AMENDMENTS 001-138
by the Committee on the Internal Market and Consumer Protection

Report
Andreas Schwab **A7-0103/2014**
High common level of network and information security

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

Amendment 1

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 of Union citizens as well as to*** economic activities and social welfare, and in particular to the functioning of the internal market.

Amendment 2

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,	(2) The magnitude***,*** frequency ***and impact*** of security incidents is increasing and represents a major threat to the functioning of networks and information systems. ***Those systems may also become an easy target for deliberate harmful actions***

generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.	***intended to damage or interrupt the operation of the 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 ***and, ultimately, endanger the wellbeing of Union citizens and the ability of Member States to protect themselves and ensure the security of critical infrastructures.***

Amendment 3

Proposal for a directive
Recital 3 a (new)

Text proposed by the Commission	*Amendment*
	(3a) Since common causes of system failure continue to be unintentional, such as natural causes or human error, infrastructure should be resilient both to intentional and unintentional disruptions, and operators of critical infrastructure should design resilience-based systems.

Amendment 4

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 ***at least certain market*** operators of information infrastructure to promote a culture of risk management and ensure that the most serious incidents are reported. ***Companies listed on the stock markets should be***

encouraged to make incidents public in their financial reports on a voluntary basis. The legal framework should be based upon the need to safeguard the privacy and integrity of citizens. The Critical Infrastructure Warning Information Network (CIWIN) should be expanded to the market operators covered by this Directive.

Amendment 5

Proposal for a directive
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4a) While public administrations, because of their public mission, should exert due diligence in the management and the protection of their own network and information systems, this Directive should focus on critical infrastructure essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, financial market infrastructures or health. Software developers and hardware manufacturers should be excluded from the scope of this Directive.

Amendment 6

Proposal for a directive
Recital 4 b (new)

Text proposed by the Commission	*Amendment*
	(4b) Cooperation and coordination between the relevant Union authorities with the High Representative/Vice President, with the responsibility for the Common Foreign and Security Policy and the Common Security and Defence Policy, as well as the EU Counter-terrorism Coordinator should be ensured where incidents having a significant impact are perceived to be of an external and terrorist nature.

Amendment 7

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 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.	(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 market operators in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level. ***Universities and research centres have a decisive role in spurring research, development and innovation in those areas and should be provided with adequate funding.***

Amendment 8

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 cyber security skills,*** exchange of information and coordination of actions, and common minimum security requirements. ***Minimum common standards should be applied in accordance with appropriate recommendations by the Cyber Security Coordination Groups (CSGC).***

Amendment 9

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.	(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. ***No Member States are obliged to disclose EU classified information as defined in Council Decision of 31 March 2011 on the security rules for protecting EU classified information (2011/292/EU), information subject to non-disclosure agreements or informal non-disclosure agreements, such as the Traffic Light Protocol.***

Justification

This amendment aims at clarifying the treatment of confidential information within the scope of this Directive.

Amendment 10

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	(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 out in this Directive,*** in order to reach capacity response levels allowing for effective and

incidents.	efficient cooperation at national and Union level in case of incidents, ***respecting and protecting private life and personal data***. ***Each Member State should therefore be obliged to meet common standards regarding data format and the exchangeability of data to be shared and evaluated. Member States should be able to ask for the assistance of the European Union Agency for Network and Information Security (ENISA) in developing their national NIS strategies, based on a common minimum NIS strategy blueprint.***

Amendment 11

Proposal for a directive
Recital 10 a (new)

Text proposed by the Commission	*Amendment*
	(10a) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, and to avoid duplication, Member States should be able to designate more than one national competent authority in charge of fulfilling the tasks linked to the security of the networks and information systems of market operators under this Directive. However, in order to ensure smooth cross-border cooperation and communication, it is necessary for each Member State, without prejudice to sectoral regulatory arrangements, to designate only one national single point of contact in charge of cross-border cooperation at Union level. Where its constitutional structure or other arrangements so require, a Member State should be able to designate only one authority to carry out the tasks of the competent authority and the single point of contact. The competent authorities and the single points of contact should be civilian bodies, subject to full democratic oversight and should not fulfil any tasks in the field of intelligence, law

	enforcement or defence or be organisationally linked in any form to bodies active in those fields.

Amendment 12

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 ***at any time***. ***Security systems of public administrations should be safe and subject to democratic control and scrutiny. Commonly required equipment and capabilities should comply with commonly agreed technical standards as well as standards procedures of operation (SPO).*** Well-functioning Computer Emergency Response Teams ***(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. ***These CERTs should be enabled to interact on the basis of common technical standards and SPO. In view of the different characteristics of existing CERTs, which responds to different subject needs and actors, Member States should guarantee that each of the sectors referred to in the list of market operators set out in this Directive is provided services by at least one CERT. Regarding cross-border CERT cooperation, Member States should ensure that CERTs have sufficient means to participate in the existing international and Union cooperation networks already in place.***

Justification

Interoperability has to be ensured.

Amendment 13

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 to bring them into permanent communication and support their cooperation. This secure and effective cooperation mechanism***, including the participation of market operators, where appropriate,*** should enable structured and coordinated information exchange, detection and response at Union level.

Amendment 14

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	(13) 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 the organisation

building capacity, steering the organisation of peer reviews and NIS exercises.	of peer reviews and NIS exercises.

Amendment 15

Proposal for a directive
Recital 13 a new

Text proposed by the Commission	*Amendment*
	(13a) Where appropriate, Member States should be able to use or adapt existing organisational structures or strategies when applying the provisions of this Directive.

Amendment 16

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. ***Existing structures within the Union should be fully used for that purpose.*** 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***, using transparent methods.***

Amendment 17

Proposal for a directive
Recital 15

Text proposed by the Commission	*Amendment*
(15) As most network and information	(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.	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*** exchange of ***relevant information and*** operational support ***and strategically analysed information,*** in case of incidents. ***To effectively encourage the sharing of information and of best practices, it is essential to ensure that market operators, 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 increased operational or security risks.***

Amendment 18

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 Union citizens and market operators, the ***single points of contact*** should set up a common ***Union-wide*** website to publish non confidential information on the incidents***, risks and means of risk mitigation, and where necessary advise on appropriate maintenance measures***. ***The information on the website should be accessible irrespective of the device used. Any personal data published on that website should be limited only to what is necessary and should be as anonymous as possible.***

Amendment 19

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 ***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.

Amendment 20

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 network.	(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 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 network.

Amendment 21

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***	(20) Upon receipt of an early warning and its assessment, the ***single points of contact***

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.	should agree on a coordinated response under the Union NIS cooperation plan. ***The single points of contact, ENISA*** as well as the Commission should be informed about the measures adopted at national level as a result of the coordinated response.

Amendment 22

Proposal for a directive
Recital 21

Text proposed by the Commission	*Amendment*
(21) Given the global nature of NIS problems, there is a need for closer international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues.	(21) Given the global nature of NIS problems, there is a need for closer international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues. ***Any framework for such international cooperation should be subject to the provisions of Directive 95/46/EC and Regulation (EC) No 45/2001.***

Amendment 23

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 market operators. A culture of risk management***, close cooperation and trust***, involving risk assessment and the implementation of security measures ***appropriate to the risks and incidents, whether deliberate or accidental,*** should be promoted and developed through appropriate regulatory requirements and voluntary industry practices. Establishing a ***trustworthy*** level playing field is also essential to the effective functioning of the cooperation network to ensure effective cooperation from all Member States.

Amendment 24

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 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.***	(24) Those obligations should be extended beyond the electronic communications sector ***to operators of infrastructure which rely heavily on information and communications technology and are essential to the maintenance of vital economic or societal functions such as electricity and gas, transport, credit institutions, financial market infrastructures and health. Disruption of those network and information systems would affect the internal market. While the obligations set out in this Directive should not extend*** 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 ***in general or*** application stores***,*** these might***, on a voluntary basis, inform the competent authority or single point of contact of*** those ***network security incidents they deem appropriate. The competent authority or the single point of contact should, if possible, present the market operators that informed of the incident with strategically analysed*** information ***that will help to overcome the security threat***.

Amendment 25

Proposal for a directive
Recital 24 a (new)

Text proposed by the Commission	*Amendment*
	(24a) While hardware and software providers are not market operators comparable to those covered in this Directive, their products facilitate the security of network and information systems. They therefore have an important role in enabling market operators to secure their network and information infrastructures. Given that hardware and software products are already subject to existing rules on product liability, Member States should ensure that those rules are enforced.

Amendment 26

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 market operators should not require that a particular commercial information and communications technology product be designed, developed or manufactured in a particular manner.

Amendment 27

Proposal for a directive
Recital 26

Text proposed by the Commission	*Amendment*
(26) The ***public administrations and*** market operators should ensure security of the networks and systems which are under their control. These would be primarily private networks and systems managed either by their internal IT staff or the security of which has been outsourced. The security and notification obligations should apply to the relevant market operators ***and public administrations*** regardless of whether they perform the maintenance of	(26) The market operators should ensure security of the networks and systems which are under their control. These would be primarily private networks and systems managed either by their internal IT staff or the security of which has been outsourced. The security and notification obligations should apply to the relevant market operators regardless of whether they perform the maintenance of their network and information systems internally or

their network and information systems internally or outsource it.	outsource it.

Amendment 28

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 ***and 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. ***Competent authorities and single points of contact should inform manufacturers and service providers of affected ICT products and services about incidents having a significant impact notified to them.*** Publicity of incidents reported to the competent authorities ***and single points of contact*** should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the market operators reporting incidents. In the implementation of the notification obligations, competent authorities ***and single points of contact*** should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the ***deployment*** of appropriate security fixes. ***As a general rule, single points of contact should not disclose the personal data of individuals involved in incidents. Single points of contact should only disclose personal data where the disclosure of such data is necessary and proportionate in view of the objective pursued.***

Amendment 29

Proposal for a directive
Recital 29

Text proposed by the Commission	*Amendment*
(29) Competent authorities should have the	(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.	necessary means to perform their duties, including powers to obtain sufficient information from market operators 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.

Amendment 30

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 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***, single points of contact*** 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.

Amendment 31

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	(31) Personal data are in many cases compromised as a result of incidents. ***Member States and market operators should protect personal data stored,***

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. 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.

processed or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, access, disclosure or dissemination; and ensure the implementation of a security policy with respect to the processing of personal data. In this context, competent authorities***, single points of contact*** and data protection authorities should cooperate and exchange information ***including, where appropriate, with market operators, in order*** to tackle the personal data breaches resulting from incidents ***in line with applicable data protection rules***. The obligation to notify security incidents ***should be carried out*** in a way that minimises the administrative burden in case the security incident is also a personal data breach ***that has to be notified in accordance with Union data protection law.*** ENISA ***should*** assist by developing information exchange mechanisms and ***a*** single notification template ***that*** would facilitate the reporting of incidents compromising personal data thereby easing the administrative burden on businesses and public administrations.

Amendment 32

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,	(32) Standardisation of security requirements is a market-driven process ***of a voluntary nature that should allow market operators to use alternative means to achieve at least similar outcomes***. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified ***interoperable*** 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 necessary step forward*** might be to draft

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] .	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]. ***In particular, ETSI, CEN and CENELEC should be mandated to suggest effective and efficient Union open security standards, where technological preferences are avoided as much as possible, and which should be made easily manageable by small and medium-sized market operators. 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 making sure 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.

Amendment 33

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 ***societal, political,*** technological or market conditions

Amendment 34

Proposal for a directive
Recital 34

Text proposed by the Commission	*Amendment*
(34) In order to allow for the proper functioning of the cooperation network, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of the definition of the criteria to be fulfilled for a Member State to be authorized to participate to the secure information-sharing system***, of the*** further specification of the triggering events for early warning, ***and of the definition of the circumstances in which market operators and public administrations are required to notify incidents***.	(34) In order to allow for the proper functioning of the cooperation network, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of the ***common set of interconnection and security standards for*** the secure information-sharing ***infrastructure and the*** further specification of the triggering events for early warning.

Amendment 35

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.	(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 ***single points of contact*** and the Commission within the cooperation network, ***without prejudice to existing cooperation mechanisms at national level,*** the Union NIS cooperation plan ***and*** the formats and procedures applicable to ***the notification of*** incidents ***having a significant impact***. 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.

Justification

This amendment replaces AM 20. The amendment aims at correcting a mistake in the Commission proposal with regard to the content of the planned implementing act and reflecting the new amendment proposed to Article 9 paragraph 3.

Amendment 36

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 sectoral committees and relevant bodies set up at Union level in particular in the field of ***e-government,*** energy, transport***, health and defence***.

Amendment 37

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 ***or a single point of contact***, in accordance with Union and national rules on business confidentiality, should be exchanged with the Commission, ***its relevant agencies, single points of contact 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***, necessary and*** proportionate to the purpose of such exchange***, and should respect pre-defined criteria for confidentiality and security, in accordance with Council Decision of 31 March 2011 on the security rules for protecting EU classified information (2011/292/EU), information subject to non-disclosure agreements and informal non-disclosure agreements, such as the Traffic Light Protocol***

Amendment 38

Proposal for a directive
Recital 39

Text proposed by the Commission	*Amendment*
(39) The sharing of information on risks and incidents within the cooperation network and compliance with the requirements to notify incidents to the national competent authorities may require the processing of personal data. Such a processing of personal data is necessary to meet the objectives of public interest pursued by this Directive and is thus legitimate under Article 7 of Directive 95/46/EC. It does not constitute, in relation to these legitimate aims, a disproportionate and intolerable interference impairing the very substance of the right to the protection of personal data guaranteed by Article 8 of the Charter of fundamental rights. In the application of this Directive, Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents should apply as appropriate. When data are processed by Union institutions and bodies, such processing for the purpose of implementing this Directive should comply with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.	(39) The sharing of information on risks and incidents within the cooperation network and compliance with the requirements to notify incidents to the national competent authorities ***or single points of contact*** may require the processing of personal data. Such a processing of personal data is necessary to meet the objectives of public interest pursued by this Directive and is thus legitimate under Article 7 of Directive 95/46/EC. It does not constitute, in relation to these legitimate aims, a disproportionate and intolerable interference impairing the very substance of the right to the protection of personal data guaranteed by Article 8 of the Charter of fundamental rights. In the application of this Directive, Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents should apply as appropriate. When data are processed by Union institutions and bodies, such processing for the purpose of implementing this Directive should comply with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

Amendment 39

Proposal for a directive
Recital 41 a (new)

Text proposed by the Commission	*Amendment*
	(41a) In accordance with the Joint Political Declaration of Member States

	and the Commission on explanatory documents of 28 September 2011, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

Amendment 40

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 a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated***,*** efficient ***and effective*** handling of and response to risks and incidents affecting network and information systems ***with the participation of relevant stakeholders***;

Amendment 41

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

Text proposed by the Commission	*Amendment*
(c) establishes security requirements for market operators ***and public administrations***.	(c) establishes security requirements for market operators.

Amendment 42

Proposal for a directive
Article 1 – paragraph 5

Text proposed by the Commission	*Amendment*
5. This Directive shall also be without	5. This Directive shall also be without

prejudice to Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data' and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and to 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.	prejudice to Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and to the Regulation ***(EC) No 45/2001*** of the European Parliament and of the Council of ***18 December 2000*** on the protection of individuals with regard to the processing of personal data ***by the Community institutions and bodies*** and on the free movement of such data. ***Any use of the personal data shall be limited to what is strictly necessary for the purposes of this Directive, and those data shall be as anonymous as possible, if not completely anonymous.***

Amendment 43

Proposal for a directive
Article 1 a (new)

Text proposed by the Commission	*Amendment*
	Article 1a
	Protection and processing of personal data
	1. Any processing of personal data in the Member States pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC and Directive 2002/58/EC.
	2. Any processing of personal data by the Commission and ENISA pursuant to this Regulation shall be carried out in accordance with Regulation (EC) No 45/2001.

	3. Any processing of personal data by the European Cybercrime Centre within Europol for the purposes of this Directive shall be carried out pursuant to Decision 2009/371/JHA.
	4. The processing of personal data shall be fair and lawful and strictly limited to the minimum data needed for the purposes for which they are processed. They shall be kept in a form which permits the identification of data subjects for no longer than necessary for the purpose for which the personal data are processed.
	5. Incident notifications referred to in Article 14 shall be without prejudice to the provisions and obligations regarding personal data breach notifications set out in Article 4 of Directive 2002/58/EC and in Regulation (EU) No 611/2013.

Amendment 44

Proposal for a directive
Article 3 – 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

Amendment 45

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

Text proposed by the Commission	*Amendment*
(c) ***computer*** data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.	(c) ***digital*** data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.

Amendment 46

Proposal for a directive

Article 3 – 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' includes appropriate technical devices, solutions and operating procedures ensuring the security requirements set out in this Directive.***

Amendment 47

Proposal for a directive
Article 3 – point 3

Text proposed by the Commission	*Amendment*
(3) 'risk' means any circumstance or event having a potential adverse effect on security;	(3) 'risk' means any ***reasonably identifiable*** circumstance or event having a potential adverse effect on security;

Amendment 48

Proposal for a directive
Article 3 – 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 event having an actual adverse effect on security;

Amendment 49

Proposal for a directive
Article 3 – 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***

Amendment 50

Proposal for a directive
Article 3 – 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;

Amendment 51

Proposal for a directive
Article 3 – 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***

Amendment 52

Proposal for a Directive
Article 3 – 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 in the fields of energy, transport, banking, ***financial market infrastructures, internet exchange points, food supply chain*** and health***, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions***, a non exhaustive list of which is set out in Annex II***, insofar as the network and information systems concerned are related to its core services;***

Amendment 53

Proposal for a directive

Article 3 – 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;

Amendment 54

Proposal for a directive
Article 3 – point 11 a (new)

Text proposed by the Commission	*Amendment*
	(11a) 'regulated market' means regulated market as defined in point 14 of Article 4 of Directive 2004/39/EC of the European Parliament and of the Council[1a];
	[1a] Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments (OJ L 45, 16.2.2005, p. 18).

Justification

Alignment of the definition with the still to be adopted Regulation of the European Parliament and of the Council on markets in financial instruments and amending Regulation [EMIR] on OTC derivatives, central counterparties and trade repositories.

Amendment 55

Proposal for a directive
Article 3 – point 11 b (new)

Text proposed by the Commission	*Amendment*
	(11b) 'multilateral trading facility (MTF)' means multilateral trading facility as defined in point 15 of Article 4 of Directive 2004/39/EC;

Justification

Alignment of the definition with the still to be adopted Regulation of the European Parliament

and of the Council on markets in financial instruments and amending Regulation [EMIR] on OTC derivatives, central counterparties and trade repositories.

Amendment 56

Proposal for a directive
Article 3 – point 11 c (new)

Text proposed by the Commission	*Amendment*
	(11c) 'organised trading facility' means a multilateral system or facility, which is not a regulated market, a multilateral trading facility or a central counterparty, operated by an investment firm or a market operator, in which multiple third-party buying and selling interests in bonds, structured finance products, emission allowances or derivatives are able to interact in the system in such a way as to result in a contract in accordance with Title II of Directive 2004/39/EC;

Justification

Introduction of the definition in line with and subject to the outcome of the still to be adopted Regulation of the European Parliament and of the Council on markets in financial instruments and amending Regulation [EMIR] on OTC derivatives, central counterparties and trade repositories.

Amendment 57

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

Text proposed by the Commission	*Amendment*
	(ea) Member States may request the assistance of ENISA in developing their national NIS strategies and national NIS cooperation plans, based on a common minimum NIS strategy.

Amendment 58

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

Text proposed by the Commission	*Amendment*
(a) A risk ***assessment plan to identify risks and assess*** the impacts of potential incidents;	(a) A risk ***management framework to establish a methodology for the identification, prioritisation, evaluation and treatment of risks, the assessment of*** the impacts of potential incidents***, prevention and control options, and to define criteria for the choice of possible countermeasures***;

Justification

This amendment replaces AM 29. The Commission proposal would have been too far-reaching with regard to questions of national security of Member States and would have rendered the cooperation plan impracticable and too complex in order to be effective.

Amendment 59

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

Text proposed by the Commission	*Amendment*
(b) The definition of the roles and responsibilities of the various actors involved in the implementation of the ***plan***;	(b) The definition of the roles and responsibilities of the various ***authorities and other*** actors involved in the implementation of the ***framework***;

Amendment 60

Proposal for a directive
Article 5 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within ***one month*** from their adoption.	3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within ***three months*** from their adoption.

Amendment 61

Proposal for a directive
Article 6 – title

Text proposed by the Commission	*Amendment*
National competent ***authority*** on the	National competent ***authorities and single***

security of network and information systems	***points of contact*** on the security of network and information systems

Amendment 62

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 ***one or more civilian*** national competent ***authorities*** on the security of network and information systems (***hereinafter referred to as*** 'competent authority***/ies***').

Justification

This amendment replaces AM 32 and aims at further specifying which type of institution should fulfil the role of national competent authority.

Amendment 63

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

Text proposed by the Commission	*Amendment*
	2a. Where a Member State designates more than one competent authority, it shall designate a civilian national authority, for instance a competent authority, as national single point of contact on the security of network and information systems (hereinafter referred to as 'single point of contact'). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.

Justification

This amendment replaces AM 33 and is in alignment to the new amendment on Article 6 Paragraph 1 by the Rapporteur. It aims at further specifying which type of institution should fulfil the role of single point of contact.

Amendment 64

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

Text proposed by the Commission	*Amendment*
	2b. The competent authorities and the single point of contact of the same Member State shall cooperate closely with regard to the obligations laid down in this Directive.

Amendment 65

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

Text proposed by the Commission	*Amendment*
	2c. The single point of contact shall ensure cross-border cooperation with other single points of contact.

Amendment 66

Proposal for a directive
Article 6 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ensure that the competent authorities have adequate technical, financial and human resources to carry out in an effective and efficient manner the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure the effective, efficient and secure cooperation of the ***competent authorities*** via the network referred to in Article 8.	3. Member States shall ensure that the competent authorities ***and the single points of contact*** have adequate technical, financial and human resources to carry out in an effective and efficient manner the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure the effective, efficient and secure cooperation of the ***single points of contact*** via the network referred to in Article 8.

Amendment 67

Proposal for a directive
Article 6 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall ensure that the competent authorities receive the notifications of incidents from ***public administrations and*** market operators as specified under Article 14(2) and are granted the implementation and enforcement powers referred to under Article 15.	4. Member States shall ensure that the competent authorities ***and single points of contact, where applicable in accordance with paragraph 2a of this Article,*** receive the notifications of incidents from market operators as specified under Article 14(2) and are granted the implementation and enforcement powers referred to under Article 15.

Justification

This amendment replaces AM 37. It aims at clarifying the role of the different authorities in order to avoid duplication of notifications to both the competent authorities and the single points of contact. Given that in some sectors incident notifications are already provided to Union bodies, duplication should be avoided.

Amendment 68

Proposal for a directive
Article 6 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. Where Union law provides for a sector-specific Union supervisory or regulatory body, inter alia on the security of network and information systems, that body shall receive the notifications of incidents in accordance with Article 14(2) from the market operators concerned in that sector and be granted the implementation and enforcement powers referred to under Article 15. That Union body shall cooperate closely with the competent authorities and the single point of contact of the host Member State with regard to those obligations. The single point of contact of the host Member State shall represent the Union body with regard to the obligations laid down in Chapter III.

Amendment 69

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 ***and single points of contact*** shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities and data protection authorities.

Amendment 70

Proposal for a directive
Article 6 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Each Member State shall notify to the Commission without delay the designation of the competent ***authority***, its tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent ***authority***.	6. Each Member State shall notify to the Commission without delay the designation of the competent ***authorities and the single point of contact***, its tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent ***authorities***.

Amendment 71

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') ***for each of the sectors established 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.

Amendment 72

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,	5. The ***CERTs*** shall act under the supervision of the competent authority ***or***

which shall regularly review the adequacy of ***its*** resources, ***its*** mandate and the effectiveness of ***its*** incident-handling process.	***the single point of contact***, which shall regularly review the adequacy of ***their*** resources, ***mandates*** and the effectiveness of ***their*** incident-handling process.

Amendment 73

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

Text proposed by the Commission	*Amendment*
	5a. Member States shall ensure that CERTs have adequate human and financial resources to actively participate in international, and in particular Union, cooperation networks

Amendment 74

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

Text proposed by the Commission	*Amendment*
	5b The CERTs shall be enabled and encouraged to initiate and to participate in joint exercises with other CERTs, with all Member States-CERTs, and with appropriate institutions of non-Member States as well as with CERTs of multi- and international institutions such as NATO and the UN.

Amendment 75

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

Text proposed by the Commission	*Amendment*
	5c. Member States may ask for the assistance of ENISA or of other Member States in developing their national CERTs.

Amendment 76

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 ***single points of contact*** and the Commission ***and ENISA*** shall form a network (***hereinafter referred to as*** 'cooperation network') to cooperate against risks and incidents affecting network and information systems.

Amendment 77

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 ***single points of contact***. When requested, ENISA shall assist the cooperation network by providing its expertise and advice. ***Where appropriate, market operators and suppliers of cyber security solutions may also be invited to participate in the activities of the cooperation network referred to in points (g) and (i) of paragraph 3.*** ***Where relevant, the cooperation network shall cooperate with the data protection authorities.*** ***The Commission shall regularly inform the cooperation network of security research and other relevant programmes of Horizon2020.***

Amendment 78

Proposal for a directive
Article 8 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Within the cooperation network the ***competent authorities*** shall:	3. Within the cooperation network the ***single points of contact*** shall:
(a) circulate early warnings on risks and incidents in accordance with Article 10;	(a) circulate early warnings on risks and incidents in accordance with Article 10;
(b) ensure a coordinated response in	(b) ensure a coordinated response in

accordance with Article 11;	accordance with Article 11;
(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;
(d) jointly discuss and assess***, at the request of one Member State or of the Commission,*** one or more national NIS strategies and national NIS cooperation plans referred to in Article 5, within the scope of this Directive***.***	(d) jointly discuss and assess one or more national NIS strategies and national NIS cooperation plans referred to in Article 5, within the scope of this Directive***;***
(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 the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level;
(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 ***expertise on*** relevant matters ***on network and information security,*** in particular in the fields of data protection, energy, transport, banking, ***financial markets*** and health ***with the European Cybercrime Centre within Europol, and with other relevant European bodies***;
	(fa) where appropriate, inform the EU Counter-terrorism Coordinator, by means of reporting, and may ask for assistance for analysis, preparatory works and actions of the cooperation network;
(g) exchange information and best practices between themselves and the Commission, and assist each other in building capacity on NIS;	(g) exchange information and best practices between themselves and the Commission, and assist each other in building capacity on NIS;
(h) organise regular peer reviews on capabilities and preparedness;	
(i) organise NIS exercises at Union level and participate, as appropriate, in international NIS exercises.	(i) organise NIS exercises at Union level and participate, as appropriate, in international NIS exercises.
	(ia) involve, consult and exchange, where appropriate, information with market operators with respect to the risks and incidents affecting their network and information systems;
	(ib) develop, in cooperation with ENISA, guidelines for sector-specific criteria for

	the notification of significant incidents, in addition to the parameters laid down in Article 14(2), for a common interpretation, consistent application and harmonious implementation within the Union.

Amendment 79

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

Text proposed by the Commission	*Amendment*
	3a. The cooperation network shall publish a report once a year, based on the activities of the network and on the summary report submitted in accordance with Article 14(4) of this Directive, for the preceding 12 months.

Amendment 80

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 ***consultation*** procedure referred to in Article 19(***2***).	4. The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between ***single points of contact,*** the Commission ***and ENISA*** referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the ***examination*** procedure referred to in Article 19(***3***).

Amendment 81

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

Text proposed by the Commission	*Amendment*
	1a. Participants to the secure infrastructure shall comply with, inter alia, appropriate confidentiality and security measures in accordance with Directive 95/46/EC and Regulation (EC)

No 45/2001 at all steps of the processing.

Amendment 82

Proposal for a directive
Article 9 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 18 concerning the definition of the criteria to be fulfilled for a Member State to be authorized to participate to the secure information-sharing system, regarding:	***deleted***
(a) the availability of a secure and resilient communication and information infrastructure at national level, compatible and interoperable with the secure infrastructure of the cooperation network in compliance with Article 7(3), and	
(b) the existence of adequate technical, financial and human resources and processes for their competent authority and CERT allowing an effective, efficient and secure participation in the secure information-sharing system under Article 6(3), Article 7(2) and Article 7(3).	

Amendment 83

Proposal for a directive
Article 9 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission shall adopt, by means of implementing acts, ***decisions on the access of the Member States to this secure infrastructure, pursuant to the criteria referred to in paragraph 2 and 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).***	3. The Commission shall adopt, by means of ***delegated*** acts, ***a common set of interconnection and security standards that single points of contact are to meet before exchanging sensitive and confidential information across the cooperation network***.

Amendment 84

Proposal for a directive
Article 10 – paragraph 1

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 ***single points of contact*** 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:
(a) they grow rapidly or may grow rapidly in scale;	
(b) ***they exceed or may exceed*** national response capacity;	(b) ***the single point of contact assesses that the risk or incident potentially exceeds*** national response capacity;
(c) ***they affect or may affect*** more than one Member State.	(c) ***the single points of contact or the Commission assess that the risk or incident affects*** more than one Member State.

Amendment 85

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 ***single points of contact*** and the Commission shall communicate ***without undue delay*** any relevant information in their possession that may be useful for assessing the risk or incident.

Amendment 86

Proposal for a directive
Article 10 – paragraph 3

Text proposed by the Commission	*Amendment*
3. At the request of a Member State, or on its own initiative, the Commission may request a Member State to provide any relevant information on a specific risk or incident.	***deleted***

Amendment 87

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 ***and where the concerned market operator has reported incidents of a suspected serious criminal nature as referred to in Article 15(4), the Member States*** shall ***ensure that*** the European Cybercrime Centre within Europol ***is informed, where appropriate***.

Amendment 88

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

Text proposed by the Commission	*Amendment*
	4a. Members of the cooperation network shall not make public any information received on risks and incidents referred to in paragraph 1 without having received the prior approval of the notifying single point of contact.
	Furthermore, prior to sharing information in the cooperation network, the notifying single point of contact shall inform the market operator to which the information relates of its intention, and where it considers this appropriate, it shall make the information concerned anonymous.

Amendment 89

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

Text proposed by the Commission	*Amendment*
	4b. Where the risk or incident subject to an early warning is of a suspected severe cross-border technical nature, the single points of contact or the Commission shall

inform ENISA.

Amendment 90

Proposal for a directive
Article 11 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Following an early warning referred to in Article 10 the ***competent authorities*** shall, after assessing the relevant information, agree on a coordinated response in accordance with the Union NIS cooperation plan referred to in Article 12.	1. Following an early warning referred to in Article 10 the ***single points of contact*** shall, after assessing the relevant information, agree ***without undue delay*** on a coordinated response in accordance with the Union NIS cooperation plan referred to in Article 12.

Amendment 91

Proposal for a directive
Article 12 – paragraph 2 – point a – indent 1

Text proposed by the Commission	*Amendment*
– a definition of the format and procedures for the collection and sharing of compatible and comparable information on risks and incidents by the ***competent authorities***,	– a definition of the format and procedures for the collection and sharing of compatible and comparable information on risks and incidents by the ***single points of contact***,

Amendment 92

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. ***The results of each revision shall be reported to the European Parliament.***

Amendment 93

Proposal for a directive
Article 12 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. Coherence between the Union NIS cooperation plan and national NIS strategies and cooperation plans, as provided for in Article 5 of this Directive, shall be ensured.

Amendment 94

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 ***and shall set out the monitoring procedure that must be followed to guarantee the protection of such personal data. The European Parliament shall be informed about the negotiation of the agreements. Any transfer of personal data to recipients located in countries outside the Union shall be conducted in accordance with Articles 25 and 26 of Directive 95/46/EC and Article 9 of Regulation (EC) No 45/2001.***

Amendment 95

Proposal for a directive
Article 13 a (new)

Text proposed by the Commission	*Amendment*
	Article 13a
	Level of criticality of market operators
	Member States may determine the level of

	criticality of market operators, taking into account the specificities of sectors, parameters including the importance of the particular market operator for maintaining a sufficient level of the sectoral service, the number of parties supplied by the market operator, and the time period until the discontinuity of the core services of the market operator has a negative impact on the maintenance of vital economic and societal activities.

Justification

This amendment is part of Chapter IV and should precede Article 14 thereunder. This articles aims at allowing for a more differentiated classification of Annex II and as a consequence the obligations laid down in Chapter IV. Incident notification shall be done by all market operators regardless of their level of criticality, while the form of security audits may be adapted to the specific level of criticality of the market operator.

Amendment 96

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 ***and proportionate*** 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, ***those*** measures shall ***ensure*** a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting ***the security of*** their network and information ***systems*** on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.

Amendment 97

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 market operators notify ***without undue delay*** to the competent authority ***or to the single point of contact*** incidents having a significant impact on the ***continuity*** of the core services they provide. ***Notification shall not expose the notifying party to increased liability.***
	To determine the significance of the impact of an incident, the following parameters shall inter alia be taken into account:

Amendment 98

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

Text proposed by the Commission	*Amendment*
	(a) the number of users whose core service is affected;

Amendment 99

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

Text proposed by the Commission	*Amendment*
	(b) the duration of the incident;

Amendment 100

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

Text proposed by the Commission	*Amendment*
	(c) geographic spread with regard to the area affected by the incident.

Amendment 101

Proposal for a directive
Article 14 – paragraph 2 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	Those parameters shall be further specified in accordance with point (ib) of Article 8(3).

Amendment 102

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

Text proposed by the Commission	*Amendment*
	2a. Market operators shall notify the incidents referred to in paragraphs 1 and 2 to the competent authority or 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 market operator, alert the other single points of contact concerned. The market operator shall 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 and any other information with relevance to the incident.

Amendment 103

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

Text proposed by the Commission	*Amendment*
	2b. Where the notification contains personal data, it shall be only disclosed to recipients within the notified competent authority or single point of contact who need to process those data for the performance of their tasks in accordance with data protection rules. The disclosed data shall be limited to what is necessary for the performance of their tasks.

Amendment 104

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

Text proposed by the Commission	*Amendment*
	2c. Market operators not covered by Annex II may report incidents as specified in Article 14(2) on a voluntary basis.

Amendment 105

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. ***After consultation with the notified*** competent authority ***and the market operator concerned, the single point of contact*** may inform the public ***about individual incidents, where it determines that public awareness is necessary to prevent an incident or deal with an ongoing incident, or where that*** market ***operator, subject to an incident, has refused to address a serious structural vulnerability related to that incident without undue delay.*** ***Before any public*** disclosure***, the notified competent authority shall ensure that the market operator concerned has the possibility to be heard and that the decision for public disclosure is duly balanced with the public interest***. ***Where information about individual incidents is made public, the notified competent authority or the single point of contact shall ensure that it is made as anonymous as possible.*** ***The competent authority or the single point of contact shall, if reasonably possible, provide the market operator concerned with information that supports the effective handling of the notified incident.***
Once a year, the ***competent authority*** shall	Once a year, the ***single point of contact***

submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.	shall submit a summary report to the cooperation network on the notifications received***, including the number of notifications and regarding the incident parameters as listed in paragraph 2 of this Article,*** and the action taken in accordance with this paragraph.

Amendment 106

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

Text proposed by the Commission	*Amendment*
	4a. Member States shall encourage market operators to make public incidents involving their business in their financial reports on a voluntary basis.

Amendment 107

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***

Amendment 108

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 the single points of contact*** may adopt guidelines concerning the circumstances in which market operators are required to notify incidents.

Amendment 109

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 as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises[35], ***unless the microenterprise acts as subsidiary for a market operator as defined in point (b) of Article 3(8)***.
[35] OJ L 124, 20.5.2003, p. 36.	[35] OJ L 124, 20.5.2003, p. 36.

Amendment 110

Proposal for a directive
Article 14 – paragraph 8 a (new)

Text proposed by the Commission	*Amendment*
	8a. Member States may decide to apply this Article and Article 15 to public administrations mutatis mutandis.

Amendment 111

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 ***and the single points of contact have*** the powers necessary to ***ensure compliance*** of market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems.

Amendment 112

Proposal for a directive
Article 15 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that the competent authorities have the power to require market operators ***and public administrations*** to:	2. Member States shall ensure that the competent authorities ***and the single points of contact*** have the power to require market operators to:

Amendment 113

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) ***provide evidence of effective implementation of security policies, such as the results of*** a security audit carried out by a qualified independent body or national authority**,** and make the ***evidence*** available to the competent authority ***or to the single point of contact***.

Amendment 114

Proposal for a directive
Article 15 – paragraph 2 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	When sending that request, the competent authorities and the single points of contact shall state the purpose of the request and sufficiently specify what information is required.

Amendment 115

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***.	3. Member States shall ensure that ***the*** competent authorities ***and the single points of contact*** have the power to issue binding instructions to market operators.

Amendment 116

Proposal for a directive
Article 15 – paragraphs 3 a and 3 b (new)

Text proposed by the Commission	*Amendment*
	3a. By way of derogation from point (b) of paragraph 2 of this Article, Member States may decide that the competent authorities or the single points of contact, as applicable, are to apply a different procedure to particular market operators, based on their level of criticality determined in accordance with Article 13a. In the event that Member States so decide:
	(a) competent authorities or the single points of contact, as applicable, shall have the power to submit a sufficiently specific request to market operators requiring them to provide evidence of effective implementation of security policies, such as the results of a security audit carried out by a qualified internal auditor, and make the evidence available to the competent authority or to the single point of contact;
	(b) where necessary, following the submission by the market operator of the request referred to in point (a), the competent authority or the single point of contact may require additional evidence or an additional audit to be carried out by a qualified independent body or national authority.
	3b. Member States may decide to reduce the number and intensity of audits for a concerned market operator, where its security audit has indicated compliance with Chapter IV in a consistent manner.

Amendment 117

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 ***and the single points of contact shall inform the market operators concerned about the possibility of reporting incidents of a suspected serious criminal nature to the*** law enforcement authorities.

Amendment 118

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 rules 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. ***The single points of contact and the data protection authorities shall develop, in cooperation with ENISA, information exchange mechanisms and a single template to be used both for notifications under Article 14(2) of this Directive and other Union law on data protection.***

Amendment 119

Proposal for a directive
Article 15 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Member States shall ensure that any obligations imposed on ***public administrations and*** market operators under this Chapter may be subject to judicial review.	6. Member States shall ensure that any obligations imposed on market operators under this Chapter may be subject to judicial review.

Amendment 120

Proposal for a directive
Article 15 – paragraph 6 a (new)

Text proposed by the Commission	*Amendment*
	6a. Member States may decide to apply Article 14 and this Article to public administrations mutatis mutandis.

Amendment 121

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 European or international interoperable*** standards and/or specifications relevant to networks and information security.

Amendment 122

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. The Commission shall ***give a mandate to a relevant European standardisation body to***, ***in consultation with relevant stakeholders,*** draw up a list of the standards ***and/or specifications*** referred to in paragraph 1. The list shall be published in the Official Journal of the European Union.

Amendment 123

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

Text proposed by the Commission	*Amendment*
	1a. Member States shall ensure that the penalties referred to in paragraph 1 of this Article only apply where the market operator has failed to fulfil its obligations under Chapter IV with intent or as a

	result of gross negligence.

Amendment 124

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 ***power*** referred to in ***Article*** 9(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the 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.

Amendment 125

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 ***Article*** 9(2) 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.

Amendment 126

Proposal for a directive
Article 20

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***, in particular the list contained in Annex II,*** 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.

Amendment 127

Proposal for a directive
Annex 1 – heading 1

Text proposed by the Commission	*Amendment*
Requirements and tasks of the Computer Emergency Response ***Team*** (CERT)	Requirements and tasks of the Computer Emergency Response ***Teams (CERTs)***

Amendment 128

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

Text proposed by the Commission	*Amendment*
(a) The ***CERT*** shall ensure high availability of its communications services by avoiding single points of failure and have several means for being contacted and for contacting others. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.	(a) The ***CERTs*** shall ensure high availability of its communications services by avoiding single points of failure and have several means for being contacted and for contacting others ***at all times***. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.

Amendment 129

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	(c) The offices of the ***CERTs*** and the supporting information systems shall be

located in secure sites**.**	located in secure sites ***with secured network information systems.***

Amendment 130

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,	– ***Detecting and*** monitoring incidents at a national level,

Amendment 131

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

Text proposed by the Commission	*Amendment*
	- Actively participating in Union and international CERT cooperation networks

Amendment 132

Proposal for a directive
Annex II – introductory part

Text proposed by the Commission	*Amendment*
List of market operators	List of market operators
Referred to in Article 3(8) a):	
1. e-commerce platforms	
2. Internet payment gateways	
3. Social networks	
4. Search engines	
5. Cloud computing services	
6. Application stores	
Referred to in Article (3(8) b):	

Amendment 133

Proposal for a directive
Annex II – point 1

Text proposed by the Commission	*Amendment*
List of market operators	List of market operators
1. Energy	1. Energy
	(a) Electricity
- Electricity and gas suppliers	**-** Suppliers
- Electricity and/or gas distribution system operators and retailers for final consumers	**-** Distribution system operators and retailers for final consumers
- Natural gas transmission system operators, storage operators and LNG operators	
- Transmission system operators in electricity	- Transmission system operators in electricity
	(b) Oil
- Oil transmission pipelines and oil storage	- Oil transmission pipelines and oil storage
	- Operators of oil production, refining and treatment facilities, storage and transmission
	(c) Gas
- Electricity and gas market operators	***- Suppliers***
	- Distribution system operators and retailers for final consumers
	- Natural gas transmission system operators, storage system operators and LNG system operators
- Operators of ***oil*** and natural gas production, refining ***and*** treatment facilities	- Operators of natural gas production, refining, treatment facilities, ***storage*** facilities ***and transmission***
	- Gas market operators

Amendment 134

Proposal for a Directive
Annex II – point 2

Text proposed by the Commission	*Amendment*
2. Transport	2. Transport
- Air carriers (freight and passenger air transport)	***(a) Road transport***
- Maritime carriers (sea and coastal passenger water transport companies and	***(i) Traffic management control operators***

sea and coastal freight water transport companies)	
- Railways (infrastructure managers, integrated companies and railway transport operators)	***(ii) Auxiliary logistics services:***
- Airports	***- warehousing and storage,***
- Ports	***- cargo handling, and***
- Traffic management control operators	***- other transportation support activities***
- Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities)	***(b) Rail transport***
	(i) Railways (infrastructure managers, integrated companies and railway transport operators)
	(ii) Traffic management control operators
	(iii) Auxiliary logistics services:
	- warehousing and storage,
	- cargo handling, and
	- other transportation support activities
	(c) Air transport
	(i) Air carriers (freight and passenger air transport)
	(ii) Airports
	(iii) Traffic management control operators
	(iv) Auxiliary logistics services:
	- warehousing,
	- cargo handling, and
	- other transportation support activities
	(d) Maritime transport
	(i) Maritime carriers (inland, sea and coastal passenger water transport companies and inland, sea and coastal freight water transport companies)

Amendment 135

Proposal for a directive
Annex II – point 4

Text proposed by the Commission	*Amendment*
4. Financial market infrastructures: ***stock exchanges*** and central counterparty clearing houses	4. Financial market infrastructures: ***regulated markets, multilateral trading facilities, organised trading facilities*** and central counterparty clearing houses

Amendment 136

Proposal for a directive
Annex II – point 5 a (new)

Text proposed by the Commission	*Amendment*
	5a. Water production and supply

Amendment 137

Proposal for a directive
Annex II – point 5 b (new)

Text proposed by the Commission	*Amendment*
	5b. Food supply chain

Amendment 138

Proposal for a directive
Annex II – point 5 c (new)

Text proposed by the Commission	*Amendment*
	5c. Internet exchange points