia Andersdotter

Proposal for a directive
Article 7 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Each Member State shall set up a Computer Emergency Response Team (hereinafter: 'CERT') responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority.	1. Each Member State shall set up an ***Industrial Control System*** Computer Emergency Response Team (hereinafter: 'CERT') responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority.

Or. en

Amendment 241
Vicky Ford

Proposal for a directive
Article 7 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The CERT shall act under the supervision of the competent authority, which shall regularly review the adequacy of ***its*** resources, ***its mandate*** and the effectiveness of ***its*** incident-handling process.	5. The CERT ***or CERTs*** shall act under the supervision of the competent authority, which shall regularly review the adequacy of ***their*** resources, ***mandates*** and the effectiveness of ***their*** incident-handling process.

Or. en

Amendment 242
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 7 – paragraph 5 – point 1 (new)

Text proposed by the Commission	*Amendment*
	(1) The CERT shall be enabled and encouraged to initiate and to participate in joint exercises with certain CERT, with all Member States-CERT, and with appropriate institutions of non-Member States as well as with CERT of multi- and international institutions such as NATO and the UN.

Or. en

Amendment 243
Ioannis A. Tsoukalas

Proposal for a directive
Article 7 – paragraph 5 a (new)

Text proposed by the Commission	*Amendment*
	5 a. Member States may ask for the assistance of the European Network and Information Security Agency ('ENISA') or of other Member States in developing their national CERT.

Or. en

Amendment 244
Silvia-Adriana Ţicău
Proposal for a directive
Article 8 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The competent authorities and the Commission shall form a network ("cooperation network") to cooperate against risks and incidents affecting network and information systems.	1The competent authorities ***, the European Network and Information Security Agency (ENISA)*** and the Commission shall form a network ("cooperation network") to cooperate against risks and incidents affecting network and information systems.

Or. ro

Amendment 245
Ioannis A. Tsoukalas

Proposal for a directive
Article 8 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The competent authorities and the Commission shall form a network ('cooperation network') to cooperate against risks and incidents affecting network and information systems.	1. The competent authorities and the Commission shall form a network ('cooperation network')***, under the coordination of ENISA,*** to cooperate against risks and incidents affecting network and information systems.

Or. en

Amendment 246
Amelia Andersdotter

Proposal for a directive
Article 8 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The competent authorities and the Commission shall form a network (‘cooperation network’) to cooperate against risks and incidents affecting network and information systems.	1. The competent authorities and the Commission shall form an ***institutional*** network (‘cooperation network’) to cooperate against risks and incidents affecting network and information systems.

Or. en

Amendment 247
Silvia-Adriana Ţicău
Proposal for a directive
Article 8 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The cooperation network shall bring into permanent communication the Commission and the competent authorities. ***When requested, the European Network and Information Security Agency ("ENISA") shall assist the cooperation network by providing its expertise and advice.***	2. The cooperation network shall bring into permanent communication the Commission, ***ENISA*** and the competent authorities.

Or. ro

Amendment 248
Ivailo Kalfin

Proposal for a directive
Article 8 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The cooperation network shall bring into permanent communication the Commission and the competent authorities. When requested, the European Network and Information Security Agency (**‘**ENISA**’**) shall assist the cooperation network by providing its expertise and advice.	2. The cooperation network shall bring into permanent communication the Commission and the competent authorities ***and, as appropriate, relevant public administrations and market operators***. When requested, the European Network and Information Security Agency (**‘**ENISA**’**) shall assist the cooperation network by providing its expertise and

advice.

Or. en

Amendment 249
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 8 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The cooperation network shall bring into permanent communication the Commission and the competent authorities. ***When requested,*** the European Network and Information Security Agency ('ENISA') shall assist the cooperation network by providing its expertise and advice.	2. The cooperation network shall bring into permanent communication the Commission and the competent authorities. The European Network and Information Security Agency ('ENISA') shall assist the cooperation network by providing its expertise and advice.

Or. en

Amendment 250
Ioannis A. Tsoukalas

Proposal for a directive
Article 8 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The cooperation network shall bring into permanent communication the Commission and the competent authorities. ***When requested,*** the European Network and Information Security Agency ('ENISA') shall assist the cooperation network by providing its expertise and advice.	2. The cooperation network shall bring into permanent communication the Commission and the competent authorities. The European Network and Information Security Agency ('ENISA') shall assist the cooperation network by providing its expertise and advice.

Or. en

Amendment 251
Ivailo Kalfin

Proposal for a directive
Article 8 – paragraph 3 – point a a (new)

Text proposed by the Commission	*Amendment*
	(aa) Where information, early warnings or best practices originating from market operators or public administrations are shared within, or disclosed by the cooperation network, such sharing or disclosure shall be in accordance with the information classification as determined by the original source in accordance with Article 9(1). It shall be ensured that the original source is informed of the sharing or disclosure, including which relevant authorities or operators are to be informed of the incident, and that and that such sharing or disclosure does not harm the legitimate interests of the source.

Or. en

Amendment 252
Hans-Peter Martin

Proposal for a directive
Article 8 – paragraph 3 – point c

Text proposed by the Commission	*Amendment*
c) publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website;	c) publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website***, in machine-readable form also;***

Or. de

Amendment 253
Silvia-Adriana Ţicău

Proposal for a directive
Article 8 – paragraph 3 – point c

Text proposed by the Commission	*Amendment*
(c) publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website;	(c) publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website ***and on the ENISA website***;

Or. ro

Amendment 254
Jürgen Creutzmann

Proposal for a directive
Article 8 – paragraph 3 – point c a (new)

Text proposed by the Commission	*Amendment*
	(c a) jointly discuss and coordinate their measures regarding security requirements and incident notification referred to in article 14 and regarding implementation and enforcement referred to in article 15;

Or. en

Justification

Diverging practices of competent authorities as to the notification and disclosure provisions and in general as to the implementation and enforcement of this Directive could render compliance more difficult for market operators active in more than one Member State. In the extreme, operators could receive diverging instructions from several competent authorities. It should therefore be ensured that competent authorities coordinate these activities to the degree possible.

Amendment 255
Christian Ehler, Manfred Weber

Proposal for a directive
Article 8 – paragraph 3 – point e

Text proposed by the Commission	*Amendment*
(e) jointly discuss and assess, at the request of a Member State or the Commission, the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level;	(e) jointly discuss and assess, at the request of a Member State or the Commission, the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level ***and implement measures to resolve identified weaknesses without measurable delay***;

Or. en

Amendment 256
Vicky Ford

Proposal for a directive
Article 8 – paragraph 3 – point f

Text proposed by the Commission	*Amendment*
(f) cooperate and exchange information on all relevant matters with ***the European Cybercrime Centre within Europol, and with other*** relevant European bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health;	(f) cooperate and exchange information on all relevant matters with relevant European bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health;

Or. en

Justification

Covered by Article 10.4.

Amendment 257
Amelia Andersdotter

Proposal for a directive
Article 8 – paragraph 3 – point f

Text proposed by the Commission	*Amendment*
(f) cooperate and exchange information on	(f) cooperate and exchange information on

all relevant matters with ***the European Cybercrime Centre within Europol, and with*** other relevant European bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health;	all relevant matters with other relevant European bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health;

Or. en

Amendment 258
Christian Ehler, Manfred Weber

Proposal for a directive
Article 8 – paragraph 3 – point f

Text proposed by the Commission	*Amendment*
(f) cooperate and exchange information on all relevant matters with the European Cybercrime Centre within Europol, and with other relevant European bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health;	(f) cooperate and exchange information on all relevant matters with the European Cybercrime Centre within Europol, and with other relevant European bodies in particular in the fields of ***criminal investigation,*** data protection, energy, transport, banking, stock exchanges and health;

Or. en

Amendment 259
Francisco Sosa Wagner
Proposal for a directive
Article 8 – paragraph 3 – point f

Text proposed by the Commission	*Amendment*
f) cooperate and exchange information on all relevant matters with the EuropeanCybercrime Center within Europol, and with other relevant European bodies in particular in the fields of ***data protection,*** energy, transport, banking, stock exchanges and health;	f) cooperate and exchange information on all relevant matters with the European Cybercrime Center within Europol, and with other relevant European bodies in particular in the fields of energy, transport, banking, stock exchanges and health;

Or. es

Justification

The creation of a security cooperation network must be balanced by the compulsory involvement of data protection bodies. A specific point should be included on developing that cooperation.

Amendment 260
Ivailo Kalfin

Proposal for a directive
Article 8 – paragraph 3 – point f a (new)

Text proposed by the Commission	*Amendment*
	(fa) jointly discuss and agree on the common interpretation, consistent application and harmonious implementation within the Union of the provisions of Chapter IV;

Or. en

Amendment 261
Francisco Sosa Wagner
Proposal for a directive
Article 8 – paragraph 3 – point f a (new)

Text proposed by the Commission	*Amendment*
	fa) cooperate as a matter of course with the national data protection authorities and the European Data Protection Supervisor;

Or. es

Justification

The creation of a security cooperation network must be balanced by the compulsory involvement of data protection bodies.

Amendment 262
Christian Ehler, Manfred Weber

Proposal for a directive
Article 8 – paragraph 3 – point i – point 1 (new)

Text proposed by the Commission	*Amendment*
	1) NIS-authorities shall be encouraged to engage in security research and other appropriate programmes of Horizon2020.

Or. en

Amendment 263
Jürgen Creutzmann

Proposal for a directive
Article 8 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. Where appropriate market operators may be invited to participate in the activities of the cooperation network referred to in points (a), (g), (h) and (i) of paragraph 3.

Or. en

Amendment 264
Silvia-Adriana Ţicău
Proposal for a directive
Article 8 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between competent authorities and the Commission referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the	4. The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between competent authorities***, ENISA*** and the Commission referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the

consultation procedure referred to in Article 19(2).	consultation procedure referred to in Article 19(2).

Or. ro

Amendment 265
Amelia Andersdotter

Proposal for a directive
Article 9

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

Or. en

Amendment 266
Hans-Peter Martin

Proposal for a directive
Article 9 – paragraph 1

Text proposed by the Commission	*Amendment*
1) The exchange of sensitive and confidential information within the cooperation network shall take place through a secure infrastructure.	1) The exchange of sensitive and confidential information within the cooperation network shall take place through a secure infrastructure. ***Member States shall ensure that shared sensitive or secret information from other States or the Commission will not be shared with third States or improper purposes, for example covert operations or financial decision making.***

Or. de

Amendment 267
Ioannis A. Tsoukalas

Proposal for a directive
Article 9 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The exchange of sensitive and confidential information within the cooperation network shall take place through a secure infrastructure.	1. The exchange of sensitive and confidential information within the cooperation network shall take place through a secure infrastructure ***operated under the supervision of ENISA***.

Or. en

Amendment 268
Silvia-Adriana Ţicău
Proposal for a directive
Article 9 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. Within five years from the entry into force of this directive, Member States shall ensure that the criteria referred to in of paragraph 2 are fulfilled.

Or. ro

Amendment 269
Ioannis A. Tsoukalas

Proposal for a directive
Article 10 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. The competent authorities or the Commission shall provide early warnings within the cooperation network on those risks and incidents that fulfil at least one of the following conditions:	1. The competent authorities or the Commission***, under the coordination of ENISA,*** shall provide early warnings within the cooperation network on those risks and incidents that fulfil at least one of the following conditions:

Or. en

Amendment 270
Amelia Andersdotter

Proposal for a directive
Article 10 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. The competent authorities or the Commission shall provide early warnings within the cooperation network on those risks and incidents that fulfil at least one of the following conditions:	1. The competent authorities or the Commission shall provide early warnings within the ***institutional*** cooperation network on those risks and incidents that fulfil at least one of the following conditions:

Or. en

Amendment 271
Jürgen Creutzmann

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

Text proposed by the Commission	*Amendment*
(a) they grow rapidly or may grow rapidly in scale;	(a) they grow rapidly or may grow rapidly in scale ***and affect or may affect more than one Member State***;

Or. en

Justification

The very fact of a rapidly growing scale itself is not yet an indication of whether the issue is relevant to the cooperation network. If the issue can be handled by authorities in one Member State and if effects on other Member States are not likely, then an early warning to the whole network does not appear appropriate.

Amendment 272
Jürgen Creutzmann

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

Text proposed by the Commission	*Amendment*
(c) they affect or may affect more than one Member State.	***deleted***

Or. en

Justification

Merged with point (a).

Amendment 273
Jean-Pierre Audy

Proposal for a directive
Article 10 – paragraph 2

Text proposed by the Commission	*Amendment*
2. In the early warnings, the competent authorities and the Commission shall communicate any relevant information in their possession that may be useful for assessing the risk or incident.	2. In the early warnings, the competent authorities and the Commission shall communicate any relevant information in their possession that may be useful for assessing the risk or incident ***where required by the gravity of the situation. The Commission shall be responsible for assessing the gravity of the situation for the purposes of implementing this provision.***

Or. fr

Justification

Systematic notification is not called for and it is important to stipulate the need for a Commission assessment of the gravity of a situation.

Amendment 274
Jürgen Creutzmann

Proposal for a directive
Article 10 – paragraph 2

Text proposed by the Commission	*Amendment*
2. In the early warnings, the competent authorities and the Commission shall communicate any relevant information in their possession that may be useful for assessing the risk or incident.	2. In the early warnings, the competent authorities and the Commission shall communicate any relevant information in their possession that may be useful for assessing the risk or incident. ***Information deemed classified or confidential by the concerned public administration or market operator respectively and the identity of the latter shall only be provided to the degree necessary to assess the risk or incident.***

Or. en

Justification

Measures need to be taken to encourage incident reporting and cooperation with authorities. This requires trust on the market operators' side which will be strengthened if anonymity and confidentiality is ensured. E.g. in case of a hacker abusing a vulnerability of software systems widely used, the identity of the first entity concerned may not be relevant and could thus be treated confidential, which in turn decreases negative impacts on the concerned entity.

Amendment 275
Amelia Andersdotter

Proposal for a directive
Article 10 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Where the risk or incident subject to an early warning is of a suspected criminal nature, the competent authorities or the Commission shall inform the European Cybercrime Centre within Europol.	***deleted***

Or. en

Amendment 276
Vicky Ford

Proposal for a directive
Article 10 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Where the risk or incident subject to an early warning is of a suspected criminal nature, the competent authorities ***or the Commission shall inform*** the European Cybercrime Centre within Europol.	4. Where the risk or incident subject to an early warning is of a suspected criminal nature, the ***national*** competent authorities ***will liaise with national cybercrime authorities who will cooperate and exchange information with*** the European Cyber Crime Centre within Europol.

Or. en

Justification

Competent Authorities should liaise first with their national cybercrime authorities who will inform EC3. This should avoid unnecessary duplication of reporting and ensure that the national point of contact remains the key interlocutor for EC3.

Amendment 277
Jürgen Creutzmann

Proposal for a directive
Article 10 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Where the risk or incident subject to an early warning is of a suspected criminal nature, the competent authorities or the Commission shall inform the European Cybercrime Centre within Europol.	4. Where the risk or incident subject to an early warning is of a suspected ***serious*** criminal nature, the competent authorities or the Commission shall inform the European Cybercrime Centre within Europol ***where appropriate***.

Or. en

Justification

An automatic obligation to inform Europol would be too far reaching. A more targeted approach focusing on serious criminal matters appears more appropriate. Furthermore, the competent authorities and the Commission should have some discretion in the decision on whether to inform Europol.

Amendment 278
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 10 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Where the risk or incident subject to an early warning is of a suspected criminal nature, the competent authorities or the Commission shall inform the European Cybercrime Centre within Europol.	4. Where the risk or incident subject to an early warning is of a suspected criminal nature, the competent authorities or the Commission shall inform the European Cybercrime Centre within Europol ***without measurable delay***.

Or. en

Amendment 279
Ivailo Kalfin

Proposal for a directive
Article 10 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. Where the risk or incident subject to an early warning is of a suspected severe cross-border technical nature, the competent authorities or the Commission shall inform the European Network Information Security Agency;

Or. en

Amendment 280
Jürgen Creutzmann

Proposal for a directive
Article 10 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 18, concerning the further specification of the risks and incidents triggering early warning referred to in paragraph 1.	***deleted***

Or. en

Justification

The criteria appear to be sufficiently clear in the Directive.

Amendment 281
Francisco Sosa Wagner
Proposal for a directive
Article 10 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 18, concerning the further specification of the risks and incidents triggering early warning referred to in paragraph 1.	***deleted***

Or. es

Amendment 282
Vicky Ford

Proposal for a directive
Article 12 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Commission shall be empowered to adopt, by means of implementing acts, a ***Union*** NIS cooperation ***plan***. Those implementing acts shall be adopted in accordance with the examination procedure	1. The Commission shall be empowered to adopt, by means of implementing acts, a ***framework to ensure*** NIS cooperation ***across Member States***. Those implementing acts shall be adopted in

referred to in Article 19(3).	accordance with the examination procedure referred to in Article 19(3).

Or. en

Justification

It will be difficult to come to agreement over operational rules which respect Member States existing processes. Not all tools and techniques are relevant to all Member States as they have different threats and different industries. A framework (such as that already produced through collaboration between several MS) would therefore be preferable as it would additional flexibility for MS to maintain their existing structures while meeting the requirements of the Directive.

Amendment 283
Amelia Andersdotter

Proposal for a directive
Article 12 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Commission shall be empowered to adopt, by means of ***implementing*** acts, a Union NIS cooperation plan. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).	1. The Commission shall be empowered to adopt, by means of ***delegated*** acts, a Union NIS cooperation plan. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).

Or. en

Amendment 284
Vicky Ford

Proposal for a directive
Article 12 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. The Union NIS cooperation ***plan*** shall provide for:	2. The Union NIS cooperation ***framework*** shall provide for:

Or. en

Amendment 285
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 12 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Union NIS cooperation plan shall be adopted no later than one year following the entry into force of this Directive and shall be revised regularly.	3. The Union NIS cooperation plan shall be adopted no later than one year following the entry into force of this Directive and shall be revised regularly. ***Results of each revision shall be reported to the European Parliament.***

Or. en

Amendment 286
Francisco Sosa Wagner
Proposal for a directive
Article 13 – paragraph 1

Text proposed by the Commission	*Amendment*
Without prejudice to the possibility for the cooperation network to have informal international cooperation, the Union may conclude international agreements with third countries or international organisations allowing and organizing their participation in some activities of the cooperation network. ***Such agreement shall take into account the need to ensure adequate protection of the*** personal data circulating on the cooperation network.	Without prejudice to the possibility for the cooperation network to have informal international cooperation, the Union may conclude international agreements with third countries or international organisations allowing and organizing their participation in some activities of the cooperation network. ***These agreements shall set out the monitoring procedure that must be followed to guarantee the protection of*** personal data circulating on the cooperation network. ***The European Parliament shall be informed on the negotiation of the agreements, the transparency of which shall be guaranteed.***

Or. es

Justification

International agreements concluded with other countries or security bodies must contain a monitoring method that guarantees respect for civil rights. Effective democratic oversight of the agreements must also be exercised by the European Parliament, which must be duly informed of the content of the negotiations on the agreements.

Amendment 287
Amelia Andersdotter
on behalf of the Greens/EFA Group

Proposal for a directive
Article 13 – paragraph 1

Text proposed by the Commission	*Amendment*
Without prejudice to the possibility for the cooperation network to have informal international cooperation, the Union may conclude international agreements with third countries or international organisations allowing and organizing their participation in some activities of the cooperation network. Such agreement shall take into account the need to ensure adequate protection of the personal data circulating on the cooperation network.	Without prejudice to the possibility for the cooperation network to have informal international cooperation, the Union may conclude international agreements with third countries or international organisations allowing and organizing their participation in some activities of the cooperation network. Such agreement shall take into account the need to ensure adequate protection of the personal data circulating on the cooperation network***, without disclosing EU citizens' personal data to third parties***.

Or. en

Amendment 288
Silvia-Adriana Ţicău
Proposal for a directive
Article 13 – paragraph 1

Text proposed by the Commission	*Amendment*
Without prejudice to the possibility for the cooperation network to have informal international cooperation, the Union may conclude international agreements with third countries or international organisations allowing and organizing their	Without prejudice to the possibility for the cooperation network to have informal international cooperation, the Union may conclude international agreements with third countries or international organisations allowing and organizing their

participation in some activities of the cooperation network. Such agreement shall take into account the need to ensure adequate protection of the personal data circulating on the cooperation network.	participation in some activities of the cooperation network Such agreement shall take into account the need to ensure adequate protection of the personal data circulating on the cooperation network, ***in accordance with European Union legislation currently in force.***

Or. ro

Amendment 289
Jean-Pierre Audy

Proposal for a directive
Article 13 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	When the Union has concluded international agreements with third countries or international organizations, it shall provide for their participation in certain cooperation network activities, including cybersecurity, without prejudice to informal international cooperation network activities. Such agreement shall take into account the need to ensure adequate protection of the personal data circulating on the cooperation network.

Or. fr

Justification

It is proposed that the mechanism be embodied in international agreements to which the Union is a signatory.

Amendment 290
Ivailo Kalfin

Proposal for a directive
Article 14 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems**.**	1. Member States shall ensure that public administrations and market operators***, providing or operating services, referred to in Article (3)(8)(b) of this Directive,*** take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems

Or. en

Amendment 291
Amelia Andersdotter

Proposal for a directive
Article 14 – paragraph 1

Text proposed by the Commission	*Amendment*
1. ***Member States shall ensure that*** public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems ***which*** they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services	1. ***The European Union and its Member States,*** public administrations and market operators ***shall*** take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems they ***develop, and/or operate, and/or*** control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and

they provide and thus ensure the continuity of the services underpinned by those networks and information systems.	information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.

Or. en

Amendment 292
Vicky Ford

Proposal for a directive
Article 14 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that ***public administrations and*** market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.	1. Member States shall ensure that market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.

Or. en

Justification

Publicly-owned organisations are already included in the definition of market operator.

Amendment 293
Jürgen Creutzmann

Proposal for a directive
Article 14 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the ***state of the art***, these measures shall ***guarantee*** a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.	1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the ***technological development***, these measures shall ***ensure*** a level of security appropriate to the risk presented. In particular, ***appropriate*** measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.

Or. en

Amendment 294
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 14 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those	1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to ***detect and effectively*** manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity

networks and information systems.

of the services underpinned by those networks and information systems.

Or. en

Amendment 295
Ivailo Kalfin

Proposal for a directive
Article 14 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the security of the core services they provide.	2. Member States shall ensure that public administrations and market operators***, providing or operating services, referred to in Article (3)(8)(b) of this Directive,*** notify to the competent authority incidents having a significant impact on the security ***and continuity*** of the core services they provide. ***Member States shall ensure that compliance with this requirement does not alter the provisions of Article 9(1) of this Directive, nor that it exposes the notifying party to increased liability or unnecessary operational or security risk.***

Or. en

Amendment 296
Vicky Ford

Proposal for a directive
Article 14 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure ***that public administrations and*** market operators ***notify*** to the competent authority incidents ***having a*** significant impact on the security of the core services they provide.	2. Member States shall ensure ***mechanisms are in place to enable*** market operators to ***notify*** the competent authority ***of*** incidents ***that have a*** significant impact on the security of the core services they provide.

Or. en

Justification

The obligation to report incidents could lead to perverse incentives for businesses to look for and address incidents, and lead to a 'tick-box' compliance culture, instead of full scale behavioural change. A voluntary approach where market operators are encouraged to report incidents would therefore be preferable.

Amendment 297
Jürgen Creutzmann

Proposal for a directive
Article 14 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the security of the core services they provide.	2. Member States shall ensure that public administrations and market operators notify to the competent authority***, in the Member State where the core services are affected,*** incidents having a significant impact on the security ***and/or continuity*** of the core services they provide.

Or. en

Justification

It should be clarified which competent authority should receive notifications. Furthermore, adaptation to ENISA guidelines on incident reporting.

Amendment 298
Christian Ehler, Manfred Weber

Proposal for a directive
Article 14 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the security of the core services they provide.	2. Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the security of the core services they provide

completely and without measurable delay.

Or. en

Amendment 299
Amelia Andersdotter

Proposal for a directive
Article 14 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a ***significant*** impact on the security of the core services they provide.	2. Member States shall ensure that public administrations and market operators notify to the competent authority incidents having an impact on the security of the core services they provide.

Or. en

Amendment 300
Ivailo Kalfin

Proposal for a directive
Article 14 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. Public administrations and market operators, referred to in Article (3)(8)(a) of this Directive, should report incidents on a voluntary basis and in the event of severe incident, disruption or threat within their network or system.

Or. en

Amendment 301
Ivailo Kalfin

Proposal for a directive
Article 14 – paragraph 2 b (new)

Text proposed by the Commission	*Amendment*
	2b. The single points of contact or national competent authorities shall, as soon as possible, report back to the relevant public administration or market operator which has reported an incident the undertaken actions, decisions or recommendations, as well as of any third party informed, and the security and confidentiality protocols governing the information sharing.

Or. en

Amendment 302
Ivailo Kalfin

Proposal for a directive
Article 14 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The requirements under paragraphs 1 and 2 apply to all market operators ***providing*** services within the European Union.	3. The requirements under paragraphs 1 and 2 apply to all ***public and*** market operators***, referred to in Article (3(8) b, and which provide*** services within the European Union. ***These operators shall notify the incidents referred to in paragraphs 1 and 2 to the single point of contact in the Member State where the core service is affected. Where core services in more than one Member State are affected, the single point of contact which has received the notification shall, based on the information provided by the originating source, alert the other single points of contact concerned, throughout mutual pre-defined confidentiality and security protocols. The originating source should be informed, as soon as possible, which other single points of contact have been informed of the incident, as well as of any undertaken steps, results or any information with relevance to the***

incident.

Or. en

Amendment 303
Christian Ehler, Manfred Weber

Proposal for a directive
Article 14 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The requirements under paragraphs 1 and 2 apply to all market operators providing services within the European Union.	3. The requirements under paragraphs 1 and 2 apply to all market operators providing services within the European Union. ***Public authorities and market operators should provide disclosure tailored to their particular circumstances.***

Or. en

Amendment 304
Ivailo Kalfin

Proposal for a directive
Article 14 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The competent authority may inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident ***is in the public interest***. Once a year, ***the competent authority*** shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.	4. The competent authority may inform the public, or require the public administrations and market operators to do so, where it determines that ***public interest in the*** disclosure of the incident ***outweighs possible reputational and commercial damages for the public administration or market operator in question. Administrations and operators shall have the right to make the case to the competent authority as to whether disclosure is appropriate prior to determinations being made. In any case, the Member States should avoid disclosure of business confidential***

information. Once a year, ***they*** shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.

Or. en

Amendment 305
Vicky Ford

Proposal for a directive
Article 14 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The competent authority may inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.	4. The competent authority may inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph. ***In case of incidents notified to the cooperation network referred to in Article 8, other national competent authorities shall not make public any information received on risks or incidents without approval of the notifying competent authority.***

Or. en

Amendment 306
Amelia Andersdotter

Proposal for a directive
Article 14 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The competent authority may inform the	4. The competent authority may inform the

public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.

public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. ***In particular, the competent authority shall ensure that members of the public can mitigate risks to themselves arising from any security incident in a public or market operated service.*** Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.

Or. en

Amendment 307
Jürgen Creutzmann

Proposal for a directive
Article 14 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The competent authority ***may*** inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest***.*** Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.	4. The competent authority***, after consultation with the concerned public administration or market operator, may*** inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest ***and where the latter outweighs any conflicting interests of the public administration or market operator concerned.*** Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.

Or. en

Justification

Prior consultation and weighting of the respective interests of the public and entities concerned is important. Additional input would allow the competent authority to properly

assess whether disclosure is necessary and it would allow concerned public administrations and market operators to prepare for any impacts, which disclosure might have on their services, be they e.g. further security incidents due to disclosure of vulnerabilities or potential reputational impacts.

Amendment 308
Christian Ehler, Manfred Weber

Proposal for a directive
Article 14 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The competent authority may inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. ***Once a year***, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.	4. The competent authority may inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. ***Every six months***, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.

Or. en

Amendment 309
Francisco Sosa Wagner
Proposal for a directive
Article 14 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The competent authority ***may*** inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.	4. The competent authority ***must*** inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.

Or. es

Justification

It should be made obligatory to inform the public of any incident of public interest, with suitable limitations to ensure that on-going incidents are resolved. This is a fundamental exercise in transparency and balancing aimed at evening out the power exercised over personal data made available to the national authorities.

Amendment 310
Christian Ehler, Manfred Weber

Proposal for a directive
Article 14 – paragraph 4 – subparagraph 1 (new)

Text proposed by the Commission	*Amendment*
	Besides reporting to the competent authority market operators shall be encouraged to announce incidents involving their corporation in their financial reports (on a voluntary basis).

Or. en

Justification

Cyber incidents could imply major financial losses and substantial costs. Shareholder and investors ought to be informed about the consequences of these incidents. By encouraging companies to publish cyber incidents on a voluntary basis the cross-sectoral discussion on the likeliness of future incidents, the dimension of those risks, as well as the appropriateness of preventive actions taken to reduce cyber security breaches might be stimulated.

Amendment 311
Vicky Ford

Proposal for a directive
Article 14 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission shall be empowered to adopt delegated acts in accordance with	***deleted***

Article 18 concerning the definition of circumstances in which public administrations and market operators are required to notify incidents.

Or. en

Amendment 312
Amelia Andersdotter

Proposal for a directive
Article 14 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 18 concerning the definition of circumstances in which public administrations and market operators are required to notify incidents.	***deleted***

Or. en

Amendment 313
Jürgen Creutzmann

Proposal for a directive
Article 14 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Subject to any delegated act adopted under paragraph 5, the competent authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which public administrations and market operators are required to notify incidents.	***deleted***

Or. en

Justification

The circumstances in which public administrations and market operators are required to notify should be solely based on the Commission's delegated act in the preceding paragraph. Otherwise operators with cross-border or even EU-wide service provision could face diverging instructions / guidelines and could theoretically be required to notify the very same incident in one Member State but not in another.

Amendment 314
Amelia Andersdotter

Proposal for a directive
Article 14 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Subject to any delegated act adopted under paragraph 5, the competent authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which public administrations and market operators are required to notify incidents.	***deleted***

Or. en

Amendment 315
Vicky Ford

Proposal for a directive
Article 14 – paragraph 6

Text proposed by the Commission	*Amendment*
6. ***Subject to any delegated act adopted under paragraph 5,*** the competent authorities ***may adopt guidelines and, where necessary, issue instructions*** concerning the circumstances in which ***public administrations and*** market operators are required to notify incidents.	6. The competent authorities ***or single points of contact shall adopt guidelines*** concerning the circumstances in which market operators are required to notify incidents.

Or. en

Justification

As the delegated act has been removed there will be a clear need to produce clear guidelines to specify when market operators are required to notify incidents to ensure clarity for businesses.

Amendment 316
Amelia Andersdotter

Proposal for a directive
Article 14 – paragraph 7

Text proposed by the Commission	*Amendment*
7. The Commission shall be empowered to define, by means of implementing acts, the formats and procedures applicable for the purpose of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).	***deleted***

Or. en

Amendment 317
Vicky Ford

Proposal for a directive
Article 14 – paragraph 7

Text proposed by the Commission	*Amendment*
7. The Commission shall be empowered to define, by means of implementing acts, the formats and procedures applicable for the purpose of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).	***deleted***

Or. en

Amendment 318
Amelia Andersdotter

Proposal for a directive
Article 14 – paragraph 8

Text proposed by the Commission	*Amendment*
8. Paragraphs 1 and 2 shall not apply to microenterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises[35] .	***deleted***

[35] OJ L 124, 20.5.2003, p. 36.

Or. en

Amendment 319
Vicky Ford

Proposal for a directive
Article 14 – paragraph 8

Text proposed by the Commission	*Amendment*
8. Paragraphs 1 and 2 shall not apply to microenterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises[35].	8. Paragraphs 1 and 2 shall not apply to microenterprises ***and SMEs*** as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises[35].
[35] OJ L 124, 20.5.2003, p. 36.	[35] OJ L 124, 20.5.2003, p. 36.

Or. en

Amendment 320
Amelia Andersdotter

Proposal for a directive
Article 15 – paragraph 1

Text proposed by the Commission	*Amendment*
1. ***Member States shall ensure that*** the competent authorities ***have all the powers necessary to*** investigate cases of non-compliance ***of public administrations or market operators with their*** obligations ***under Article 14*** and the effects thereof on the security of networks and information systems.	1. The competent authorities ***shall*** investigate cases of non-compliance ***with the*** obligations ***of this Directive*** and the effects thereof on the security of networks and information systems.

Or. en

Amendment 321
Jürgen Creutzmann

Proposal for a directive
Article 15 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that the competent authorities have all the powers necessary to ***investigate cases of non-compliance*** of public administrations or market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems.	1. Member States shall ensure that the competent authorities have all the powers necessary to ***ensure compliance*** of public administrations or market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems.

Or. en

Justification

Member states should decide upon which powers competent authorities should have to ensure compliance.

Amendment 322
Ivailo Kalfin

Proposal for a directive
Article 15 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.	***deleted***

Or. en

Amendment 323
András Gyürk

Proposal for a directive
Article 15 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) ***undergo a security audit carried out by a qualified independent body or national authority and make the results thereof*** available to the competent authority.	(b) ***demonstrate the effective implementation of a policies (measured by ongoing application of industry global best-practices) by suitable means, notably by making*** available to the competent authority ***or to the single point of contact the results of a security audit carried out by an authorised internal representative or a qualified external auditor***.

Or. en

Amendment 324
Jürgen Creutzmann

Proposal for a directive
Article 15 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.	(b) undergo***, where the information provided according to point (a) of this paragraph is not conclusive,*** a security audit carried out by a qualified independent

body or national authority and make the results thereof available to the competent authority.

Or. en

Justification

Security audits should not be carried out for their own sake but only in case a public administration or market operator fails to provide convincing information on the state of the security of its networks and information systems.

Amendment 325
Jürgen Creutzmann

Proposal for a directive
Article 15 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ensure that competent authorities have the power to issue binding instructions to market operators and public administrations.	***deleted***

Or. en

Justification

No longer needed as it is proposed in paragraph 1 to give competent authorities "all powers necessary to ensure compliance [...]", which may or may not entail binding instructions.

Amendment 326
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 15 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ensure that competent authorities have the power to issue binding instructions to market	3. Member States shall ensure that competent authorities have the power to issue binding instructions to market

operators and public administrations.	operators and public administrations ***and to issue enactments for legal and liability obligations, especially where a voluntary approach does not prove efficient***.

Or. en

Amendment 327
Amelia Andersdotter

Proposal for a directive
Article 15 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The competent authorities shall notify incidents of a suspected serious criminal nature to law enforcement authorities.	***deleted***

Or. en

Amendment 328
Jürgen Creutzmann

Proposal for a directive
Article 15 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The competent authorities ***shall*** notify incidents of a suspected serious criminal nature to law enforcement authorities.	4. The competent authorities ***may, subsequent to informing the concerned public administration or market operator,*** notify incidents of a suspected serious criminal nature to law enforcement authorities.

Or. en

Justification

While incidents of a serious criminal nature should be notified to law enforcement authorities, the concerned companies should be informed in order to be able to prepare for any impacts on their interests. Furthermore, as the term 'serious criminal nature' might be interpreted

differently across Member States and in order to give competent authorities the needed discretion in judging incidents, 'shall' is replaced by 'may'.

Amendment 329
András Gyürk

Proposal for a directive
Article 15 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.	5. ***Without prejudice to applicable data protection law, and in full consultation with the relevant data controllers and processors,*** The competent authorities ***and the single points of contact*** shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.

Or. en

Amendment 330
Vicky Ford

Proposal for a directive
Article 16 – paragraph 1

Text proposed by the Commission	*Amendment*
1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security.	1. To ensure convergent implementation of Article 14(1), Member States***, without prescribing the use of any particular technology,*** shall encourage the use of ***interoperable*** standards and /or specifications relevant to networks and information security. ***Such standards and/or specifications where appropriate shall take into account international and/or global equivalents.***

Or. en

Amendment 331
Ivailo Kalfin

Proposal for a directive
Article 16 – paragraph 1

Text proposed by the Commission	*Amendment*
1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security.	1. To ensure convergent implementation of Article 14(1), Member States***, without prescribing the use of any particular technology,*** shall encourage the use of ***open and interoperable international*** standards and/or specifications relevant to networks and information security.

Or. en

Amendment 332
Amelia Andersdotter

Proposal for a directive
Article 16 – paragraph 1

Text proposed by the Commission	*Amendment*
1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security.	1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of ***open*** standards and/or specifications relevant to networks and information security***, and ensure that these standards comply with existing Union legislation***.

Or. en

Amendment 333
Jürgen Creutzmann

Proposal for a directive
Article 16 – paragraph 1

Text proposed by the Commission	*Amendment*
1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security.	1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of ***European and international*** standards and/or specifications relevant to networks and information security.

Or. en

Justification

Diverging national standards should be avoided to the degree possible in order to have a level playing field and comparable legal requirements across Member States.

Amendment 334
Vicky Ford

Proposal for a directive
Article 16 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ***The Commission*** shall draw up***, by means of implementing acts*** a list of the standards referred to in paragraph 1***. The list shall be published in the Official Journal*** of the ***European Union***.	2. ***An industry-led taskforce*** shall draw up a list of the standards ***and/or specifications*** referred to in paragraph 1 ***with the help*** of the ***Commission***.

Or. en

Amendment 335
Francisco Sosa Wagner
Proposal for a directive
Article 17 – paragraph 1

Text proposed by the Commission	*Amendment*
1. ***Member States shall lay down rules on*** sanctions applicable to infringements of the national provisions adopted pursuant to this Directive ***and*** shall take all measures	1. ***The Commission shall bring forward a resolution establishing the minimum criteria for a system of*** sanctions applicable to infringements of the national

necessary to ensure that they are implemented. ***The sanctions provided for must be effective, proportionate and dissuasive. The Member States shall notify those provisions to the Commission by the date of transposition of this Directive at the latest and shall notify it without delay of any subsequent amendment affecting them***.	provisions adopted pursuant to this Directive***. Member States*** shall take all measures necessary to ensure that they are implemented.

Or. es

Justification

Harmonised minimum standards should be introduced to avoid economic imbalances and competition issues liable to affect security itself in some Member States with minimum sanctions requirements.

Amendment 336
Jürgen Creutzmann

Proposal for a directive
Article 17 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall lay down rules on sanctions applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The sanctions provided for must be effective, proportionate and dissuasive. The Member States shall notify those provisions to the Commission by the date of transposition of this Directive at the latest and shall notify it without delay of any subsequent amendment affecting them.	1. Member States shall lay down rules on sanctions applicable to ***negligent and intentional*** infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The sanctions provided for must be effective, proportionate and dissuasive. The Member States shall notify those provisions to the Commission by the date of transposition of this Directive at the latest and shall notify it without delay of any subsequent amendment affecting them.

Or. en

Justification

It should be clear that penalties can only be applied to infringements where market operators

have failed to take all measures that could have been reasonable expected of them. Market operators could otherwise be discouraged from reporting incidents.

Amendment 337
András Gyürk

Proposal for a directive
Article 17 – paragraph 1 – subparagraph 1 (new)

Text proposed by the Commission	*Amendment*
	Member States shall guarantee that the penalties in paragraph 1 of this Article are applied only if market operators and public administrations due to gross negligence or intent failed to fulfil their obligations under Chapter IV.

Or. en

Amendment 338
Silvia-Adriana Ţicău
Proposal for a directive
Article 18 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The power to adopt delegated acts referred to in Articles 9(2), 10(5) and 14(5) shall be conferred on the Commission. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.	2. Se conferă Comisiei competenţa de a adopta actele delegate menţionate la articolul 9 alineatul (2), la articolul 10 alineatul (5) şi la articolul 14 alineatul (5)***, for a period of five years from [OPOCE please introduce date of the entry into force of this Directive].*** The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

Or. ro

Amendment 339
Amelia Andersdotter

Proposal for a directive
Article 18 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The power to adopt delegated acts referred to in Articles ***9(2),*** 10(5) and 14(5) shall be conferred on the Commission. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.	2. The power to adopt delegated acts referred to in Articles 10(5) and 14(5) shall be conferred on the Commission. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

Or. en

Amendment 340
Amelia Andersdotter

Proposal for a directive
Article 18 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The delegation of powers referred to in Articles ***9(2),*** 10(5) and 14(5) 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 powers 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 act already in force.	3. The delegation of powers referred to in Articles 10(5) and 14(5) 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 powers 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 act already in force.

Or. en

Amendment 341
Amelia Andersdotter

Proposal for a directive
Article 18 – paragraph 5

Text proposed by the Commission	*Amendment*
5. A delegated act adopted pursuant to Articles ***9(2),*** 10(5) and 14(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and 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.	5. A delegated act adopted pursuant to Articles 10(5) and 14(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Or. en

Amendment 342
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
The Commission shall periodically review the functioning of this Directive and report to the European Parliament and the Council. The first report shall be submitted no later than ***three*** years after the date of transposition referred to in Article 21. For this purpose, the Commission may request Member States to provide information without undue delay.	The Commission shall periodically review the functioning of this Directive and report to the European Parliament and the Council. The ***main focus of the review should be the provisions of Annex II, in particular the provisions regarding the internet enablers. The*** first report shall be submitted no later than ***two*** years after the date of transposition referred to in Article 21. For this purpose, the Commission may

request Member States to provide information without undue delay.

The review should also evaluate the voluntary incentives for stock listed companies set forth in this Directive: The effectiveness of this voluntary approach is to be evaluated by the competent national authority every 2 years. Results ought to be reported to the European Commission without delay. Should the voluntary approach aimed at protecting customers and investors interests not prove sufficient Member States shall introduce legal obligations.

Or. en

Justification

To stay abreast of changing threats and conditions in the field of cyber security Annex II shall be reviewed and edited regularly.

Amendment 343
Silvia-Adriana Ţicău
Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
The Commission shall ***periodically*** review the functioning of this Directive and report to the European Parliament and the Council. The first report shall be submitted no later than three years after the date of transposition referred to in Article 21. For this purpose, the Commission may request Member States to provide information without undue delay.	The Commission shall ***every three years*** review the functioning of this Directive and report to the European Parliament and the Council. The first report shall be submitted no later than three years after the date of transposition referred to in Article 21.For this purpose, the Commission may request Member States to provide information without undue delay.

Or. ro

Amendment 344
Ivailo Kalfin

Proposal for a directive
Annex 1 – paragraph 1 – point 1 – point c

Text proposed by the Commission	*Amendment*
(c) The offices of the CERT and the supporting information systems shall be located in secure sites**.**	(c) The offices of the CERT and the supporting information systems shall be located in secure sites ***with secured network information systems.***

Or. en

Amendment 345
Christian Ehler, Maria Da Graça Carvalho, Manfred Weber

Proposal for a directive
Annex 1 – paragraph 1 – point 2 – point a – indent 1

Text proposed by the Commission	*Amendment*
– Monitoring incidents at a national level,	– ***Detection and*** monitoring incidents at a national level,

Or. en

Amendment 346
Christian Ehler, Manfred Weber

Proposal for a directive
Annex 2 – heading 1

Text proposed by the Commission	*Amendment*
List of market operators	List of market operators ***- This list is non-exhaustive and shall be reviewed every 2 years:***

Or. en

Amendment 347
Ivailo Kalfin

Proposal for a directive
Annex 2 – heading 1

Text proposed by the Commission	*Amendment*
List of ***market*** operators	List of ***public and private*** operators

Or. en

Amendment 348
Jürgen Creutzmann

Proposal for a directive
Annex 2 – paragraph 1 – point 1

Text proposed by the Commission	*Amendment*
1. e-commerce platforms	***deleted***

Or. en

Amendment 349
Ivailo Kalfin

Proposal for a directive
Annex 2 – paragraph 1 – point 2

Text proposed by the Commission	*Amendment*
2. Internet payment gateways	***deleted***

Or. en

Amendment 350
Jürgen Creutzmann

Proposal for a directive
Annex 2 – paragraph 1 – point 2

Text proposed by the Commission	*Amendment*
2. Internet payment gateways	***deleted***

Or. en

Amendment 351
Jürgen Creutzmann

Proposal for a directive
Annex 2 – paragraph 1 – point 3

Text proposed by the Commission	*Amendment*
3. Social networks	***deleted***

Or. en

Amendment 352
Jürgen Creutzmann

Proposal for a directive
Annex 2 – paragraph 1 – point 4

Text proposed by the Commission	*Amendment*
4. Search engines	***deleted***

Or. en

Amendment 353
Christian Ehler, Manfred Weber

Proposal for a directive
Annex 2 – paragraph 1 – point 4

Text proposed by the Commission	*Amendment*
4. Search engines	***deleted***

Or. en

Amendment 354
Jürgen Creutzmann

Proposal for a directive
Annex 2 – paragraph 1 – point 5

Text proposed by the Commission	*Amendment*
5. Cloud computing services	***deleted***

Or. en

Amendment 355
Ivailo Kalfin

Proposal for a directive
Annex 2 – paragraph 1 – point 5

Text proposed by the Commission	*Amendment*
5. Cloud computing services	5. ***Business-to-users*** Cloud computing services

Or. en

Amendment 356
Ioannis A. Tsoukalas

Proposal for a directive
Annex 2 – paragraph 1 – point 5

Text proposed by the Commission	*Amendment*
5. Cloud computing services	5. Cloud computing ***and storage*** services

Or. en

Amendment 357
Ivailo Kalfin

Proposal for a directive
Annex 2 – paragraph 1 – point 5 a (new)

Text proposed by the Commission	*Amendment*
	5a. Information and Communication Technologies: Business-to-business Cloud computing services, Internet payment gateways.

Or. en

Amendment 358
Jürgen Creutzmann

Proposal for a directive
Annex 2 – paragraph 1 – point 5 a (new)

Text proposed by the Commission	*Amendment*
	5a. Water services.

Or. en

Amendment 359
Christian Ehler, Manfred Weber

Proposal for a directive
Annex 2 – paragraph 1 – point 5 a (new)

Text proposed by the Commission	*Amendment*
	5a. Hardware developers and producers

Or. en

Amendment 360
Christian Ehler, Manfred Weber

Proposal for a directive
Annex 2 – paragraph 1 – point 5 b (new)

Text proposed by the Commission	*Amendment*
	5b. Software developers and producers

Or. en

Amendment 361
Jürgen Creutzmann

Proposal for a directive
Annex 2 – paragraph 1 – point 6

Text proposed by the Commission	*Amendment*
6. Application stores	***deleted***

Or. en

Amendment 362
Ioannis A. Tsoukalas

Proposal for a directive
Annex 2 – paragraph 1 – point 6 a (new)

Text proposed by the Commission	*Amendment*
	6a. High Performance Computing infrastructures

Or. en