



EUROPEAN PARLIAMENT

2009 - 2014

Committee on Industry, Research and Energy

2013/0027(COD)

16.10.2013

DRAFT OPINION

of the Committee on Industry, Research and Energy

for the Committee on the Internal Market and Consumer Protection

on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Rapporteur(*): del Pilar del Castillo Vera

(*) Associated committee – Rule 50 of the Rules of Procedure

PA_Legam

SHORT JUSTIFICATION

In February 2013 the European Commission, as requested by the European Parliament in its own initiative report on a Digital Agenda for Europe, presented a proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, together with the first EU cyber-security strategy. Taking into account that analysing the available data it can be estimated that ICT-related incidents of a malicious nature could incur direct costs of more than 560 million Euros per year for SMEs alone, and that all types of incidents (including upstream environmental or physical problems such as natural disasters) could incur direct costs of more than 2.3 billion, the Rapporteur warmly welcomes the proposal.

Regarding its structure, the Rapporteur agrees with a number of the proposed measures, such as the extension of the provisions of reporting security incidents currently limited to telecommunications providers under Article 13a of the 2009 Framework Directive to other critical infrastructure sectors. Accordingly, proposals such as requiring that all Member States must have properly functioning computer emergency response teams and designate a competent authority to be part of a secure pan-European electronic data interchange network to permit the secure sharing and exchange of cyber-security related information, are well received and have the potential to greatly contribute to the objective of the proposed Directive, namely to ensure a high common level of network and information security across the Union.

Your Rapporteur is however of the opinion that there is room for improving the proposal, applying the prism of two main principles: Efficiency and Trust.

First Principle - Efficiency

Regarding the obligations on the Member States to designate a competent authority responsible for monitoring the application of the Directive for all the sectors present in Annex II of the proposal, the Rapporteur is of the opinion that each Member State must not only be free to choose the cyber-security governance model it deems most appropriate, but also that it is imperative to avoid duplication of institutional structures that will potentially lead to conflicts of competence and disruption of communications. Accordingly the Rapporteur is of the opinion that existing national structures that are already efficiently in place and respond to Member State needs and constitutional requirements should not be disrupted. She believes however that in order to guarantee the exchange of information at Union level, the notification of early warning threats and the participation in the Cooperation Network in an efficient manner, each Member State must appoint a **Single Point of Contact**.

In the same spirit of maximizing the efficiency of the proposed Directive the Rapporteur is of the opinion that the proposed measures regarding the establishment of a national **Computer Emergency Response Team (CERT)** might not prove to be the most adequate requirement, given that it disregards the different natures and compositions of existing CERTs. Not only do most Member States have more than one CERT, these also deal with different types of incidents. The quantity and quality of activities also differ depending on whether academic or research institutions, governments or the private sector are hosting and operating them. In

addition the current proposal would disrupt existing international and European cooperation networks, to which existing CERTs already belong, which have proven efficient in coordinating international and European responses to incidents. Consequently, your Rapporteur is of the opinion that instead of referring to a single national CERT, the Directive should be targeted to those CERTs that provide their services to the sectors in Annex II, consequently allowing for example that one CERT provides services to all Annex II sectors or that several CERTs provide services to the same sector. The Rapporteur is however of the opinion that Member States must guarantee full operability at all times of their CERTs and guarantee they have sufficient technical, financial and human resources to properly operate and participate in international and union cooperation networks.

The efficiency principle furthermore requires changes to the proposed Directive regarding **the scope**. While the Rapporteur agrees that an extension of the reporting system obligations to the energy, transport, health and financial sectors is needed, the proposal to extend the compulsory measures laid down in Chapter IV to all market operators in the “Internet economy” is disproportionate and unmanageable. Disproportionate because the indiscriminate imposition of new obligations to an open and non-defined category such as every “provider of information society services which enable the provision of other information society services” is not only incomprehensible but also not duly justified with regards to possible damage produced by a security incident, and carries with it the potential to add another layer of bureaucracy to our industrial sector and more particularly to SMEs. Unmanageable, because serious doubts arise to whether competent authorities would be able to cope with all potential notifications in a proactive manner that would encourage a bidirectional dialogue with market operators in order to resolve the security threat.

Regarding **public administrations**, the Directive should balance the need for further development of eGovernment services with the already existing due diligence obligations on public administrations regarding the management and protection of their networks and information systems. Consequently, the Rapporteur is of the opinion that while the exchange of information requirements established in Article 14 should fully apply to public administrations, they should not be subject to the obligations of Article 15.

Second Principle - Trust

The Rapporteur’s view is that a great part of the success of the Directive lies in its ability to incentivise participation of market operators, leading to the creation of a trustworthy NIS environment where those that are on the ground are willing to proactively participate. If it does not achieve this, it will fail. In this regard the Rapporteur proposes to guarantee that participation and notification of market operators is not negatively impacted by unnecessary publications of security incidents they have notified, or that they can be held liable for information loss by competent authorities or single points of contact. In addition a bidirectional dialog must be open between operators and competent authorities and participation of the market operators must be encouraged in all fora, including the cooperation network.

The Rapporteur also believes that trust should be the pillar of the participation of the competent authorities and/or the single points of contact, especially regarding the exchange of

information. In order to guarantee this provisions regarding confidentiality and security requirements of the network should be reflected in the Directive.

AMENDMENTS

The Committee on Industry, Research and Energy calls on the Committee on the Internal Market and Consumer Protection, as the committee responsible, to incorporate the following amendments in its report:

Amendment 1

Proposal for a directive

Recital 4

Text proposed by the Commission

(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.

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 information infrastructure to promote a culture of risk management and ensure that the most serious incidents are reported.

Or. en

Amendment 2

Proposal for a directive

Recital 4 a (new)

Text proposed by the Commission

Amendment

(4 a) This Directive should take into account the need for further development of eGovernment services by establishing

certain due diligence obligations on public administrations regarding the management and protection of their networks and information systems, while otherwise focusing on critical infrastructure essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, financial market infrastructures and health.

Or. en

Amendment 3

Proposal for a directive Recital 6

Text proposed by the Commission

(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.

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, *damaging in addition the effectiveness of international cooperation and consequently the fight against global security challenges.*

Or. en

Amendment 4

Proposal for a directive Recital 10 a (new)

(10 a) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements 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 that each Member State 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.

Or. en

Amendment 5

Proposal for a directive Recital 11

Text proposed by the Commission

(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

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 ***at any moment***. 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.

incidents and risks and ensure efficient cooperation at Union level. ***In view of the different characteristics of existing Computer Emergency Response Teams (CERT), which responds to different subject needs and actors, Member States should guarantee that each of the sectors covered by Annex II is provided services by at least one CERT. Regarding cross border CERT cooperation, Member States should assure that CERTs have sufficient means to participate in the existing international and European cooperation networks already in place.***

Or. en

Amendment 6

Proposal for a directive Recital 12

Text proposed by the Commission

(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.

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, ***where the participation of market operators is assured***, should enable structured and coordinated information exchange, detection and response at Union level.

Or. en

Amendment 7

Proposal for a directive Recital 14

Text proposed by the Commission

(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.

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. ***In order for the cooperation network to be able to efficiently fulfil its mission, the Commission should establish a budget line for the network.***

Or. en

Amendment 8

Proposal for a directive Recital 14 a (new)

Text proposed by the Commission

Amendment

(14 a) Where appropriate, market operators may also be invited to participate in the activities of the cooperation network. In order to achieve greater efficiency convergence opportunities with the CIWIN Network must be evaluated.

Or. en

Amendment 9

Proposal for a directive Recital 15

Text proposed by the Commission

(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.

Amendment

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

Or. en

Amendment 10

Proposal for a directive Recital 16

Text proposed by the Commission

(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.

Amendment

(16) To ensure transparency and properly inform EU 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 and risks.

Or. en

Amendment 11

Proposal for a directive Recital 19

Text proposed by the Commission

(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.

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 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.

Or. en

Amendment 12

Proposal for a directive Recital 20

Text proposed by the Commission

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

Amendment

(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. **The single points of contact** as well as the Commission should be informed about the measures adopted at national level as a result of the coordinated response.

Or. en

Amendment 13

Proposal for a directive Recital 22

Text proposed by the Commission

(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.

Amendment

(22) Responsibilities in ensuring NIS lie to a great extent on public administrations and market operators. A culture of risk management **and trust**, 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 **trustworthy** level playing field is also essential to the effective functioning of the cooperation network to ensure effective cooperation from all Member States.

Or. en

Amendment 14

Proposal for a directive
Recital 24

Text proposed by the Commission

(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.***

Amendment

(24) Those obligations should be extended beyond the electronic communications sector ***and public administrations to operators of 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, 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 do 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

Software developers and hardware manufacturers are not providers of information society services and are therefore excluded. Those obligations should also be extended to public administrations, and operators of critical infrastructure which rely heavily on information and communications technology and are essential to the maintenance of vital economical or societal functions such as electricity and gas, transport, credit institutions, stock exchange and health. Disruption of those network and information systems would affect the internal market.

²⁷ OJ L 204, 21.7.1998, p. 37.

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, these *may, on a voluntary basis, inform the competent authority or single point of contact of those network security incidents they deem appropriate, and the competent authority or the single point of contact should, if reasonably possible, present the public administrations or the market operators that informed of the incident with strategically analysed information that will help overcome the security threat.*

²⁷ OJ L 204, 21.7.1998, p. 37.

Or. en

Amendment 15

Proposal for a directive Recital 28

Text proposed by the Commission

(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

Amendment

(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. 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 public administrations and market operators reporting incidents. In *order to safeguard trust and efficiency, publicity of*

to the need to maintain information about product vulnerabilities strictly confidential prior to the *release* of appropriate security fixes.

incidents shall only take place after consultation with those who reported the incident and only when strictly necessary for achieving the objectives of this Directive. 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 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.

Or. en

Amendment 16

Proposal for a directive Recital 29

Text proposed by the Commission

(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.

Amendment

(29) Competent authorities **and single points of contact** 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.

Or. en

Amendment 17

Proposal for a directive Recital 30

Text proposed by the Commission

(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.

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, ***single points of contact*** and law enforcement authorities should form part of an effective and comprehensive response to the threat of security incidents. In particular, promoting a safe, secure and more resilient environment requires a systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities. The serious criminal nature of incidents should be assessed in the light of EU laws on cybercrime.

Or. en

Amendment 18

Proposal for a directive Recital 31

Text proposed by the Commission

(31) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle the personal data breaches resulting from incidents. ***Member states shall implement*** the obligation to notify security incidents in a way that minimises the administrative burden in case the security incident is also a personal data

Amendment

(31) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities, ***single points of contact*** and data protection authorities should cooperate and exchange information on all relevant matters to tackle the personal data breaches resulting from incidents. 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

breach *in line with the Regulation* of the European Parliament and of the Council *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*²⁸. *Liaising with the competent authorities and the data protection authorities*, ENISA *could* assist by developing information exchange mechanisms and *templates avoiding the need for two notification templates*. This single notification template would facilitate the reporting of incidents compromising personal data thereby easing the administrative burden on businesses and public administrations.

²⁸ SEC(2012) 72 final

a personal data breach *that is required to be notified in accordance with applicable 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.

Or. en

Amendment 19

Proposal for a directive Recital 32

Text proposed by the Commission

(32) Standardisation of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards to ensure a high level of security at Union level. To this end, it might be necessary to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and

Amendment

(32) Standardisation of security requirements is a market-driven process *of a voluntary nature that should allow market operators and public administrations 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, 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

2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council²⁹ .

Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council²⁹ .

²⁹ OJ L 316, 14.11.2012, p. 12.

²⁹ OJ L 316, 14.11.2012, p. 12.

Or. en

Amendment 20

Proposal for a directive Recital 34

Text proposed by the Commission

(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.*

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 further specification of the triggering events for early warning.

Or. en

Amendment 21

Proposal for a directive Recital 35

Text proposed by the Commission

(35) It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

Amendment

(35) It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including ***all stakeholders and in particular*** at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

Or. en

Amendment 22

**Proposal for a directive
Recital 36**

Text proposed by the Commission

(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 powers³⁰.

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 ***single points of contact*** and the Commission within the cooperation network, ***without prejudice to existing cooperation mechanisms at national level, the common set of interconnection and security standards*** for the secure information-sharing infrastructure, the Union NIS cooperation plan ***and*** the formats and procedures applicable to ***notifying significant*** incidents. 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 powers³⁰.

³⁰ OJ L 55, 28.2.2011, p.13.

³⁰ OJ L 55, 28.2.2011, p.13.

Or. en

Amendment 23

Proposal for a directive Recital 38

Text proposed by the Commission

(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.

Amendment

(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 and other **single points of contact** 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.

Or. en

Amendment 24

Proposal for a directive Recital 39

Text proposed by the Commission

(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

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 **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

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 documents³¹ 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.

³¹ OJ L 145, 31.5.2001, p. 43.

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 documents³¹ 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.

³¹ OJ L 145, 31.5.2001, p. 43.

Or. en

Amendment 25

Proposal for a directive Recital 41 a (new)

Text proposed by the Commission

Amendment

(41 a) 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.

Or. en

Amendment 26

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

Text proposed by the Commission

(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;

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 *with the participation of relevant stakeholders*;

Or. en

Amendment 27

Proposal for a directive Article 1 – paragraph 6

Text proposed by the Commission

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

Amendment

6. The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require the processing of personal data. *Market operators and public administrations should not be held liable for* such processing, which is necessary to meet the objectives of public interest pursued by this Directive, shall be authorised by the Member State pursuant to Article 7 of Directive 95/46/EC and

Directive 2002/58/EC, as implemented in national law.

Or. en

Amendment 28

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

Text proposed by the Commission

(4) ‘incident’ means any circumstance or event having an actual adverse effect on security;

Amendment

(4) ‘incident’ means any ***reasonably identifiable*** circumstance or event having an actual adverse effect on security;

Or. en

Amendment 29

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

Text proposed by the Commission

(5) ‘***information society service***’ mean ***service within the meaning of point (2) of Article 1 of Directive 98/34/EC***;

Amendment

deleted

Or. en

Amendment 30

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

Text proposed by the Commission

(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***

Amendment

deleted

Amendment 31

Proposal for a directive

Article 3 – paragraph 1 – point 8 – point b

Text proposed by the Commission

(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.

Amendment

(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** and health, **and the disruption or destruction of which would have a significant negative 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.

Amendment 32

Proposal for a directive

Article 3 – paragraph 1 – point 11 a (new)

Text proposed by the Commission

Amendment

(11 a) '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^{28a};

^{28a} **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).**

Amendment 33

Proposal for a directive

Article 3 – paragraph 1 – point 11 b (new)

Text proposed by the Commission

Amendment

(11 b) 'multilateral trading facility (MTF)' means multilateral trading facility as defined in point 15 of Article 4 of Directive 2004/39/EC;

Or. en

Amendment 34

Proposal for a directive

Article 3 – paragraph 1 – point 11 c (new)

Text proposed by the Commission

Amendment

(11 c) '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 a way that results in a contract in accordance with the provisions of Title II of Directive 2004/39/EC;

Or. en

Amendment 35

Proposal for a directive

Article 5 – paragraph 2 – point a

Text proposed by the Commission

(a) A risk **assessment plan to identify risks and assess** the impacts of potential incidents;

Amendment

(a) A risk **management framework including the identification, prioritisation, evaluation and treatment of risks, the assessment of** the impacts of potential incidents, **prevention and control options, and criteria for the choice of possible countermeasures;**

Or. en

Amendment 36

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

Text proposed by the Commission

(b) The definition of the roles and responsibilities of the various actors involved in the implementation of the **plan**;

Amendment

(b) The definition of the roles and responsibilities of the various **authorities and other** actors involved in the implementation of the **framework**;

Or. en

Amendment 37

**Proposal for a directive
Article 6 – title**

Text proposed by the Commission

National competent **authority** on the security of network and information systems

Amendment

National competent **authorities and single points of contact** on the security of network and information systems

Or. en

Amendment 38

Proposal for a directive Article 6 – paragraph 1

Text proposed by the Commission

1. Each Member State shall designate **a** national competent **authority** on the security of network and information systems (**the** ‘competent authority’).

Amendment

1. Each Member State shall designate **one or more** national competent **authorities** on the security of network and information systems (**hereinafter referred to as the** ‘competent authority’).

Or. en

Amendment 39

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

Text proposed by the Commission

Amendment

2 a. Where a Member State designates more than one competent authority, it shall designate a 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.

Or. en

Amendment 40

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

Text proposed by the Commission

Amendment

2 b. 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.

Or. en

Amendment 41

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

Text proposed by the Commission

Amendment

2 c. The single point of contact shall ensure cross-border cooperation with other single points of contact.

Or. en

Amendment 42

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.

Or. en

Amendment 43

Proposal for a directive Article 6 – paragraph 4

Text proposed by the Commission

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.

Amendment

4. Member States shall ensure that the competent authorities **and single points of contact** 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.

Or. en

Amendment 44

Proposal for a directive Article 6 – paragraph 5

Text proposed by the Commission

5. The competent authorities shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities and data protection authorities.

Amendment

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.

Or. en

Amendment 45

Proposal for a directive Article 6 – paragraph 6

Text proposed by the Commission

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

Amendment

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

designation of the competent *authority*.

State shall make public its designation of the competent *authorities*.

Or. en

Amendment 46

Proposal for a directive Article 7 – paragraph 1

Text proposed by the Commission

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.

Amendment

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.

Or. en

Amendment 47

Proposal for a directive Article 7 – paragraph 5

Text proposed by the Commission

5. The *CERT* shall act under the supervision of the competent authority, which shall regularly review the adequacy of its resources, its mandate and the effectiveness of its incident-handling process.

Amendment

5. The *CERTs* shall act under the supervision of the competent authority *or the single point of contact*, which shall regularly review the adequacy of its resources, its mandate and the effectiveness of its incident-handling process.

Or. en

Amendment 48

Proposal for a directive

Article 7 – paragraph 5 a (new)

Text proposed by the Commission

Amendment

5 a. Member States shall ensure that CERTs have adequate human and financial resources to actively participate in international, and in particular Union, cooperation networks

Or. en

Amendment 49

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 shall form a network ('cooperation network') ***where they shall*** cooperate against risks and incidents affecting network and information systems.

Or. en

Amendment 50

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, the European Network and Information Security Agency ('ENISA') shall assist the cooperation network by providing its expertise and advice. ***Where appropriate, market operators may also be***

invited to participate in the activities of the cooperation network referred to in points (c), (g), (h) and (i) of paragraph 3. In order to achieve greater efficiency convergence opportunities with the CIWIN Network must be evaluated.

Or. en

Amendment 51

Proposal for a directive

Article 8 – paragraph 3 – introductory part

Text proposed by the Commission

3. Within the cooperation network the *competent authorities* shall:

Amendment

3. Within the cooperation network the *single points of contact* shall:

Or. en

Amendment 52

Proposal for a directive

Article 8 – paragraph 3 – point e

Text proposed by the Commission

(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;

Amendment

(e) jointly discuss and assess, at the request of *ENISA*, a Member State or the Commission, the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level;

Or. en

Amendment 53

Proposal for a directive

Article 8 – paragraph 3 – point f

Text proposed by the Commission

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

Amendment

(f) cooperate and exchange information on all relevant matters *on network and information security* with the European Cybercrime Center within Europol, and with other relevant European bodies in particular in the fields of data protection, energy, transport, banking, *financial market infrastructures* and health;

Or. en

Amendment 54

Proposal for a directive

Article 8 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3 a. The cooperation network shall yearly publish a report, 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. Publicity of any individual 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 public administrations and market operators that reported them and can only take place after prior consultation.

Or. en

Amendment 55

Proposal for a directive

Article 8 – paragraph 3 – point i a (new)

Text proposed by the Commission

Amendment

(i a) actively promote involvement and consult and exchange information with market operators.

Or. en

Amendment 56

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*** 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).

Or. en

Amendment 57

Proposal for a directive Article 9 – paragraph 2 – introductory part

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:

2. The Commission shall be empowered to adopt ***implementing*** acts in accordance with Article ***19*** concerning the definition of the criteria to be fulfilled for a ***single point of contact*** to be authorized to participate to the secure information-sharing system, regarding:

Or. en

Amendment 58

Proposal for a directive Article 9 – paragraph 3

Text proposed by the Commission

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).

Amendment

3. The Commission shall adopt, by means of implementing acts, *a common set of interconnections and security standards that single points of contact must meet in order to exchange information*. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).

Or. en

Amendment 59

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

Text proposed by the Commission

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:

Amendment

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:

Or. en

Amendment 60

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

Text proposed by the Commission

(a) they grow rapidly or may grow rapidly in scale;

Amendment

deleted

Amendment 61

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

Text proposed by the Commission

(b) *they exceed or may exceed* national response capacity;

Amendment

(b) *the single point of contact assesses that the risk or incident potentially exceeds* national response capacity *and they grow rapidly or may grow rapidly in scale*

Or. en

Amendment 62

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

Text proposed by the Commission

(c) *they affect or may affect* more than one Member State.

Amendment

(c) *the single points of contact or the Commission assess that the risk or incident affects* more than one Member State *and they grow rapidly or may grow rapidly in scale*.

Or. en

Amendment 63

Proposal for a directive Article 10 – paragraph 2

Text proposed by the Commission

2. In the early warnings, the *competent authorities* and the Commission shall communicate any relevant information in their possession that may be useful for

Amendment

2. In the early warnings, the *single points of contact* and the Commission shall communicate *without undue delay* any relevant *non-classified* information in their

assessing the risk or incident.

possession that may be useful for assessing the risk or incident.

Or. en

Amendment 64

Proposal for a directive Article 10 – paragraph 3

Text proposed by the Commission

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.

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 ***non-classified*** information on a specific risk or incident.

Or. en

Amendment 65

Proposal for a directive Article 10 – paragraph 4

Text proposed by the Commission

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.

Amendment

4. Where the risk or incident subject to an early warning is of a suspected criminal nature, the ***single points of contact*** or the Commission shall inform the European Cybercrime Centre within Europol.

Or. en

Amendment 66

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

Text proposed by the Commission

Amendment

4 a. Members of the cooperation network shall not make public any information received on risks and incidents according to paragraph 1 without having received the prior approval of the notifying single point of contact.

Or. en

Amendment 67

Proposal for a directive Article 10 – paragraph 5

Text proposed by the Commission

Amendment

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

5. The Commission shall be empowered to adopt **implementing** acts in accordance with Article 19, concerning the further specification of the risks and incidents triggering early warning referred to in paragraph 1, **as well as the procedures for sharing sensitive information for market operators, national security or national defense referred to in paragraph 2.**

Or. en

Amendment 68

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.

Or. en

Amendment 69

Proposal for a directive

Article 12 – paragraph 2 – point a – indent 1

Text proposed by the Commission

– 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*,

Amendment

– 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*,

Or. en

Amendment 70

Proposal for a directive

Article 12 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3 a. The Commission shall provide a budget for the development of the Union NIS cooperation plan.

Or. en

Amendment 71

Proposal for a directive

Article 13 – paragraph 1

Text proposed by the Commission

Without prejudice to the possibility for the cooperation network to have informal international cooperation, the Union may

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.

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.

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.

Or. en

Amendment 72

Proposal for a directive Article 14 – paragraph 1

Text proposed by the Commission

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.

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, ***accordingly the Commission shall ensure that the European Institutions also undertake the appropriate technical and organisational measures.*** Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.

Or. en

Amendment 73

Proposal for a directive Article 14 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. Member States shall ensure that public administrations and market operators notify 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, **accordingly the Commission shall ensure the same obligations vis a vis the European Institutions. To determine the significance of the impact of an incident, the following parameters shall inter alia be taken into account:**

Or. en

Amendment 74

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

Text proposed by the Commission

Amendment

These criteria shall be further specified according to Article 8 paragraph 3 point i b (new).

Or. en

Amendment 75

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;

Or. en

Amendment 76

Proposal for a directive

Article 14 – paragraph 2 – point b (new)

Text proposed by the Commission

Amendment

(b) the duration of the incident;

Or. en

Amendment 77

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.

Or. en

Amendment 78

Proposal for a directive

Article 14 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3 a. Market operators and public administrations 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.

Or. en

Amendment 79

Proposal for a directive Article 14 – paragraph 4

Text proposed by the Commission

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.

Amendment

4. *After consultation with* the competent authority *and the public administration and market operator concerned, the single point of contact may exceptionally* inform the public *about individual incidents, where public awareness is necessary to prevent an incident or deal with an ongoing incident, or where the market operator, subject to an incident, has refused to address a serious structural vulnerability related to that incident without undue delay. The single point of contact must properly justify such decision. The competent authority or the single point of contact shall, if reasonably possible, present* the public *administrations or the market operators that informed of the incident with strategic analysed information that will help overcome the security threat.* Once a year, the *single point of contact* shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph. *Publicity of any individual 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 public administrations and market operators that reported them and can only take place after prior consultation.

Or. en

Amendment 80

Proposal for a directive Article 14 – paragraph 5

Text proposed by the Commission

Amendment

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

deleted

Or. en

Amendment 81

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.

Or. en

Amendment 82

Proposal for a directive Article 15 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. Member States shall ensure that the competent authorities **and the single points of contact have** the powers necessary to **examine** 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.

Or. en

Amendment 83

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

Text proposed by the Commission

2. Member States shall ensure that the competent authorities have the power to require market operators **and public administrations** to:

Amendment

2. Member States shall ensure that the competent authorities **and the single points of contact** have the power to require market operators to:

Or. en

Amendment 84

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

Text proposed by the Commission

(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.

Amendment

(b) **provide evidence of effective implementation of security policies, such as results of** a security audit carried out by **internal auditors**, a qualified independent body or national authority, and make the **evidence** available to the competent

authority *or to the single point of contact*. *Where necessary, the competent authority or the single point of contact may require additional evidence or exceptionally, and providing due justification, carry out an additional audit. This requirement shall only apply to all market operators laid down in Annex II, where not provided otherwise according to Article 15 paragraph 2 point b a (new).*

Or. en

Amendment 85

Proposal for a directive

Article 15 – paragraph 2 – subparagraph 1 (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.

Or. en

Amendment 86

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 *all* market operators *laid down in Annex II*.

Or. en

Amendment 87

Proposal for a directive Article 15 – paragraph 4

Text proposed by the Commission

4. The competent authorities ***shall notify incidents of a suspected serious criminal nature to*** law enforcement authorities.

Amendment

4. The competent authorities ***and the single point of contact shall inform the concerned market operators about the possibility to bring criminal charges to the*** law enforcement authorities ***in case of incidents of a suspected serious criminal nature.***

Or. en

Amendment 88

Proposal for a directive Article 15 – paragraph 5

Text proposed by the Commission

5. The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.

Amendment

5. 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 Regulation 95/46 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.***

Or. en

Amendment 89

Proposal for a directive Article 16 – paragraph 1

Text proposed by the Commission

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.

Amendment

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

Or. en

Amendment 90

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

Text proposed by the Commission

Amendment

1 a. 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.

Or. en

Amendment 91

Proposal for a directive Article 18 – paragraph 2

Text proposed by the Commission

Amendment

2. The power to adopt delegated acts referred to in Articles 9(2), 10(5) and 14(5) shall be conferred on the Commission. The Commission shall draw up a report in respect of the delegation of

deleted

power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

Or. en

Amendment 92

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.

deleted

Or. en

Amendment 93

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

deleted

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

Or. en

Amendment 94

Proposal for a directive Annex 1 – heading 1

Text proposed by the Commission

Requirements and tasks of the Computer Emergency Response *Team* (CERT)

Amendment

Requirements and tasks of the Computer Emergency Response *Teams* (CERT)

Or. en

Amendment 95

Proposal for a directive Annex 1 – paragraph 1 – introductory part

Text proposed by the Commission

The requirements and tasks of the *CERT* shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following elements:

Amendment

The requirements and tasks of the *CERTs* shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following elements:

(This amendment applies throughout the text of annex 1)

Or. en

Amendment 96

Proposal for a directive

Annex 1 – paragraph 1 – point 1 – point a

Text proposed by the Commission

(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.

Amendment

(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.

Or. en

Amendment 97

Proposal for a directive

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

Text proposed by the Commission

Amendment

- Actively participate in Union and International CERT cooperation networks

Or. en

Amendment 98

Proposal for a directive

Annex 2 – paragraph 1 – introductory part

Text proposed by the Commission

Amendment

Referred to in Article 3(8) a): Referred to in Article (3(8) b):

deleted

Or. en

Amendment 99

Proposal for a directive

Annex 2 – paragraph 1 – point 1

Text proposed by the Commission

Amendment

1. e-commerce platforms

deleted

Or. en

Amendment 100

Proposal for a directive

Annex 2 – paragraph 1 – point 2

Text proposed by the Commission

Amendment

2. Internet payment gateways

deleted

Or. en

Amendment 101

Proposal for a directive

Annex 2 – paragraph 1 – point 3

Text proposed by the Commission

Amendment

3. Social networks

deleted

Or. en

Amendment 102

Proposal for a directive

Annex 2 – paragraph 1 – point 4

Text proposed by the Commission

Amendment

4. Search engines

deleted

Amendment 103

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

Text proposed by the Commission

Amendment

5. Cloud computing services *deleted*

Or. en

Amendment 104

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

Text proposed by the Commission

Amendment

6. Application stores *deleted*

Or. en

Amendment 105

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

Text proposed by the Commission

Amendment

– Electricity and gas suppliers *deleted*

Or. en

Amendment 106

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

Text proposed by the Commission

Amendment

– Electricity and/or gas distribution system operators and retailers for final consumers

deleted

Or. en

Amendment 107

Proposal for a directive

Annex 2 – paragraph 1 – point 1 – indent 3

Text proposed by the Commission

Amendment

– Natural gas transmission system operators, storage operators and LNG operators

deleted

Or. en

Amendment 108

Proposal for a directive

Annex 2 – paragraph 1 – point 1 – indent 4

Text proposed by the Commission

Amendment

– Transmission system operators in electricity

deleted

Or. en

Amendment 109

Proposal for a directive

Annex 2 – paragraph 1 – point 1 – indent 5

Text proposed by the Commission

Amendment

– Oil transmission pipelines and oil

deleted

storage

Or. en

Amendment 110

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

Text proposed by the Commission

Amendment

– Electricity and gas market operators *deleted*

Or. en

Amendment 111

Proposal for a directive Annex 2 – paragraph 1 – point 1 – indent 7

Text proposed by the Commission

Amendment

**– Operators of oil and natural gas
production, refining and treatment
facilities** *deleted*

Or. en

Amendment 112

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

Text proposed by the Commission

Amendment

(a) Electricity
- Suppliers
**- Distribution system operators and
retailers for final consumers**
**- Transmission system operators in
electricity**

- Electricity market operators

Or. en

Amendment 113

Proposal for a directive

Annex 2 – paragraph 1 – point 1 – point b (new)

Text proposed by the Commission

Amendment

(b) Oil

- Oil transmission pipelines and oil storage

- Operators of oil production, refining and treatment facilities, storage and transmission

Or. en

Amendment 114

Proposal for a directive

Annex 2 – paragraph 1 – point 1 – point c (new)

Text proposed by the Commission

Amendment

(c) Gas

- Suppliers

- Distribution system operators and retailers for final consumers

- Natural gas transmission system operators, storage system operators and LNG system operators

- Operators of natural gas production, refining, treatment facilities, storage facilities and transmission

- Gas market operators

Or. en

Amendment 115

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

Text proposed by the Commission

Amendment

– Air carriers (freight and passenger air transport) *deleted*

Or. en

Amendment 116

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

Text proposed by the Commission

Amendment

– Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies) *deleted*

Or. en

Amendment 117

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

Text proposed by the Commission

Amendment

– Railways (infrastructure managers, integrated companies and railway transport operators) *deleted*

Or. en

Amendment 118

Proposal for a directive

Annex 2 – paragraph 1 – point 2 – indent 4

Text proposed by the Commission

Amendment

– Airports

deleted

Or. en

Amendment 119

Proposal for a directive

Annex 2 – paragraph 1 – point 2 – indent 5

Text proposed by the Commission

Amendment

– Ports

deleted

Or. en

Amendment 120

Proposal for a directive

Annex 2 – paragraph 1 – point 2 – indent 6

Text proposed by the Commission

Amendment

– Traffic management control operators

deleted

Or. en

Amendment 121

Proposal for a directive

Annex 2 – paragraph 1 – point 2 – indent 7

Text proposed by the Commission

Amendment

– Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation

deleted

support activities)

Or. en

Amendment 122

Proposal for a directive

Annex 2 – paragraph 1 – point 2 – point a (new)

Text proposed by the Commission

Amendment

(a) Road transport

(i) Traffic management control operators

(ii) Auxiliary logistics services:

- warehousing and storage,

- cargo handling, and

- other transportation support activities

Or. en

Amendment 123

Proposal for a directive

Annex 2 – paragraph 1 – point 2 – point b (new)

Text proposed by the Commission

Amendment

(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

Or. en

Amendment 124

Proposal for a directive

Annex 2 – paragraph 1 – point 2 – point c (new)

Text proposed by the Commission

Amendment

(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

Or. en

Amendment 125

Proposal for a directive

Annex 2 – paragraph 1 – point 2 – point d (new)

Text proposed by the Commission

Amendment

(d) Maritime transport

(i) Maritime carriers (inland, sea and coastal passenger water transport companies and inland, sea and coastal freight water transport companies)

(ii) Ports

(iii) Traffic management control operators

(iv) Auxiliary logistics services:

- warehousing and storage,

- cargo handling, and

- other transportation support activities

Or. en

Amendment 126

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

Text proposed by the Commission

Amendment

2 a. Water services

Or. en

Amendment 127

Proposal for a directive
Annex 2 – paragraph 1 – 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

Or. en