STATUTORY INSTRUMENTS

2018 No. 506

The Network and Information Systems Regulations 2018

PART 4

Digital Services

Relevant digital service providers

12.—(1) A RDSP must identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems on which it relies to provide, within the European Union, the following services—

(a) online marketplace;

(b) online search engine; or

(c) cloud computing service.

(2) The measures taken by a RDSP under paragraph (1) must—

(a) (having regard to the state of the art) ensure a level of security of network and information systems appropriate to the risk posed;

(b) prevent and minimise the impact of incidents affecting their network and information systems with a view to ensuring the continuity of those services; and

(c) take into account the following elements as specified in Article 2 of EU Regulation 2018/151—

(i) the security of systems and facilities;

(ii) incident handling;

(iii) business continuity management;

(iv) monitoring auditing and testing; and

(v) compliance with international standards.

(3) A RDSP must notify the Information Commissioner about any incident having a substantial impact on the provision of any of the digital services mentioned in paragraph (1) that it provides.

(4) The requirement to notify in paragraph (3) applies only if the RDSP has access to information which enables it to assess whether the impact of an incident is substantial.

(5) The notification mentioned in paragraph (3) must provide the following information—

(a) the operator's name and the essential services it provides;

(b) the time the NIS incident occurred;

(c) the duration of the NIS incident;

(d) information concerning the nature and impact of the NIS incident;

(e) information concerning any, or any likely, cross-border impact of the NIS incident; and

(f) any other information that may be helpful to the competent authority.

(6) The notification under paragraph (3) must—

(a) be made without undue delay and in any event no later than 72 hours after the RDSP is aware that an incident has occurred; and

(b) contain sufficient information to enable the Information Commissioner to determine the significance of any cross-border impact.

(7) In order to determine whether the impact of an incident is substantial the RDSP must—

(a) take into account the following parameters, as specified in Article 3 of EU Regulation 2018/151—

(i) the number of users affected by the incident and, in particular, the users relying on the digital service for the provision of their own services;

(ii) the duration of the incident;

(iii) the geographical area affected by the incident;

(iv) the extent of the disruption to the functioning of the service;

(v) the extent of the impact on economic and societal activities; and

(b) assess whether at least one of situations described in Article 4 of EU Regulation 2018/151 has taken place.

(8) After receipt of a notification under paragraph (3) the Information Commissioner must share the incident notification with the CSIRT as soon as reasonably practicable.

(9) If an OES is reliant on a RDSP to provide an essential service, the operator must notify the relevant competent authority in relation to it about any significant impact on the continuity of the service it provides caused by an incident affecting the RDSP as soon as it occurs.

(10) If an incident notified under paragraph (3) affects two or more Member States, the Information Commissioner must inform the relevant authorities in each of the affected Member States about that incident as soon as reasonably practicable.

(11) The Information Commissioner is not required to share information under paragraph (9) if the information contains—

(a) confidential information; or

(b) information which may prejudice the security or commercial interests of a RDSP.

(12) If the Information Commissioner or CSIRT—

(a) consults with the RDSP responsible for an incident notification under paragraph (3), and

(b) is of the view that public awareness about that incident is necessary to prevent or manage it, or is in the public interest,

the Information Commissioner or CSIRT may inform the public about that incident or direct the RDSP responsible for the notification to do so.

(13) Before the Information Commissioner or CSIRT informs the public about an incident notified under paragraph (3), the Information Commissioner or CSIRT must consult each other and the RDSP who provided the notification.

(14) The Information Commissioner may inform the public about an incident affecting digital services in another Member State if—

(a) the relevant authorities in the affected Member State notify the Information Commissioner about the incident;

(b) the Commissioner consults with those relevant authorities; and

(c) the Commissioner is of the view mentioned in paragraph (11)(b).

(15) The Information Commissioner must provide an annual report to the SPOC identifying the number and nature of incidents notified to it under paragraph (3).

(16) The first report mentioned in paragraph (15) must be submitted on or before 1st July 2018 and subsequent reports must be submitted at annual intervals after that date.

(17) In this regulation "EU Regulation 2018/151" means Commission Implementing Regulation (EU) 2018/151 laying down rules for the application of Directive (EU) 2016/148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact(**1**).

(**1**) OJ No. L 26, 31.1.2018, p. 48.