STATUTORY INSTRUMENTS

2018 No. 506

The Network and Information Systems Regulations 2018

PART 3

Operators of essential services

Identification of operators of essential services

8.—(1) If a person provides an essential service of a kind referred to in paragraphs 1 to 9 of Schedule 2 and that service—

(a) relies on network and information systems; and

(b) satisfies a threshold requirement described for that kind of essential service,

that person is deemed to be designated as an OES for the subsector that is specified with respect to that essential service in that Schedule.

(2) A person who falls within paragraph (1) must notify the designated competent authority of that fact before the notification date.

(3) Even if a person does not meet the threshold requirement mentioned in paragraph (1)(b), a competent authority may designate that person as an OES for the subsector in relation to which that competent authority is designated under regulation 3(1), if the following conditions are met—

(a) that person provides an essential service of a kind specified in paragraphs 1 to 9 of Schedule 2 for the subsector in relation to which the competent authority is designated under regulation 3(1);

(b) the provision of that essential service by that person relies on network and information systems; and

(c) the competent authority concludes that an incident affecting the provision of that essential service by that person is likely to have significant disruptive effects on the provision of the essential service.

(4) In order to arrive at the conclusion mentioned in paragraph (3)(c), the competent authority must have regard to the following factors—

(a) the number of users relying on the service provided by the person;

(b) the degree of dependency of the other relevant sectors on the service provided by that person;

(c) the likely impact of incidents on the essential service provided by that person, in terms of its degree and duration, on economic and societal activities or public safety;

(d) the market share of the essential service provided by that person;

(e) the geographical area that may be affected if an incident impacts on the service provided by that person;

(f) the importance of the provision of the service by that person for maintaining a sufficient level of that service, taking into account the availability of alternative means of essential service provision;

(g) the likely consequences for national security if an incident impacts on the service provided by that person; and

(h) any other factor the competent authority considers appropriate to have regard to, in order to arrive at a conclusion under this paragraph.

(5) A competent authority must designate an OES under paragraph (3) by notice in writing served on the person who is to be designated and provide reasons for the designation in the notice.

(6) Before a competent authority designates a person as an OES under paragraph (3), the authority may—

(a) request information from that person under regulation 15(4); and

(b) invite the person to submit any written representations about the proposed decision to designate it as an OES.

(7) A competent authority must consult with the relevant authorities in another Member State before designating a person as an OES under paragraph (3) if that person already provides an essential service in that Member State.

(8) A competent authority must maintain a list of all the persons who are deemed to be designated under paragraph (1) or designated under paragraph (3) for the subsectors in relation to which that competent authority is designated under regulation 3(1).

(9) The competent authority must review the list mentioned in paragraph (8) at regular intervals and in accordance with paragraph (10).

(10) The first review under paragraph (9) must take place before 9th May 2020, and subsequent reviews must take place, at least, biennially.

(11) In this regulation the "notification" date means—

(a) 10th August 2018, in the case of a person who falls within paragraph (1) on the date these Regulations come into force; or

(b) in any other case, the date three months after the date on which the person falls within that paragraph.

Revocation

9.—(1) Even if a person satisfies the threshold mentioned in regulation 8(1)(b), a relevant competent authority may revoke the deemed designation of that person, by notice, if the authority concludes that an incident affecting the provision of that essential service by that person is not likely to have significant disruptive effects on the provision of the essential service.

(2) A competent authority may revoke a designation of a person under regulation 8(3), by notice, if the conditions mentioned in that regulation are no longer met by that person.

(3) Before revoking a deemed designation of a person under regulation 8(1), or a designation of a person under regulation 8(3), the competent authority must—

(a) serve a notice in writing of proposed revocation on that person;

(b) provide reasons for the proposed decision;

(c) invite that person to submit any written representations about the proposed decision within such time period as may be specified by the competent authority; and

(d) consider any representations submitted by the person under sub-paragraph (c) before a final decision is taken to revoke the designation.

(4) In order to arrive at the conclusion mentioned in paragraph (1), the competent authority must have regard to the factors mentioned in regulation 8(4).

(5) A competent authority may revoke a deemed designation under regulation 8(1), or a designation of a person under regulation 8(3), if the authority has received a request from another Member State to do so and the competent authority is in agreement that the designation of that person should be revoked.

The security duties of operators of essential services

10.—(1) An OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies.

(2) An OES must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

(3) The measures taken under paragraph (1) must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed.

(4) Operators of essential services must have regard to any relevant guidance issued by the relevant competent authority when carrying out their duties imposed by paragraphs (1) and (2).

The duty to notify incidents

11.—(1) An OES must notify the designated competent authority about any incident which has a significant impact on the continuity of the essential service which that OES provides ("a network and information systems ("NIS") incident").

(2) In order to determine the significance of the impact of an incident an OES must have regard to the following factors—

(a) the number of users affected by the disruption of the essential service;

(b) the duration of the incident; and

(c) the geographical area affected by the incident.

(3) The notification mentioned in paragraph (1) must—

(a) provide the following—

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

(ii) the time the NIS incident occurred;

(iii) the duration of the NIS incident;

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

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

(vi) any other information that may be helpful to the competent authority; and

(b) be provided to the competent authority—

(i) without undue delay and in any event no later than 72 hours after the operator is aware that a NIS incident has occurred; and

(ii) in such form and manner as the competent authority determines.

(4) The information to be provided by an OES under paragraph (3)(a) is limited to information which may reasonably be expected to be within the knowledge of that OES.

(5) After receipt of a notification under paragraph (1), the competent authority must—

(a) assess what further action, if any, is required in respect of that incident; and

(b) share the NIS incident information with the CSIRT as soon as reasonably practicable.

(6) After receipt of the NIS incident information under paragraph (5)(b), and based on that information, the CSIRT must inform the relevant authorities in a Member State if the incident has a significant impact on the continuity of an essential service provision in that Member State.

(7) After receipt of a notification under paragraph (1), the competent authority or CSIRT may inform—

(a) the OES who provided the notification about any relevant information that relates to the NIS incident, including how it has been followed up, in order to assist that operator to deal with that incident more effectively or prevent a future incident; and

(b) the public about the NIS incident, as soon as reasonably practicable, if the competent authority or CSIRT is of the view that public awareness is necessary in order to handle that incident or prevent a future incident.

(8) Before the competent authority or CSIRT informs the public about a NIS incident under paragraph (7)(b), the competent authority or CSIRT must consult each other and the OES who provided the notification under paragraph (1).

(9) The competent authority must provide an annual report to the SPOC identifying the number and nature of NIS incidents notified to it under paragraph (1).

(10) The first report mentioned in paragraph (9) must be submitted on or before 1st July 2018 and subsequent reports must be submitted at annual intervals.

(11) The CSIRT is not required to share information under paragraph (6) if the information contains—

(a) confidential information; or

(b) information which may prejudice the security or commercial interests of an OES.

(12) Operators of essential services must have regard to any relevant guidance issued by the relevant competent authority when carrying out their duties imposed by paragraphs (1) to (4).