Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 6 July 2016

concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[(1)],

Acting in accordance with the ordinary legislative procedure[(2)],

Whereas:

(1) 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.

(2) The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

(3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

(4) Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security (‘ENISA’), should be

established to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems. For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory. In addition, security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.

(5) 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. This results in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union. Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level. Universities and research centres have a decisive role to play in spurring research, development and innovation in those areas.

(6) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information, cooperation and common security requirements for operators of essential services and digital service providers. However, operators of essential services and digital service providers are not precluded from implementing security measures that are stricter than those provided for under this Directive.

(7) To cover all relevant incidents and risks, this Directive should apply to both operators of essential services and digital service providers. However, the obligations on operators of essential services and digital service providers should not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council[(3)], which are subject to the specific security and integrity requirements laid down in that Directive, nor should they apply to trust service providers within the meaning of Regulation (EU) No 910/2014 of the European Parliament and of the Council[(4)], which are subject to the security requirements laid down in that Regulation.

(8) This Directive should be without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of the essential interests of its security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences. In accordance with Article 346 of the Treaty on the Functioning of the European Union (TFEU), no Member State is to be obliged to supply information the disclosure of which it considers to be contrary to the essential interests of its security. In this context, Council Decision 2013/488/EU[(5)] and non-disclosure agreements, or informal non-disclosure agreements such as the Traffic Light Protocol, are of relevance.

(9) Certain sectors of the economy are already regulated or may be regulated in the future by sector-specific Union legal acts that include rules related to the security of network and information systems. Whenever those Union legal acts contain provisions imposing requirements concerning the security of network and information systems or notifications of incidents, those provisions should apply if they contain requirements which are at least equivalent in effect to the obligations contained in this Directive. Member States should then apply the provisions of such sector-specific Union legal acts, including those relating to jurisdiction, and should not carry out the identification process for operators of essential services as defined by this Directive. In this context, Member States should provide information to the Commission on the application of such *lex specialis* provisions. In determining whether the requirements on the security of network and information systems and the notification of incidents contained in sector-specific Union legal acts are equivalent to those contained in this Directive, regard should only be had to the provisions of relevant Union legal acts and their application in the Member States.

(10) In the water transport sector, security requirements for companies, ships, port facilities, ports and vessel traffic services under Union legal acts cover all operations, including radio and telecommunication systems, computer systems and networks. Part of the mandatory procedures to be followed includes the reporting of all incidents and should therefore be considered as *lex specialis*, in so far as those requirements are at least equivalent to the corresponding provisions of this Directive.

(11) When identifying operators in the water transport sector, Member States should take into account existing and future international codes and guidelines developed in particular by the International Maritime Organisation, with a view to providing individual maritime operators with a coherent approach.

(12) Regulation and supervision in the sectors of banking and financial market infrastructures is highly harmonised at Union level, through the use of primary and secondary Union law and standards developed together with the European supervisory authorities. Within the banking union, the application and the supervision of those requirements are ensured by the single supervisory mechanism. For Member States that are not part of the banking union, this is ensured by the relevant banking regulators of Member States. In other areas of financial sector regulation, the European System of Financial Supervision also ensures a high degree of commonality and convergence in supervisory practices. The European Securities Markets Authority also plays a direct supervision role for certain entities, namely credit-rating agencies and trade repositories.

(13) Operational risk is a crucial part of prudential regulation and supervision in the sectors of banking and financial market infrastructures. It covers all operations including the security, integrity and resilience of network and information systems. The requirements in respect of those systems, which often exceed the requirements provided for under this Directive, are set out in a number of Union legal acts, including: rules on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, and rules on prudential requirements for credit institutions

and investment firms, which include requirements concerning operational risk; rules on markets in financial instruments, which include requirements concerning risk assessment for investment firms and for regulated markets; rules on OTC derivatives, central counterparties and trade repositories, which include requirements concerning operational risk for central counterparties and trade repositories; and rules on improving securities settlement in the Union and on central securities depositories, which include requirements concerning operational risk. Furthermore, requirements for notification of incidents are part of normal supervisory practice in the financial sector and are often included in supervisory manuals. Member States should consider those rules and requirements in their application of *lex specialis*.

(14) As noted by the European Central Bank in its opinion of 25 July 2014[(6)], this Directive does not affect the regime under Union law for the Eurosystem's oversight of payment and settlement systems. It would be appropriate for the authorities responsible for such oversight to exchange experiences on matters concerning security of network and information systems with the competent authorities under this Directive. The same consideration applies to non-euro area members of the European System of Central Banks exercising such oversight of payment and settlement systems on the basis of national laws and regulations.

(15) An online marketplace allows consumers and traders to conclude online sales or service contracts with traders, and is the final destination for the conclusion of those contracts. It should not cover online services that serve only as an intermediary to third-party services through which a contract can ultimately be concluded. It should therefore not cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product. Computing services provided by the online marketplace may include processing of transactions, aggregations of data or profiling of users. Application stores, which operate as online stores enabling the digital distribution of applications or software programmes from third parties, are to be understood as being a type of online marketplace.

(16) An online search engine allows the user to perform searches of, in principle, all websites on the basis of a query on any subject. It may alternatively be focused on websites in a particular language. The definition of an online search engine provided in this Directive should not cover search functions that are limited to the content of a specific website, irrespective of whether the search function is provided by an external search engine. Neither should it cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product.

(17) Cloud computing services span a wide range of activities that can be delivered according to different models. For the purposes of this Directive, the term ‘cloud computing services’ covers services that allow access to a scalable and elastic pool of shareable computing resources. Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services. The term ‘scalable’ refers to computing resources that are flexibly allocated by the cloud service provider,

irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment.

(18) The function of an internet exchange point (IXP) is to interconnect networks. An IXP does not provide network access or act as a transit provider or carrier. Nor does an IXP provide other services unrelated to interconnection, although this does not preclude an IXP operator from providing unrelated services. An IXP exists to interconnect networks that are technically and organisationally separate. The term 'autonomous system' is used to describe a technically stand-alone network.

(19) Member States should be responsible for determining which entities meet the criteria of the definition of operator of essential services. In order to ensure a consistent approach, the definition of operator of essential services should be coherently applied by all Member States. To that end, this Directive provides for the assessment of the entities active in specific sectors and subsectors, the establishment of a list of essential services, the consideration of a common list of cross-sectoral factors to determine whether a potential incident would have a significant disruptive effect, a consultation process involving relevant Member States in the case of entities providing services in more than one Member State, and the support of the Cooperation Group in the identification process. In order to ensure that possible changes in the market are accurately reflected, the list of identified operators should be reviewed regularly by Member States and updated when necessary. Finally, Member States should submit to the Commission the information necessary to assess the extent to which this common methodology has allowed a consistent application of the definition by Member States.

(20) In the process of identification of operators of essential services, Member States should assess, at least for each subsector referred to in this Directive, which services have to be considered as essential for the maintenance of critical societal and economic activities, and whether the entities listed in the sectors and subsectors referred to in this Directive and providing those services meet the criteria for the identification of operators. When assessing whether an entity provides a service which is essential for the maintenance of critical societal or economic activities, it is sufficient to examine whether that entity provides a service that is included in the list of essential services. Furthermore, it should be demonstrated that provision of the essential service is dependent on network and information systems. Finally, when assessing whether an incident would have a significant disruptive effect on the provision of the service, Member States should take into account a number of cross-sectoral factors, as well as, where appropriate, sector-specific factors.

(21) For the purposes of identifying operators of essential services, establishment in a Member State implies the effective and real exercise of activity through stable

arrangements. The legal form of such arrangements, whether through a branch or a subsidiary possessing legal personality, is not the determining factor in this respect.

(22) It is possible that entities operating in the sectors and subsectors referred to in this Directive provide both essential and non-essential services. For example, in the air transport sector, airports provide services which might be considered by a Member State to be essential, such as the management of the runways, but also a number of services which might be considered as non-essential, such as the provision of shopping areas. Operators of essential services should be subject to the specific security requirements only with respect to those services which are deemed to be essential. For the purpose of identifying operators, Member States should therefore establish a list of the services which are considered as essential.

(23) The list of services should contain all services provided in the territory of a given Member State that fulfil the requirements under this Directive. Member States should be able to supplement the existing list by including new services. The list of services should serve as a reference point for Member States, allowing for identification of operators of essential services. Its purpose is to identify the types of essential services in any given sector referred to in this Directive, thus distinguishing them from non-essential activities for which an entity active in any given sector might be responsible. The list of services established by each Member State would serve as further input in the assessment of the regulatory practice of each Member State with a view to ensuring the overall level of consistency of the identification process amongst Member States.

(24) For the purposes of the identification process, where an entity provides an essential service in two or more Member States, those Member States should engage in bilateral or multilateral discussions with each other. This consultation process is intended to help them to assess the critical nature of the operator in terms of cross-border impact, thereby allowing each Member State involved to present its views regarding the risks associated with the services provided. The Member States concerned should take into account each other's views in this process, and should be able to request the assistance of the Cooperation Group in this regard.

(25) As a result of the identification process, Member States should adopt national measures to determine which entities are subject to obligations regarding the security of network and information systems. This result could be achieved by adopting a list enumerating all operators of essential services or by adopting national measures including objective quantifiable criteria, such as the output of the operator or the number of users, which make it possible to determine which entities are subject to obligations regarding the security of network and information systems. The national measures, whether already existing or adopted in the context of this Directive, should include all legal measures, administrative measures and policies allowing for the identification of operators of essential services under this Directive.

(26) In order to give an indication of the importance, in relation to the sector concerned, of the identified operators of essential services, Member States should take into account the number and the size of those operators, for example in terms of market share or of

the quantity produced or carried, without being obliged to divulge information which would reveal which operators have been identified.

(27) In order to determine whether an incident would have a significant disruptive effect on the provision of an essential service, Member States should take into account a number of different factors, such as the number of users relying on that service for private or professional purposes. The use of that service can be direct, indirect or by intermediation. When assessing the impact that an incident could have, in terms of its degree and duration, on economic and societal activities or public safety, Member States should also assess the time likely to elapse before the discontinuity would start to have a negative impact.

(28) In addition to the cross-sectoral factors, sector-specific factors should also be considered in order to determine whether an incident would have a significant disruptive effect on the provision of an essential service. With regard to energy suppliers, such factors could include the volume or proportion of national power generated; for oil suppliers, the volume per day; for air transport, including airports and air carriers, rail transport and maritime ports, the proportion of national traffic volume and the number of passengers or cargo operations per year; for banking or financial market infrastructures, their systemic importance based on total assets or the ratio of those total assets to GDP; for the health sector, the number of patients under the provider's care per year; for water production, processing and supply, the volume and number and types of users supplied, including, for example, hospitals, public service organisations, or individuals, and the existence of alternative sources of water to cover the same geographical area.

(29) To achieve and maintain a high level of security of network and information systems, each Member State should have a national strategy on the security of network and information systems defining the strategic objectives and concrete policy actions to be implemented.

(30) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, and to avoid duplication, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of operators of essential services and digital service providers under this Directive.

(31) In order to facilitate cross-border cooperation and communication and to enable this Directive to be implemented effectively, it is necessary for each Member State, without prejudice to sectoral regulatory arrangements, to designate a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level. Competent authorities and single points of contact should have the adequate technical, financial and human resources to ensure that they can carry out the tasks assigned to them in an effective and efficient manner and thus achieve the objectives of this Directive. As this Directive aims to improve the functioning of the internal market by creating trust and confidence, Member State bodies need to be able to cooperate effectively with economic actors and to be structured accordingly.

(32) Competent authorities or the computer security incident response teams ('CSIRTs') should receive notifications of incidents. The single points of contact should not receive directly any notifications of incidents unless they also act as a competent authority or a CSIRT. A competent authority or a CSIRT should however be able to task the single point of contact with forwarding incident notifications to the single points of contact of other affected Member States.

(33) To ensure the effective provision of information to the Member States and to the Commission, a summary report should be submitted by the single point of contact to the Cooperation Group, and should be anonymised in order to preserve the confidentiality of the notifications and the identity of operators of essential services and digital service providers, as information on the identity of the notifying entities is not required for the exchange of best practice in the Cooperation Group. The summary report should include information on the number of notifications received, as well as an indication of the nature of the notified incidents, such as the types of security breaches, their seriousness or their duration.

(34) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ensure that they have well-functioning CSIRTs, also known as computer emergency response teams ('CERTs'), complying with essential requirements to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level. In order for all types of operators of essential services and digital service providers to benefit from such capabilities and cooperation, Member States should ensure that all types are covered by a designated CSIRT. Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive.

(35) As most network and information systems are privately operated, cooperation between the public and private sectors is essential. Operators of essential services and digital service providers should be encouraged to pursue their own informal cooperation mechanisms to ensure the security of network and information systems. The Cooperation Group should be able to invite relevant stakeholders to the discussions where appropriate. To encourage effectively the sharing of information and of best practice, it is essential to ensure that operators of essential services and digital service providers who participate in such exchanges are not disadvantaged as a result of their cooperation.

(36) ENISA should assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practice. In particular, in the application of this Directive, the Commission should, and Member States should be able to, consult ENISA. To build capacity and knowledge among Member States, the Cooperation Group should also serve as an instrument for the exchange of best practice, discussion of capabilities and preparedness of the Member States and, on a voluntary basis, to assist its members in evaluating national strategies on the security of network and information

systems, building capacity and evaluating exercises relating to the security of network and information systems.

(37) Where appropriate, Member States should be able to use or adapt existing organisational structures or strategies when applying this Directive.

(38) The respective tasks of the Cooperation Group and of ENISA are interdependent and complementary. In general, ENISA should assist the Cooperation Group in the execution of its tasks, in line with the objective of ENISA set out in Regulation (EU) No 526/2013 of the European Parliament and the Council[7], namely to assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information system security under existing and future legal acts of the Union. In particular, ENISA should provide assistance in those areas that correspond to its own tasks, as set out in Regulation (EU) No 526/2013, namely analysing network and information system security strategies, supporting the organisation and running of Union exercises relating to the security of network and information systems, and exchanging information and best practice on awareness-raising and training. ENISA should also be involved in the development of guidelines for sector-specific criteria for determining the significance of the impact of an incident.

(39) In order to promote advanced security of network and information systems, the Cooperation Group should, where appropriate, cooperate with relevant Union institutions, bodies, offices and agencies, to exchange know-how and best practice, and to provide advice on security aspects of network and information systems that might have an impact on their work, while respecting existing arrangements for the exchange of restricted information. In cooperating with law enforcement authorities regarding the security aspects of network and information systems that might have an impact on their work, the Cooperation Group should respect existing channels of information and established networks.

(40) Information about incidents is increasingly valuable to the general public and businesses, particularly small and medium-sized enterprises. In some cases, such information is already provided via websites at the national level, in the language of a specific country and focusing mainly on incidents and occurrences with a national dimension. Given that businesses increasingly operate across borders and citizens use online services, information on incidents should be provided in an aggregated form at Union level. The secretariat of the CSIRTs network is encouraged to maintain a website or to host a dedicated page on an existing website, where general information on major incidents that have occurred across the Union is made available to the general public, with a specific focus on the interests and needs of businesses. CSIRTs participating in the CSIRTs network are encouraged to provide on a voluntary basis the information to be published on that website, without including confidential or sensitive information.

(41) Where information is considered to be confidential in accordance with Union and national rules on business confidentiality, such confidentiality should be ensured when carrying out the activities and fulfilling the objectives set by this Directive.

(42) Exercises which simulate real-time incident scenarios are essential for testing Member States' preparedness and cooperation regarding the security of network and information systems. The CyberEurope cycle of exercises coordinated by ENISA with the participation of the Member States is a useful tool for testing and drawing up recommendations on how incident-handling at Union level should improve over time. Considering that the Member States are not currently under any obligation to either plan or participate in exercises, the creation of the CSIRTs network under this Directive should enable Member States to participate in exercises on the basis of accurate planning and strategic choices. The Cooperation Group set up under this Directive should discuss the strategic decisions regarding exercises, in particular but not exclusively as regards the regularity of the exercises and the design of the scenarios. ENISA should, in accordance with its mandate, support the organisation and running of Union-wide exercises by providing its expertise and advice to the Cooperation Group and the CSIRTs network.

(43) Given the global nature of security problems affecting network and information systems, there is a need for closer international cooperation to improve security standards and information exchange, and to promote a common global approach to security issues.

(44) Responsibilities in ensuring the security of network and information systems lie, to a great extent, with operators of essential services and digital service providers. 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 trustworthy level playing field is also essential to the effective functioning of the Cooperation Group and the CSIRTs network, to ensure effective cooperation from all Member States.

(45) This Directive applies only to those public administrations which are identified as operators of essential services. Therefore, it is the responsibility of Member States to ensure the security of network and information systems of public administrations not falling within the scope of this Directive.

(46) Risk-management measures include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems comprises the security of stored, transmitted and processed data.

(47) Competent authorities should retain the ability to adopt national guidelines concerning the circumstances in which operators of essential services are required to notify incidents.

(48) Many businesses in the Union rely on digital service providers for the provision of their services. As some digital services could be an important resource for their users, including operators of essential services, and as such users might not always have alternatives available, this Directive should also apply to providers of such services. The security, continuity and reliability of the type of digital services referred to in this

Directive are of the essence for the smooth functioning of many businesses. A disruption of such a digital service could prevent the provision of other services which rely on it and could thus have an impact on key economic and societal activities in the Union. Such digital services might therefore be of crucial importance for the smooth functioning of businesses that depend on them and, moreover, for the participation of such businesses in the internal market and cross-border trade across the Union. Those digital service providers that are subject to this Directive are those that are considered to offer digital services on which many businesses in the Union increasingly rely.

(49) Digital service providers should ensure a level of security commensurate with the degree of risk posed to the security of the digital services they provide, given the importance of their services to the operations of other businesses within the Union. In practice, the degree of risk for operators of essential services, which are often essential for the maintenance of critical societal and economic activities, is higher than for digital service providers. Therefore, the security requirements for digital service providers should be lighter. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems. Because of their cross-border nature, digital service providers should be subject to a more harmonised approach at Union level. Implementing acts should facilitate the specification and implementation of such measures.

(50) While hardware manufacturers and software developers are not operators of essential services, nor are they digital service providers, their products enhance the security of network and information systems. Therefore, they play an important role in enabling operators of essential services and digital service providers to secure their network and information systems. Such hardware and software products are already subject to existing rules on product liability.

(51) Technical and organisational measures imposed on operators of essential services and digital service providers should not require a particular commercial information and communications technology product to be designed, developed or manufactured in a particular manner.

(52) Operators of essential services and digital service providers should ensure the security of the network and information systems which they use. These are primarily private network and information systems managed by their internal IT staff or the security of which has been outsourced. The security and notification requirements should apply to the relevant operators of essential services and digital service providers regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

(53) To avoid imposing a disproportionate financial and administrative burden on operators of essential services and digital service providers, the requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. In the case of digital service providers, those requirements should not apply to micro- and small enterprises.

(54) Where public administrations in Member States use services offered by digital service providers, in particular cloud computing services, they might wish to require from the

providers of such services additional security measures beyond what digital service providers would normally offer in compliance with the requirements of this Directive. They should be able to do so by means of contractual obligations.

(55) The definitions of online marketplaces, online search engines and cloud computing services in this Directive are for the specific purpose of this Directive, and without prejudice to any other instruments.

(56) This Directive should not preclude Member States from adopting national measures requiring public-sector bodies to ensure specific security requirements when they contract cloud computing services. Any such national measures should apply to the public-sector body concerned and not to the cloud computing service provider.

(57) Given the fundamental differences between operators of essential services, in particular their direct link with physical infrastructure, and digital service providers, in particular their cross-border nature, this Directive should take a differentiated approach with respect to the level of harmonisation in relation to those two groups of entities. For operators of essential services, Member States should be able to identify the relevant operators and impose stricter requirements than those laid down in this Directive. Member States should not identify digital service providers, as this Directive should apply to all digital service providers within its scope. In addition, this Directive and the implementing acts adopted under it should ensure a high level of harmonisation for digital service providers with respect to security and notification requirements. This should enable digital service providers to be treated in a uniform way across the Union, in a manner proportionate to their nature and the degree of risk which they might face.

(58) This Directive should not preclude Member States from imposing security and notification requirements on entities that are not digital service providers within the scope of this Directive, without prejudice to Member States' obligations under Union law.

(59) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats against possible reputational and commercial damage for the operators of essential services and digital service providers reporting incidents. In the implementation of the notification obligations, competent authorities and the CSIRTs should pay particular attention to the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixes.

(60) Digital service providers should be subject to light-touch and reactive *ex post* supervisory activities justified by the nature of their services and operations. The competent authority concerned should therefore only take action when provided with evidence, for example by the digital service provider itself, by another competent authority, including a competent authority of another Member State, or by a user of the service, that a digital service provider is not complying with the requirements of this Directive, in particular following the occurrence of an incident. The competent authority should therefore have no general obligation to supervise digital service providers.

(61) Competent authorities should have the necessary means to perform their duties, including powers to obtain sufficient information in order to assess the level of security of network and information systems.

(62) Incidents may be the result of criminal activities the prevention, investigation and prosecution of which is supported by coordination and cooperation between operators of essential services, digital service providers, competent authorities and law enforcement authorities. Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage operators of essential services and digital service providers to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the European Cybercrime Centre (EC3) and ENISA.

(63) 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 any personal data breaches resulting from incidents.

(64) Jurisdiction in respect of digital service providers should be attributed to the Member State in which the digital service provider concerned has its main establishment in the Union, which in principle corresponds to the place where the provider has its head office in the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect. This criterion should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not criteria for determining the main establishment.

(65) Where a digital service provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such a digital service provider is offering services within the Union, it should be ascertained whether it is apparent that the digital service provider is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the digital service provider's or an intermediary's website or of an email address and of other contact details, or the use of a language generally used in the third country where the digital service provider is established, is insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the digital service provider is planning to offer services within the Union. The representative should act on behalf of the digital service provider and it should be possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a written mandate of the digital service

provider to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting.

(66) 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 so as to ensure a high level of security of network and information systems at Union level. ENISA should assist Member States through advice and guidelines. To this end, it might be helpful to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council[(8)].

(67) Entities falling outside the scope of this Directive may experience incidents having a significant impact on the services they provide. Where those entities consider that it is in the public interest to notify the occurrence of such incidents, they should be able to do so on a voluntary basis. Such notifications should be processed by the competent authority or the CSIRT where such processing does not constitute a disproportionate or undue burden on the Member States concerned.

(68) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission to lay down the procedural arrangements necessary for the functioning of the Cooperation Group and the security and notification requirements applicable to digital service providers. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[(9)]. When adopting implementing acts related to the procedural arrangements necessary for the functioning of the Cooperation Group, the Commission should take the utmost account of the opinion of ENISA.

(69) When adopting implementing acts on the security requirements for digital service providers, the Commission should take the utmost account of the opinion of ENISA and should consult interested stakeholders. Moreover, the Commission is encouraged to take into account the following examples: as regards security of systems and facilities: physical and environmental security, security of supplies, access control to network and information systems and integrity of network and information systems; as regards incident handling: incident-handling procedures, incident detection capability, incident reporting and communication; as regards business continuity management: service continuity strategy and contingency plans, disaster recovery capabilities; and as regards monitoring, auditing and testing: monitoring and logging policies, exercise contingency plans, network and information systems testing, security assessments and compliance monitoring.

(70) In the implementation of this Directive, the Commission should liaise as appropriate with relevant sectoral committees and relevant bodies set up at Union level in the fields covered by this Directive.

(71) The Commission should periodically review this Directive, in consultation with interested stakeholders, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.

(72) The sharing of information on risks and incidents within the Cooperation Group and the CSIRTs network and the compliance with the requirements to notify incidents to the national competent authorities or the CSIRTs might require processing of personal data. Such processing should comply with Directive 95/46/EC of the European Parliament and the Council[(10)] and Regulation (EC) No 45/2001 of the European Parliament and of the Council[(11)]. In the application of this Directive, Regulation (EC) No 1049/2001 of the European Parliament and of the Council[(12)] should apply as appropriate.

(73) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 14 June 2013[(13)].

(74) Since the objective of this Directive, namely to achieve a high common level of security of network and information systems in the Union, cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(75) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles,

HAVE ADOPTED THIS DIRECTIVE:

(**1**) OJ C 271, 19.9.2013, p. 133.

(**2**) Position of the European Parliament of 13 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 17 May 2016 (not yet published in the Official Journal). Position of the European Parliament of 6 July 2016 (not yet published in the Official Journal).

(**3**) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p. 33).

(**4**) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

(**5**) Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

(**6**) OJ C 352, 7.10.2014, p. 4.

(**7**) Regulation (EU) No 526/2013 of the European Parliament and the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (OJ L 165, 18.6.2013, p. 41).

(**8**) Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

(**9**) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(**10**) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

(**11**) 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 (OJ L 8, 12.1.2001, p. 1).

(**12**) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

(**13**) OJ C 32, 4.2.2014, p. 19.