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

Status: *EU Directives are being published on this site to aid cross referencing from UK legislation. After exit day no further amendments will be applied to this version.*

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

Status: *EU Directives are being published on this site to aid cross referencing from UK legislation. After exit day no further amendments will be applied to this version.*

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