Roinn Cumarsáide, Gníomhaithe
ar son na hAeráide & Comhshaoil
Department of Communications,
Climate Action & Environment

Information Note for Digital Service Providers

1. Introduction

European Union Directive 2016/1148, concerning measures for a high common level of security of network and information systems (NIS Directive), was adopted by the European Parliament on the 6th of July 2016 and entered into force in August 2016. It is the first piece of EU-wide legislation on cybersecurity and provides legal measures to boost the overall level of cybersecurity in the EU.

It places a number of significant responsibilities on the State and on businesses in respect of cyber security. These responsibilities are wide ranging, but inter alia:

- Involve the application of a set of binding security obligations to a wide range of critical infrastructure operators, i.e. operators of essential services including the energy, transport, banking, financial market infrastructures, health, drinking water supply and digital infrastructure sectors;
- Require the State to apply and police a new regulatory regime on so called Digital Service Providers (DSPs);
- Give the State responsibility for dealing with the security of services provided by multinational companies across the European Union that have their European headquarters located in Ireland. The majority of these multinational companies are from the United States.

The aim of this information note is to assist Digital Service Providers in understanding their obligations in relation to compliance with the NIS Directive.

2. Definitions

A Digital Service Provider (DSP) is defined in the Directive as any legal person that provides a digital service and the types of digital services covered under its scope, as outlined in Annex 3 of the Directive, are as follows:

1. Online marketplaces
2. Online search engines
3. Cloud computing services

It is important to note that **micro and small enterprises** are **not** covered under the scope of the Directive as stated in Article 16(11). These are defined as the following:

- A small enterprise is an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.
- A microenterprise is an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

This means that any enterprise that employs fewer than 50 people and whose annual turnover and/or annual balance sheet total is less than EUR 10 million **does not** come under the scope of the Directive and as such should not consider themselves as a Digital Service Provider.

2.1 Online Marketplaces

An online marketplace is a platform which allows consumers and traders to conclude online sales or service contracts with traders, and is the final destination for the conclusion of those contracts.

Important points to note

- Online services that serve only as an intermediary to third-party services through which a contract can ultimately be concluded are not covered within the scope of the Directive. Therefore it does not include price comparison sites which compare the price of a particular product or service from different traders, but then redirects the user to the preferred trader to conduct the actual transaction. Also not covered under the scope are sites which only serve to connect buyers and sellers to trade with each other, e.g. classified advert sites, and sites which only sell products or services that they themselves own e.g. online retailers.
- 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.

2.2 Online Search Engines

An online search engine allows the user to perform searches of, in principle, all websites on the basis of a query on any subject or which are focused on websites in a particular language.

Important points to note

- It does 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.
- Additionally, and in line with the definition of online marketplaces above, it does not cover price comparison sites.

2.3 Cloud Computing Services

A cloud computing service means a digital service that enables access to a scalable and elastic pool of shareable computing resources. These services span a wide range of activities that can be delivered according to different models.

Important points to note

- The term ‘scalable’ refers to the ability of users to increase their computing resources according to their needs as their business fluctuates, irrespective of the geographical location of those resources.
- The term ‘elastic pool’ is used to describe the ability of users to shift and pool resources so that data needs can be kept in sync with resource availability.
- 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.

Note on Telecom Providers and Trust Service Providers

Article 1 (3) of the Directive states that the security and notification requirements provided for in the Directive do not apply to providers which are subject to the requirements of Article 13a and 13b of Directive 2002/21/EC or to trust providers which are subject to the requirements of Article 19 of Regulation (EU) No. 910/2014. Article 13a and 13b of Directive 2002/21/EC applies to undertakings providing public communications networks or publicly available electronic communications services.

Further clarification on this matter is provided in an annex to a communication from the Commission to the European Parliament and the Council. This communication states that if companies who fall into the above mentioned exemption also provide other services such as digital services (e.g. online marketplaces, online search engines or cloud computing services), then that company **will** be subject to the security and notification requirements of the NIS Directive for the provision of these particular services.

In summary, if an undertaking provides digital services as laid out in Annex 3 of the Directive (i.e. online marketplaces, online search engines or cloud computing services), they **are** subject to the security and notification requirements provided for in the NIS Directive, even if they are also subject to either the Article 13a and 13b of Directive 2002/21/EC or Article 19 of Regulation (EU) No. 910/2014. But only in respect to the digital services they provide.

3. Security Requirements and Incident Notification for Digital Service Providers

Chapter 5 of the Directive is of particular relevance to Digital Service Providers, especially Article 16 (1) and (4) which are outlined below.

3.1 Article 16 (1)

Under **Article 16(1)** of the Directive, Digital Service Providers must ensure that they;

- 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 respect of offering the three types of digital services covered under the Directive's scope and outlined above.
- 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

An Implementing Act (Commission Implementing Regulation (EU) 2018/151) was adopted on January 30th 2018 and provides rules that further specify elements and parameters for setting the security and notification requirements for Digital Service Providers. Article 2 of the Implementing Act states the following in this regard:

1. *"Security of systems and facilities referred to in point (a) of Article 16(1) of Directive (EU) 2016/1148 means the security of network and information systems and of their physical environment and shall include the following elements:*

- ***(a)*** *the systematic management of network and information systems which means a mapping of information systems and the establishment of a set of appropriate policies on managing information security, including risk analysis, human resources, security of operations, security architecture, secure data and system lifecycle management and where applicable, encryption and its management.*
- ***(b)*** *physical and environmental security which means the availability of a set of measures to protect the security of digital service providers' network and information systems from damage using an all hazards risk-based approach, addressing for instance system failure, human error, malicious action or natural phenomena*
- ***(c)*** *the security of supplies which means the establishment and maintenance of appropriate policies in order to ensure the accessibility and where applicable the traceability of critical supplies used in the provision of the services;*
- ***(d)*** *the access controls to network and information systems which means the availability of a set of measures to ensure that the physical and logical access to network and information systems, including administrative security of network and information systems, is authorized and restricted based on business and security requirements.*

2. *With regard to incident handling referred to in point (b) of Article 16(1) of Directive (EU) 2016/1148, the measures taken by the digital service provider shall include:*

- ***(a)*** *detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous events;*
- ***(b)*** *processes and policies on reporting incidents and identifying weaknesses and vulnerabilities in their information systems;*
- ***(c)*** *a response in accordance with established procedures and reporting the results of the measure taken;*

(d) *an assessment of the incident's severity, documenting knowledge from incident analysis and collection of relevant information which may serve as evidence and support a continuous improvement process.*

3. *Business continuity management referred to in point (c) of Article 16(1) of Directive (EU) 2016/1148 means the capability of an organisation to maintain or as appropriate restore the delivery of services at acceptable predefined levels following a disruptive incident and shall include:*

(a) *the establishment and the use of contingency plans based on a business impact analysis for ensuring the continuity of the services provided by digital service providers which shall be assessed and tested on a regular basis for example, through exercises;*

(b) *disaster recovery capabilities which shall be assessed and tested on a regular basis for example, through exercises.*

4. *The monitoring, auditing and testing referred to in point (d) of Article 16(1) of Directive (EU) 2016/1148 shall include the establishment and maintenance of policies on:*

(a) *the conducting of a planned sequence of observations or measurements to assess whether network and information systems are operating as intended;*

(b) *inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, and efficiency and effectiveness targets are being met;*

(c) *a process intended to reveal flaws in the security mechanisms of a network and information system that protect data and maintain functionality as intended. Such process shall include technical processes and personnel involved in the operation flow.*

5. *International standards referred to in point (e) of Article 16(1) of Directive (EU) 2016/1148 mean standards that are adopted by an international standardisation body as referred to in point (a) of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council2. Pursuant to Article 19 of Directive (EU) 2016/1148, European or internationally accepted standards and specifications relevant to the security of network and information systems, including existing national standards, may also be used.*

6. *Digital service providers shall ensure that they have adequate documentation available to enable the competent authority to verify compliance with the security elements set out in paragraphs 1, 2, 3, 4 and 5."*

3.2 Article 16(4)

Article 16 (4) outlines the parameters which shall be taken into account in determining how substantial the impact of an incident is. These are as follows:

(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 16(1).

Article 3 of the previously mentioned Implementing Act (Commission Implementing Regulation (EU) 2018/151) also gives further detail on the parameters outlined in 16(4) as follows:

1. *"With regard to the number of users affected by an incident, in particular users relying on the service for the provision of their own services referred to in point (a) of Article 16(4) of Directive (EU) 2016/1148, the digital service provider shall be in a position to estimate either of the following:*

(a) *the number of affected natural and legal persons with whom a contract for the provision of the service has been concluded; or*

(b) *the number of affected users having used the service based in particular on previous traffic data.*

2. *The duration of an incident referred to in point (b) of Article 16(4) means the time period from the disruption of the proper provision of the service in terms of availability, authenticity, integrity or confidentiality until the time of recovery.*

3. *As far as the geographical spread with regard to the area affected by the incident referred to in point (c) of Article 16(4) of Directive (EU) 2016/1148 is concerned, the digital service provider shall be in a position to identify whether the incident affects the provision of its services in specific Member States.*

4. *The extent of disruption of the functioning of the service referred to in point (d) of Article 16(4) of Directive (EU) 2016/1148 shall be measured as regards one or more of the following characteristics impaired by an incident: the availability, authenticity, integrity or confidentiality of data or related services.*

5. *With regard to the extent of the impact on economic and societal activities referred to in point (e) of Article 16(4) of Directive (EU) 2016/1148, the digital service provider shall be able to conclude, based on indications such as the nature of his contractual relations with the customer or, where appropriate, the potential number of affected users, whether the incident has caused significant material or non-material losses for the users such as in relation to health, safety or damage to property.*

6. *For the purpose of paragraph 1, 2, 3, 4 and 5, the digital service providers shall not be required to collect additional information to which they do not have access."*

Article 4 of Commission Implementing Regulation (EU) 2018/151 gives further information regarding what constitutes a substantial impact of an incident and states the following in this regard:

1. *"An incident shall be considered as having a substantial impact where at least one of the following situations has taken place:*

    (a) *The service provided by a digital service provider was unavailable for more than 5000 000 user hours whereby the term user hour refers to the number of affected users for a duration of sixty minutes;*

    (b) *The incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100 000 users in the Union;*

    (c) *The incident has created a risk for the public safety;*

    (d) *The incident has caused material damage to at least one user where the damage caused to that user exceeds EUR 1 000 000;*

    (e) *The incident has affected the provision of the services in two or more Member States.*

2. *Drawing on the best practice collected by the Cooperation Group in the exercise of its tasks under Article 11(3) of Directive (EU) 2016/1148 and on the discussions under point (m) of Article 11(3) thereof, the Commission may review the thresholds laid down in paragraph 1."*