Procedure file

Basic information

COD - Ordinary legislative procedure (ex-codecision procedure) Directive	2013/0027(COD)	Procedure completed
High common level of network and information security across the Union. NIS Directive Repealed by 2020/0359(COD) Subject 2.80 Cooperation between administrations 3.30.06 Information and communication technologies, digital technologies 3.30.07 Cybersecurity, cyberspace policy 3.30.25 International information networks and society, internet 7.30.09 Public security		

Key players

European Parliament	Committee responsible	Rapporteur	Appointed
	IMCO Internal Market and Consumer Protection		20/03/2013
		PPE SCHWAB Andreas	
		Shadow rapporteur	
		S&D DANTI Nicola	
		ECR FORD Vicky	
		GUOGA Antanas	
		ALBRECHT Jan Philipp	
	Former committee responsible		
	IMCO Internal Market and Consumer Protection		20/03/2013
		PPE SCHWAB Andreas	
	Former committee for opinion		
	ITRE Industry, Research and Energy (Associated committee)		23/05/2013
		PPE DEL CASTILLO VERA Pilar	
	LIBE Civil Liberties, Justice and Home Affairs (Associated committee)		07/03/2013
		Verts/ALE SCHLYTER Carl	
	AFET Foreign Affairs		19/02/2013
		S&D GOMES Ana	
	INTA International Trade	The committee decided not to give an opinion.	
	BUDG Budgets	The committee decided not to give an opinion.	

	ECON Economic and Monetary Affairs	The committee decided not to give an opinion.	
	ENVI Environment, Public Health and Food Safety	The committee decided not to give an opinion.	
	TRAN Transport and Tourism	The committee decided not to give an opinion.	
	JURI Legal Affairs	The committee decided not to give an opinion.	
Council of the European Union	Council configuration	Meeting	Date
	Competitiveness (Internal Market, Industry, Research and Space)	3451	29/02/2016
	Transport, Telecommunications and Energy	3318	05/06/2014
	Transport, Telecommunications and Energy	3278	05/12/2013
	Transport, Telecommunications and Energy	3243	06/06/2013
European Commission	Commission DG	Commissioner	
	Communications Networks, Content and Technology	KROES Neelie	
European Economic and Social Committee			

Key events

07/02/2013	Legislative proposal published	COM(2013)0048	Summary
15/04/2013	Committee referral announced in Parliament, 1st reading		
06/06/2013	Debate in Council	3243	Summary
12/09/2013	Referral to associated committees announced in Parliament		
05/12/2013	Debate in Council	3278	Summary
23/01/2014	Vote in committee, 1st reading		
12/02/2014	Committee report tabled for plenary, 1st reading	A7-0103/2014	Summary
12/03/2014	Debate in Parliament		
13/03/2014	Results of vote in Parliament		
13/03/2014	Decision by Parliament, 1st reading	T7-0244/2014	Summary
05/06/2014	Debate in Council	3318	
06/10/2014	Committee decision to open interinstitutional negotiations after 1st reading in Parliament		
14/01/2016	Approval in committee of the text agreed at 2nd reading interinstitutional negotiations	PE612.044 PE612.045	
17/05/2016	Council position published	05581/1/2016	Summary
09/06/2016	Committee referral announced in Parliament, 2nd reading		

14/06/2016	Vote in committee, 2nd reading		
17/06/2016	Committee recommendation tabled for plenary, 2nd reading	A8-0211/2016	Summary
05/07/2016	Debate in Parliament		
06/07/2016	Decision by Parliament, 2nd reading	T8-0303/2016	Summary
06/07/2016	Final act signed		
06/07/2016	End of procedure in Parliament		
19/07/2016	Final act published in Official Journal		

Technical information

Procedure reference	2013/0027(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Directive
	Repealed by 2020/0359(COD)
Legal basis	Treaty on the Functioning of the EU TFEU 114-p1
Other legal basis	Rules of Procedure EP 165
Mandatory consultation of other institutions	European Economic and Social Committee
Stage reached in procedure	Procedure completed
Committee dossier	IMCO/8/05266

Documentation gateway

Legislative proposal		COM(2013)0048	07/02/2013	EC	Summary
Document attached to the procedure		SWD(2013)0031	07/02/2013	EC	
Document attached to the procedure		SWD(2013)0032	07/02/2013	EC	
Economic and Social Committee: opinion, report		CES1414/2013	22/05/2013	ESC	
Document attached to the procedure		N7-0072/2014 OJ C 032 04.02.2014, p. 0019	14/06/2013	EDPS	Summary
Committee draft report		PE514.882	10/07/2013	EP	
Amendments tabled in committee		PE519.685	02/10/2013	EP	
Committee opinion	AFET	PE516.830	05/12/2013	EP	
Committee opinion	ITRE	PE519.596	19/12/2013	EP	
Committee opinion	LIBE	PE514.755	15/01/2014	EP	
Committee report tabled for plenary, 1st reading/single reading		A7-0103/2014	12/02/2014	EP	Summary
Text adopted by Parliament, 1st reading/single reading		T7-0244/2014	13/03/2014	EP	Summary
Commission response to text adopted in		SP(2014)455	10/06/2014	EC	

plenary					
European Central Bank: opinion, guideline, report		CON/2014/0058 OJ C 352 07.10.2014, p. 0004	25/07/2014	ECB	Summary
Council statement on its position		08300/2016	29/04/2016	CSL	
Council position		05581/1/2016	17/05/2016	CSL	Summary
Commission communication on Council's position		COM(2016)0363	30/05/2016	EC	Summary
Committee draft report		PE584.110	14/06/2016	EP	
Committee recommendation tabled for plenary, 2nd reading		A8-0211/2016	17/06/2016	EP	Summary
Text adopted by Parliament, 2nd reading		T8-0303/2016	06/07/2016	EP	Summary
Draft final act		00026/2016/LEX	06/07/2016	CSL	
Committee letter confirming interinstitutional agreement		PE612.045	04/10/2017	EP	
Text agreed during interinstitutional negotiations		PE612.044	04/10/2017	EP	
Follow-up document		COM(2019)0546	28/10/2019	EC	

Additional information

National parliaments	IPEX
European Commission	EUR-Lex

Final act

Directive 2016/1148
OJ L 194 19.07.2016, p. 0001 Summary

High common level of network and information security across the Union. NIS Directive

PURPOSE: ensure a high common level of network and information security (NIS) across the Union.

PROPOSED ACT: Directive of the European Parliament and of the Council.

PARLIAMENTS ROLE: Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: network and information systems and services play a vital role in in facilitating the cross-border movement of goods, services and people. Substantial disruption of these systems in one Member State can affect other Member States and the EU as a whole.

The resilience and stability of network and information systems is therefore essential to the smooth functioning of the internal market.

The extent and frequency of security incidents, caused by human error or malicious attacks is increasing: the Commissions public consultation found that 57 % of respondents had experienced NIS incidents over the previous year that had a serious impact on their activities. A 2012 Eurobarometer survey found that 38% of EU internet users are concerned about the safety of online payments.

There is currently no effective mechanism at EU level for effective cooperation and collaboration and for secure information sharing on NIS incidents and risks among the Member States.

However, the Digital Agenda for Europe and the related Council conclusions highlighted the shared understanding that trust and security are fundamental pre-conditions for the wide uptake of information and communication technologies (ICT).

This proposal is presented in connection with the joint Communication of the Commission and High Representative of the Union for Foreign Affairs and Security Policy on a European Cybersecurity Strategy.

IMPACT ASSESSMENT: the Commission analysed three different options.

- Option 1: status quo: maintain the current approach.
- Option 2: regulatory approach, consisting of a legislative proposal establishing a common EU legal framework for NIS regarding

Member State capabilities, mechanisms for EU-level cooperation, and requirements for key private players and public administrations.

- Option 3: mixed approach, combining voluntary initiatives for Member State NIS capabilities and mechanisms for EU-level cooperation with regulatory requirements for key private players and public administrations.

The Commission concluded that Option 2 would have the strongest positive impacts. The quantitative assessment showed that this option would not impose a disproportionate burden on Member States. The costs for the private sector would also be limited since many of the entities concerned are already supposed to comply with existing security requirements.

LEGAL BASIS: Article 114 of the Treaty on the Functioning of the European Union (TFEU).

CONTENT: the proposal aims to effect a fundamental change in the way NIS is dealt with in the EU. It provides for regulatory obligations to create a level playing field and close existing legislative loopholes. The objectives of the proposed Directive are as follows:

(1) To require all Member States to have in place a minimum level of national capabilities by establishing competent authorities for NIS, setting up Computer Emergency Response Teams (CERTs), and adopting national NIS strategies and national NIS cooperation plans.

(2) To ensure that the national competent authorities cooperate within a network enabling secure and effective coordination, including coordinated information exchange as well as detection and response at EU level. Through this network, Member States will exchange information and cooperate, through the European Network and Information Security Agency (ENISA) to counter NIS threats and incidents and facilitate a uniform application of the directive throughout the EU.

(3) To ensure that a culture of risk management develops and that information is shared between the private and public sectors. Companies in the specific critical sectors banking, stock exchanges, energy generation, transmission and distribution, transport (air, rail, maritime), health, internet services as well as public administrations will be required to:

- assess the risks they face and adopt appropriate and proportionate measures to ensure NIS;
- report to the competent authorities any incidents seriously compromising their networks and information systems and significantly affecting the continuity of critical services and supply of goods.

BUDGETARY IMPLICATIONS: cooperation and exchange of information between Member States should be supported by a secure infrastructure. The proposal will have EU budgetary implications only if Member States choose to adapt an existing infrastructure (e.g. sTESTA) and task the Commission to implement this under the Multiannual Financial Framework 2014-2020. The one-off cost is estimated to be EUR 1 250 000 on condition that sufficient funds are available under the Connecting Europe Facility (CEF).

Alternatively, Member States can either share the one-off cost of adapting an existing infrastructure or decide to set up a new infrastructure and bear the costs, which are estimated to be approximately EUR 10 million per year.

DELEGATED ACTS: the proposal contains provisions empowering the Commission to adopt delegated acts in accordance with Article 290 of the Treaty on the Functioning of the EU.

High common level of network and information security across the Union. NIS Directive

The Council discussed the proposal for a Directive aimed at ensuring a high common level of security of electronic communication networks and information systems across the EU. The discussion was based on a progress report by the Irish Presidency on the work done so far in the Council's preparatory bodies.

The Presidency has identified the following main issues, which it believes are matters delegations would like to discuss further:

Impact assessment (IA): with regard to the IA which accompanies the proposal, a number of Member States pointed out that there appears to be a number of discrepancies between the two documents and that, in particular, the IA does not sufficiently justify why specific sectors have been included in the proposal, such as enablers of information society services, and others not, such as hardware/software manufacturers. Member States were also looking for more substance in the IA with regard to the impact of the proposal on employment, competitiveness and innovation, data protection, operations of multinational companies, investment climate, etc. Most Member States also raised the issue of the perceived significant costs involved in the implementation of the proposed Directive and regretted that the IA fails to sufficiently assess the possible benefits.

At a more fundamental level, Member States requested further justification from the Commission why a legislative, rather than a voluntary approach, would be the preferred option to tackle the uneven level of security capabilities across the EU and the insufficient sharing of information on incidents, risks and threats, which the Commission perceives as being the root causes of the situation. Delegations asked for more information about which companies and other stakeholders had replied to which questions in the Commission's public consultation, as this would help them to better assess where urgent problems exist.

Scope: detailed discussions will be necessary on which "market operators" would fall within the scope of the proposed Directive. In this regard, doubts were expressed about putting providers of information society services under the same obligations as operators of critical infrastructures and questions were raised with the proposed non exhaustive list of market operators, which would need to be agreed upon and which would cover those entities to which obligations with regard to incidents' notifications would apply.

Organisational framework: with regard to the organisational framework for the implementation of the proposed Directive, delegations have not yet expressed firm positions on the proposed governance structure as they are carrying out national consultations with stakeholders and are analysing the details of the proposal in the context of existing or planned national cyber strategies.

High common level of network and information security across the Union. NIS Directive

Opinion of the European Data Protection Supervisor on (i) the Joint Communication of the Commission and of the High Representative of the

European Union for Foreign Affairs and Security Policy on a Cyber Security Strategy of the European Union: An open, safe and secure cyberspace, and (ii) on the Commission proposal for a directive concerning measures to ensure a high common level of network and information security across the Union.

The EDPS welcomes the comprehensive Cyber Security Strategy and that the Strategy goes beyond the traditional approach of opposing security to privacy by providing for the explicit recognition of privacy and data protection as core values.

However, the EDPS notes that due to the lack of consideration and taking full account of other parallel Commission initiatives and ongoing legislative procedures, such as the data protection reform and the proposed regulation on electronic identification and trust services, the Cyber Security Strategy fails to provide a really comprehensive and holistic view of cyber security in the EU and risks to perpetuate a fragmented and compartmentalised approach.

The EDPS formulates the following recommendations:

The Cyber Security Strategy:

- it would be advisable to have a clear and restrictive definition of cybercrime rather than an overreaching one;
- data protection law should apply to all actions of the Strategy whenever they concern measures that entail the processing of personal data; he also notes that many actions consist in the setting up of coordination mechanisms;
- as guardians of the privacy and data protection rights of individuals, data protection authorities (DPAs) should be appropriately involved in their capacity of supervisory bodies with respect to implementing measures that involve the processing of personal data (such as the launch of the EU pilot project on fighting botnets and malware).

Proposed directive on network and information security (NIS):

- provide more clarity and certainty on the definition of the market operators that fall within the scope of the proposal, and to set up an exhaustive list that includes all relevant stakeholders, with a view to ensuring a fully harmonised and integrated approach to security within the EU;
- explicitly provide that the directive should apply without prejudice to existing or future more detailed rules in specific areas (such as those to be set forth upon trust service providers in the proposed regulation on electronic identification),
- add a recital to explain the need to embed data protection by design and by default from the early stage of the design of the mechanisms established in the proposal;
- specify that the processing of personal data would be justified under insofar as it is necessary to meet the objectives of public interest pursued by the proposed directive;
- lay down the circumstances when a notification is required and whether or not, and to which extent, the notification and its supporting documents will include details of personal data affected by a specific security incident (such as IP addresses);
- ensure that the exclusion of microenterprises from the scope of the notification does not apply to those operators that play a crucial role in the provision of information society services, for instance in view of the nature of the information they process (e.g. biometric data or sensitive data);
- add provisions in the proposal governing the further exchange of personal data by NIS competent authorities with other recipients, to ensure that (i) personal data are only disclosed to recipients whose processing is necessary for the performance of their tasks;
- specify the time limit for the retention of personal data;
- remind NIS competent authorities of their duty to provide appropriate information to data subjects on the processing of personal data, for example by posting a privacy policy on their website;
- add a provision regarding the level of security to be complied with by NIS competent authorities as regards the information collected, processed, and exchanged;
- clarify that the criteria for the participation of Member States in the secure information-sharing system should ensure that a high level of security and resilience is guaranteed by all the participants in the information-sharing systems at all steps of the processing;
- add a description of the roles and responsibilities of the Commission and of the Member States in the setup, operation and maintenance of the secure information-sharing system;
- add that any transfer of personal data to recipients located in countries outside the EU should take place in accordance with Directive 95/46/EC and Regulation (EC) No 45/2001.

High common level of network and information security across the Union. NIS Directive

The Council took note of the state of play regarding a draft directive aimed at ensuring a high common level of security of electronic communication networks and information systems across the EU.

Although all delegations fully acknowledge the need for action to combat cyber attacks, views differ on the best way to ensure network security throughout the EU:

- some delegations prefer a flexible approach, with EU-wide binding rules limited to critical infrastructure and basic requirements, complemented by voluntary measures;
- other delegations, as well as the Commission, consider that only legally binding measures would bring about the necessary security at EU level.

As regards more detailed provisions, further discussion is needed on a number of questions, such as:

NIS strategy and NIS competent body: delegations acknowledge that a substantial disruption in one Member State can also affect other Member States and could support the principle of a coordinating entity at national level. However, in particular those Member States, which already adopted NIS strategies, designated competent bodies and set up a national computer emergency response teams (CERT), seem to critically look at chapter II of the proposal, which deals with the national framework on NIS: they wish to make sure that the requirements that will have to be met by Member States are consistent with and do not go beyond the current national practice.

Other delegations seek further clarification about the terminology used in this chapter, such as 'risks' and 'threats' and wonder what the exact requirements are and also question whether these requirements should only concern the private sector or also the public sector.

Competent authority and its task description: many issues require further clarification, such as whether the authority should assume operational tasks, which is something many Member States object to, and what should be the division of responsibilities with the national CERT.

Risk management and incident notification: many delegations:

- doubt whether in addition to 'operators of critical infrastructures', also 'information society service providers' should be covered by the proposal;
- called for more clarity on the definition and for more flexibility for Member States to define which sectors constitute national critical infrastructures. Some delegations wish to limit the proposed requirements to the private sector only and others call for the security breach reporting requirements in this chapter to be voluntary;
- questioned whether or how Member States could actually "ensure" that parties secure their networks and notify incidents.

There are also concerns with regard to the implications of notifications on matters of privacy and confidentiality of information.

Cooperation network: further discussion will be needed on the tasks of the cooperation network although many delegations are of the opinion that it should not assume any operational tasks; some argue in this respect that it would be better to refer to a mechanism rather than to a network.

A number of organisational issues also require further clarification, such as:

- who will chair the cooperation network, what its costs would be, and what the relationship and division of responsibilities would be with the cooperation of national CERTs with ENISA and with Europol;
- the sharing of information in the network should be done on a voluntary basis;
- the question of the need for the proposed and dedicated 'secure information-sharing system';
- the proposed early warning mechanism raises many queries and concerns, e.g. which information shall be shared at what point in time and with what possible consequences for the incident or risk;
- the question of the scope of the proposed coordinated response mechanism and when and under what conditions a coordinated response would be required requires further discussion.

According to the Presidency, the main challenge will be to agree on an approach, which strikes the right balance between EU-wide binding rules and optional, voluntary measures, all of which should lead to similar levels of NIS preparedness among the Member States and allow the EU to respond effectively to NIS challenges.

High common level of network and information security across the Union. NIS Directive

The Committee on the Internal Market and Consumer Protection adopted the report by Andreas SCHWAB (EPP, DE) 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.

The Committee on Industry, Research and Energy and the Committee on Civil Liberties, Justice and Home Affairs, exercised the prerogatives of associated committees in line with Article 50 of the Parliament's Rules of Procedure, were also consulted to give an opinion on this report.

The parliamentary committee recommended that the position of the European Parliament adopted at first reading under the ordinary legislative procedure modify the Commission proposal as follows.

Scope: the Directive aims at imposing obligations on public administrations and market operators, including critical infrastructures and information society services.

In order to achieve proportionality and swift results of the Directive, Members consider that the compulsory measures laid down in Chapter IV should be limited to infrastructures that are critical in a stricter sense. They took the view that information society services should therefore not be included in Annex II of this Directive (list of market operators). Instead,

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 and health. Software developers and hardware manufacturers should be excluded from the scope of this Directive.

Protection and processing of personal data: Members stressed that 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. Any use of personal data should be limited only to what is necessary and should be as anonymous as possible, or even totally anonymous.

National competent authorities and single points of contact on the security of network and information systems: Members proposed amending the directive to authorise the designation of one or more competent authorities by Member States.

However, in order to ensure a coherent application within the Member State and in order to allow for an effective and streamlined cooperation at Union level, each Member State should appoint one single point of contact. The single point of contact shall ensure, among other things, cross-border cooperation with other single points of contact.

Computer Emergency Response Teams (CERTs): each Member State shall set up at least one Response Team for each of the sectors established in Annex II, responsible for handling incidents and risks according to a well-defined process.

CERTs should have adequate human and financial resources to actively participate in international, and in particular Union, cooperation networks.

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 United Nations.

Cooperation network: with the aim of strengthening the activities of the cooperation network, the Members consider that the latter should envisage inviting market operators and suppliers of cyber security solutions to participate where appropriate.

Security requirements and incident notification: the proposal foresees that the Commission shall be empowered to adopt delegated acts concerning the definition of circumstances in which public administrations and market operators are required to notify incidents.

For the purpose of clarifying the scope of obligations and enshrining them in the basic act, it is proposed to replace the delegated acts with clear criteria to determine the significance of incidents to be reported. To determine the significance of the impact of an incident, the following parameters shall inter alia be taken into account: i) the number of users whose core service is affected; ii) the duration of the incident; iii) the geographic spread with regard to the area affected by the incident.

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. Member States shall encourage market operators to make public incidents involving their business in their financial reports on a voluntary basis.

Implementation and enforcement: the proposal foresees that market operators provide an audit carried out by a qualified independent body or national authority, and make the evidence available to the competent authority. For their part Members recognise it is necessary to allow for flexibility regarding the evidence for compliance with the security requirements imposed on market operators by admitting proof of compliance provided in a form other than security audits.

The single points of contact and the data protection authorities shall develop, in cooperation with the European Union Agency for Network and Information Security (ENISA), information exchange mechanisms and a single template to be used both for notifications.

Sanctions : Members proposed clarifying that where the market operator has failed to comply with the obligations in relation to the directive, but has not acted with intent or gross negligence, no sanction should be imposed.

High common level of network and information security across the Union. NIS Directive

The European Parliament adopted by 521 votes to 22 with 25 abstentions, a legislative resolution 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 (NIS) across the Union.

Parliaments position in first reading following the ordinary legislative procedure amended the Commission proposal as follows:

Scope: the draft Directive aims at imposing obligations on public administrations and market operators, including critical infrastructures and information society services.

In order to achieve proportionality and swift results of the Directive, Members consider that the compulsory measures laid down in Chapter IV should be limited to infrastructures that are critical in a stricter sense. They took the view that information society services should therefore not be included in the list of market operators in Annex II of the draft directive (such as internet payment gateways, social networks, search engines, cloud computing services).

The 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 and health. Software developers and hardware manufacturers should be excluded from the scope of this Directive.

Protection and processing of personal data: Members stressed that 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. Any use of personal data should be limited only to what is necessary and should be as anonymous as possible, or even totally anonymous.

National NIS strategies: Parliament proposed that Member States may request the assistance of the European Union Agency for Network and Information Security (ENISA) in developing their national NIS strategies and national NIS cooperation plans, based on a common minimum NIS strategy.

National competent authorities and single points of contact on the security of network and information systems: Members proposed amending the directive to authorise the designation of one or more competent authorities by Member States.

However, in order to ensure a coherent application within the Member State and in order to allow for an effective and streamlined cooperation at Union level, each Member State should appoint one single point of contact. The single point of contact shall ensure, among other things, cross-border cooperation with other single points of contact.

Computer Emergency Response Teams (CERTs): each Member State shall set up at least one Response Team for each of the sectors established in Annex II, responsible for handling incidents and risks according to a well-defined process.

CERTs should have adequate human and financial resources to actively participate in international, and in particular Union, cooperation networks.

CERTs will be 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 United Nations.

Cooperation network: with the aim of strengthening the activities of the cooperation network, Members consider that the latter should

envisage inviting market operators and suppliers of cyber security solutions to participate where appropriate. The cooperation network shall publish a report once a year on the activities of the network.

Member States may determine the level of criticality of market operators, taking into account the specificities of sectors, and different parameters.

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.

Security requirements and incident notification: the proposal provides that the Commission shall be empowered to adopt delegated acts concerning the definition of circumstances in which public administrations and market operators are required to notify incidents.

For the purpose of clarifying the scope of obligations and enshrining them in the basic act, it is proposed to replace the delegated acts with clear criteria to determine the significance of incidents to be reported. To determine the significance of the impact of an incident, the following parameters shall inter alia be taken into account: i) the number of users whose core service is affected; ii) the duration of the incident; iii) the geographic spread with regard to the area affected by the incident.

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. Member States shall encourage market operators to make public incidents involving their business in their financial reports on a voluntary basis.

Implementation and enforcement: the proposal provides that market operators provide an audit carried out by a qualified independent body or national authority, and make the evidence available to the competent authority. Parliament suggested allowing for flexibility regarding the evidence for compliance with the security requirements imposed on market operators by admitting proof of compliance provided in a form other than security audits.

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.

Sanctions: Members proposed clarifying that where the market operator has failed to comply with the obligations in relation to the directive, but has not acted with intent or gross negligence, no sanction should be imposed.

High common level of network and information security across the Union. NIS Directive

OPINION OF THE EUROPEAN CENTRAL BANK (ECB) on a 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 (NIS) across the Union.

The ECB decided to deliver an own initiative opinion on the proposed directive, since it was not formally consulted by the legislators.

The ECB supports the aim of the proposed directive to ensure a high common level of NIS across the Union and to achieve a consistency of approach in this area across business sectors and Member States.

However, the ECB considers that the proposed directive should be without prejudice to the existing regime for the Eurosystem's oversight of payment and settlement systems, which includes appropriate arrangements, inter alia, in the area of NIS. It is for this reason that the ECB suggests amending the proposed directive to properly reflect the Eurosystem's responsibilities in this area.

The ECB notes that the existing oversight arrangements in respect of payment systems and payment service providers (PSPs) already contain procedures for early warnings and coordinated responses within and beyond the Eurosystem to deal with possible cyber-security threats, which are equivalent to those laid down in the proposed directive.

The ESCB has set standards regarding reporting and risk management obligations for payment systems. Furthermore, the ECB regularly assesses securities settlement systems in order to determine their eligibility for use in the Eurosystem credit operations.

Therefore, the ECB considers it necessary that the requirements in the proposed directive affecting critical market infrastructures and their operators do not prejudice the standards in the draft regulation on oversight requirements for systemically important payment systems (SIPS Regulation), the Eurosystem's oversight policy framework or other Union regulations, and in particular the European Market Infrastructure Regulation (EMIR) and the future Regulation on improving securities settlement in the European Union and on central securities depositories (CSDs).

Moreover, they should not interfere with the tasks of the European Banking Authority or the European Securities and Markets Authority and other prudential supervisors.

Notwithstanding the above, the ECB considers that there is a strong case for the Eurosystem to share relevant information with the NIS Committee to be set up pursuant to Article 19 of the proposed directive.

High common level of network and information security across the Union. NIS Directive

The Council adopted its position at first reading with a view to the adoption of a Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

The proposed Directive lays down measures with a view to achieving a high common level of security of networks and information systems within the European Union so as to improve the functioning of the internal market.

The main elements of the compromise reached with the European Parliament are outlined below:

Obligations with regard to their national cybersecurity capabilities: under the Council position, Member States are required to:

adopt a national strategy defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of networks and information system;

- designate one or more national competent authorities on the security of network and information systems to monitor the application of the Directive at national level;
- designate a national single point of contact on the security of networks and information systems that will exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the cooperation group and the CSIRTs network. The single point of contact will also submit a yearly report on notifications received to the Cooperation Group;
- designate one or more Computer Security Incident Response Teams ("CSIRTs ") responsible for handling incidents and risks. The compromise text provides for requirements and tasks of CSIRTs in its Annex I.

Cooperation: in order to support and facilitate strategic cooperation among Member States, to develop trust and confidence and with a view to achieving a high common level of security of networks and information systems in the Union, the Council position:

- establishes a Cooperation Group which will be composed of representatives from the Member States, the Commission and the European Union Agency for Network and Information Security ('ENISA') and will have specific tasks listed in the text, such as exchanging best practices and information on a number of issues or discussing capabilities and preparedness of Member States;
- establishes a network of the national CSIRTs in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation. The text provides for a list of tasks to be carried out by the network, such as exchanging information on CSIRTs services, operations and cooperation capabilities, supporting Member States in addressing cross border incidents or, under certain conditions, exchanging and discussing information related to incidents and associated risks.

Security and notification requirements: under the Council position, the Directive shall lay down certain obligations for two sets of market players: (i) operators of essential services and (ii) digital service providers.

The Directive takes a differentiated approach with regard to the two categories of players. The security and notification requirements are lighter for digital service providers than for operators of essential services, which reflects the degree of risk that disruption to their services may pose to society and economy.

Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information systems' incidents and risks.

Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide.

Essential services (Annex II) of the Directive lists a number of sectors important for society and economy, namely energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution and digital infrastructure. Within these sectors Member States will identify the operators of essential services, based on precise criteria provided for in the Directive.

Digital services (Annex III) of the Directive lists three types of digital services, the providers of which will have to comply with the requirements of the Directive: online market places, online search engines and cloud computing services. All digital service providers providing the listed services will have to comply with the requirements of the Directive with the exclusion of micro and small enterprises.

Entities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.

Transposition: Member States will be required to transpose the Directive by 21 months after the date of its entry into force and will have 6 additional months to identify their operators of essential services.

High common level of network and information security across the Union. NIS Directive

The Commission supports the results of the inter-institutional negotiations and can therefore accept the Council's position at first reading on the adoption of a Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

The Commission noted that overall the Councils position endorses the core objectives of the Commission proposal, namely to ensure a high common level of security of network and information systems. However, the Council makes a number of changes regarding how to achieve this goal.

National cybersecurity capabilities: under the Council position, Member States will be required to adopt a national NIS strategy setting out the strategic objectives and appropriate policy and regulatory measures for cybersecurity. Member States will also be required to designate a national competent authority for the implementation and enforcement of the Directive, as well as Computer Security Incident Response Teams (CSIRTs) responsible for handling incidents and risks. Although the Council position does not require Member States to adopt a national NIS cooperation plan, as envisaged in the original proposal, the position can be supported as some aspects of the cooperation plan are retained in the provision on the NIS strategy.

Cooperation between Member States: under the Council position, the Directive will: (i) create a Cooperation Group to support and facilitate strategic cooperation and the exchange of information between the Member States; (ii) create a network of Computer Security Incident Response Teams, known as the CSIRTs Network, to promote swift and effective operational cooperation on specific cybersecurity incidents and the sharing of information about risks.

Though substantively different from the approach taken in the original proposal, the Council position can be supported as it corresponds overall to the objective of improving cooperation between Member States.

Security and notification requirements for operators of essential services: the Commission noted that the Council did not support an obligation for national competent authorities to notify incidents of a criminal nature to law enforcement authorities.

As per the original proposal, the Council position covers such operators in the energy, transport, banking, financial market infrastructures and

health sectors. However, the Council position includes additionally the water and digital infrastructure sectors.

Member States will be required to identify these operators on the basis of certain criteria, such as whether the service is essential for the maintenance of critical societal or economic activities. Although this identification process was not part of the original proposal, it can be accepted given the Member States obligation to submit to the Commission the information it needs to assess whether Member States are using consistent approaches to identify operators of essential services.

Security and notification requirements for digital service providers: the Council position covers online marketplaces (equivalent to e-commerce platforms in the original proposal), cloud computing services and search engines.

Compared with the original proposal, the Council position does not include: (i) internet payment gateways these are now covered by the revised Payment Services Directive; (ii) application stores these are to be understood as being a type of online marketplace; (iii) social networks as per the Councils political agreement with the European Parliament.

The Commission has been granted implementing powers for laying down procedural arrangements necessary for the functioning of the Cooperation Group as well as to specify further certain elements concerning DSPs, including the formats and procedures applicable to DSPs notification requirements.

High common level of network and information security across the Union. NIS Directive

The Committee on the Internal Market and Consumer Protection adopted the recommendation for a second reading contained in the report by Andreas SCHWAB (EPP, DE) on the Council position at first reading with a view to the adoption of a directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

The committee recommended the European Parliament to adopt the Council position at first reading without amendment.

To recall, the proposal aims to lay down measures with a view to achieving a high common level of security of networks and information systems within the European Union so as to improve the functioning of the internal market.

High common level of network and information security across the Union. NIS Directive

The European Parliament adopted, at second reading of the ordinary legislative procedure, a legislative resolution on the Council position at first reading with a view to the adoption of a directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

In line with the recommendation made by the Committee on the Internal Market and Consumer Protection, Parliament adopted the Council position at first reading without amendment.

To recall, the proposed Directive seeks to achieve a high common level of security of networks and information systems within the European Union.

High common level of network and information security across the Union. NIS Directive

PURPOSE: ensure a high common level of security of network and information systems across the Union.

LEGISLATIVE ACT: Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

CONTENT: the Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market. Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

However, the existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union.

Obligations with regard to their national cybersecurity capabilities: the Directive requires Members States to:

- adopt an national strategy and designate a national authority on security of network and information systems (NIS) with adequate resources to prevent, handle and respond to NIS risks and incidents;
- establish a network of the national Computer Security Incident Response Teams (CSIRTs) responsible for handling incidents and risks.

Cooperation: in order to support strategic cooperation among Member States, to develop trust and confidence and with a view to achieving a high common level of security of networks and information systems in the Union, the Directive provides for the establishment of a Cooperation Group which will be composed of representatives from the Member States, the Commission and the European Union Agency for Network and Information Security ('ENISA'). This Group will have specific tasks, such as exchanging best practices and information on a number of issues or discussing capabilities and preparedness of Member States.

In order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation, the Directive establishes a network of the national CSIRTs.

Security and notification requirements: the Directive aims to promote a culture of risk management and encourage the sharing of information between the public and private sectors.

Companies operating in certain critical sectors as well as public administrations must evaluate the risks they run and adopt appropriate and

proportionate measures to ensure NIS. These companies must notify competent authorities of all incidents that seriously compromise their networks and information systems and have a significant disruptive effect on the continuity of critical services and supply of goods.

The requirement to notify security incidents affects:

- operators of essential services in sectors such as financial services, transport, energy and health;
- providers of digital services providing three types of services: (i) online market places, (ii) online search engines and (iii) cloud computing services;
- public administrations which are identified as operators of essential services.

Taking a differentiated approach with regard to the two categories of players, the Directive provides that the security and notification requirements are lighter for digital service providers than for operators of essential services.

ENTRY INTO FORCE: 8.8.2016.

TRANSPOSITION: by 9.5.2018.

APPLICATION: from 10.5.2016.