

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 V

SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF DIGITAL SERVICE PROVIDERS

Article 16

Security requirements and incident notification

1 Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

- a the security of systems and facilities;
- b incident handling;
- c business continuity management;
- d monitoring, auditing and testing;
- e compliance with international standards.

2 Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services.

3 Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.

4 In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:

- a the number of users affected by the incident, in particular users relying on the service for the provision of their own services;
- b the duration of the incident;
- c the geographical spread with regard to the area affected by the incident;
- d the extent of the disruption of the functioning of the service;
- e the extent of the impact on economic and societal activities.

The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.

Status: EU Directives are being published on this site to aid cross referencing from UK legislation. After IP completion day (31 December 2020 11pm) no further amendments will be applied to this version.

5 Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.

6 Where appropriate, and in particular if the incident referred to in paragraph 3 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law, or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.

7 After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

8 The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2) by 9 August 2017.

9 The Commission may adopt implementing acts laying down the formats and procedures applicable to notification requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

10 Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers.

11 Chapter V shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC⁽¹⁾.

Article 17

Implementation and enforcement

1 Member States shall ensure that the competent authorities take action, if necessary, through *ex post* supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. Such evidence may be submitted by a competent authority of another Member State where the service is provided.

2 For the purposes of paragraph 1, the competent authorities shall have the necessary powers and means to require digital service providers to:

- a provide the information necessary to assess the security of their network and information systems, including documented security policies;
- b remedy any failure to meet the requirements laid down in Article 16.

3 If a digital service provider has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and the competent authorities of those other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between the competent authorities concerned and requests to take the supervisory measures referred to in paragraph 2.

Article 18

Jurisdiction and territoriality

1 For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in that Member State.

2 A digital service provider that is not established in the Union, but offers services referred to in Annex III within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established.

3 The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.

Status: EU Directives are being published on this site to aid cross referencing from UK legislation. After IP completion day (31 December 2020 11pm) no further amendments will be applied to this version.

- (1) Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises ([OJ L 124, 20.5.2003, p. 36](#)).