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

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1 This 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.

2 To that end, this Directive:

- a lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;
- b creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;
- c creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;
- d establishes security and notification requirements for operators of essential services and for digital service providers;
- e lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

3 The security and notification requirements provided for in this Directive shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC, or to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.

4 This Directive applies without prejudice to Council Directive 2008/114/EC[(1)] and Directives 2011/93/EU[(2)] and 2013/40/EU[(3)] of the European Parliament and of the Council.

5 Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where such exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of such exchange. Such exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of operators of essential services and digital service providers.

6 This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential

interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.

7 Where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply.

Article 2

Processing of personal data

1 Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC.

2 Processing of personal data by Union institutions and bodies pursuant to this Directive shall be carried out in accordance with Regulation (EC) No 45/2001.

Article 3

Minimum harmonisation

Without prejudice to Article 16(10) and to their obligations under Union law, Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems.

Article 4

Definitions

For the purposes of this Directive, the following definitions apply:

(1) ‘network and information system’ means:

(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(2) ‘security of network and information systems’ means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

(3) 'national strategy on the security of network and information systems' means a framework providing strategic objectives and priorities on the security of network and information systems at national level;

(4) 'operator of essential services' means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2);

(5) 'digital service' means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[(4)] which is of a type listed in Annex III;

(6) 'digital service provider' means any legal person that provides a digital service;

(7) 'incident' means any event having an actual adverse effect on the security of network and information systems;

(8) 'incident handling' means all procedures supporting the detection, analysis and containment of an incident and the response thereto;

(9) 'risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;

(10) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of a digital service provider not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that digital service provider under this Directive;

(11) 'standard' means a standard within the meaning of point (1) of Article 2 of Regulation (EU) No 1025/2012;

(12) 'specification' means a technical specification within the meaning of point (4) of Article 2 of Regulation (EU) No 1025/2012;

(13) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

(14) 'domain name system (DNS)' means a hierarchical distributed naming system in a network which refers queries for domain names;

(15) 'DNS service provider' means an entity which provides DNS services on the internet;

(16) 'top-level domain name registry' means an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD);

(17) 'online marketplace' means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council[(5)] to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;

(18) 'online search engine' means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query

on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;

(19) 'cloud computing service' means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

Article 5

Identification of operators of essential services

1 By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.

2 The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:

a an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

b the provision of that service depends on network and information systems; and

c an incident would have significant disruptive effects on the provision of that service.

3 For the purposes of paragraph 1, each Member State shall establish a list of the services referred to in point (a) of paragraph 2.

4 For the purposes of paragraph 1, where an entity provides a service as referred to in point (a) of paragraph 2 in two or more Member States, those Member States shall engage in consultation with each other. That consultation shall take place before a decision on identification is taken.

5 Member States shall, on a regular basis, and at least every two years after 9 May 2018, review and, where appropriate, update the list of identified operators of essential services.

6 The role of the Cooperation Group shall be, in accordance with the tasks referred to in Article 11, to support Member States in taking a consistent approach in the process of identification of operators of essential services.

7 For the purpose of the review referred to in Article 23 and by 9 November 2018, and every two years thereafter, Member States shall submit to the Commission the information necessary to enable the Commission to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services. That information shall include at least:

a national measures allowing for the identification of operators of essential services;

b the list of services referred to in paragraph 3;

c the number of operators of essential services identified for each sector referred to in Annex II and an indication of their importance in relation to that sector;

d thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service as referred to in point (a) of Article 6(1) or to the importance of that particular operator of essential services as referred to in point (f) of Article 6(1).

In order to contribute to the provision of comparable information, the Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical guidelines on parameters for the information referred to in this paragraph.

Article 6

Significant disruptive effect

1 When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following cross-sectoral factors:

a the number of users relying on the service provided by the entity concerned;

b the dependency of other sectors referred to in Annex II on the service provided by that entity;

c the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;

d the market share of that entity;

e the geographic spread with regard to the area that could be affected by an incident;

f the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

2 In order to determine whether an incident would have a significant disruptive effect, Member States shall also, where appropriate, take into account sector-specific factors.

(**1**) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

(**2**) Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

(**3**) Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

(**4**) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(**5**) Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) (OJ L 165, 18.6.2013, p. 63).