
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 ^{F1}... 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.

[^{F2}(1A) Paragraph (1) does not apply to a network provider or service provider who is subject to the requirements of sections 105A to 105C of the Communications Act 2003 and in this paragraph “network provider” and “service provider” have the meanings given in section 105A(5) of that Act.]

(2) A person who falls within paragraph (1) must notify the designated competent authority [^{F3}in writing] of that fact before the notification date.

[^{F4}(2A) Each integrated care board is deemed to be designated as an OES for the healthcare settings subsector and, in relation to an integrated care board, any services provided by it (including the making of arrangements for the provision of services by others) are deemed to be essential services.]

(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 ^{F5}... 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;

Status: Point in time view as at 01/07/2022.

Changes to legislation: There are currently no known outstanding effects for the The Network and Information Systems Regulations 2018, PART 3. (See end of Document for details)

- (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—
- ^{F6}(a)
 - (b) invite the person to submit any written representations about the proposed decision to designate it as an OES.
- ^{F7}(7)
- ^{F8}(7A) If a person has reasonable grounds to believe that they no longer fall within paragraph (1) or that the conditions for designation under paragraph (3) are no longer met in relation to them, they must as soon as practicable notify the designated competent authority in writing and provide with that notification evidence supporting that belief.
- (7B) A competent authority that receives from a person a notification and supporting evidence referred to in paragraph (7A) must have regard to that notification and evidence in considering whether to revoke that person’s designation.]
- (8) A competent authority must maintain a list of all the persons who are deemed to be designated under paragraph (1) [^{F9}or (2A)] 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 [^{F10}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.

F1 Words in reg. 8(1) omitted (20.6.2018) by virtue of [The Network and Information Systems \(Amendment\) Regulations 2018 \(S.I. 2018/629\)](#), regs. 1, **2(5)**

F2 Reg. 8(1A) inserted (31.12.2020) by [The Network and Information Systems \(Amendment and Transitional Provision etc.\) Regulations 2020 \(S.I. 2020/1245\)](#), regs. 1(1), **5(a)** (with reg. 21)

F3 Words in reg. 8(2) inserted (31.12.2020) by [The Network and Information Systems \(Amendment and Transitional Provision etc.\) Regulations 2020 \(S.I. 2020/1245\)](#), regs. 1(1), **5(b)** (with reg. 21)

- F4** Reg. 8(2A) inserted (1.7.2022) by Health and Care Act 2022 (c. 31), s. 186(6), **Sch. 4 para. 237(2)**; S.I. 2022/734, reg. 2(a), Sch. (with regs. 13, 29, 30)
- F5** Words in reg. 8(3)(a) omitted (20.6.2018) by virtue of The Network and Information Systems (Amendment) Regulations 2018 (S.I. 2018/629), regs. 1, **2(5)**
- F6** Reg. 8(6)(a) and word omitted (31.12.2020) by virtue of The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **5(c)** (with reg. 21)
- F7** Reg. 8(7) omitted (20.1.2021) by virtue of The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), reg. 1(2), **Sch. para. 8**; 2020 c. 1, Sch. 5 para. 1(1)
- F8** Reg. 8(7A)(7B) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **5(d)** (with reg. 21)
- F9** Words in reg. 8(8) inserted (1.7.2022) by Health and Care Act 2022 (c. 31), s. 186(6), **Sch. 4 para. 237(3)**; S.I. 2022/734, reg. 2(a), Sch. (with regs. 13, 29, 30)
- F10** Words in reg. 8(11) substituted (20.6.2018) by The Network and Information Systems (Amendment) Regulations 2018 (S.I. 2018/629), regs. 1, **2(6)**

[F11] Nomination by an OES of a person to act on its behalf in the United Kingdom

8A.—(1) This regulation applies to any OES who has their head office outside the United Kingdom and—

- (a) provides an essential service of a kind referred to in one or more of paragraphs 1, 2, 3 and 10 of Schedule 2 (energy or digital infrastructure sector) within the United Kingdom; or
- (b) provides an essential service of a kind referred to in one or more of paragraphs 4 to 9 of Schedule 2 (transport, health or drinking water supply and distribution sector) within the United Kingdom and falls within paragraph (2).

(2) An OES falls within this paragraph if they have received a notice in writing from a designated competent authority for the OES requiring them to comply with this regulation.

(3) An OES to whom this regulation applies must—

- (a) nominate in writing a person in the United Kingdom with the authority to act on their behalf under these Regulations, including for the service of documents for the purposes of regulation 24 (a “nominated person”);
- (b) before the relevant date, notify the designated competent authority for the OES in writing of—
 - (i) their name;
 - (ii) the name and address of the nominated person; and
 - (iii) up-to-date contact details of the nominated person (including email addresses and telephone numbers).

(4) The OES must notify the designated competent authority for the OES of any changes to the information notified under paragraph (3)(b) as soon as practicable and in any event within seven days beginning with the day on which the change took effect.

(5) The designated competent authority for the OES and GCHQ may, for the purposes of carrying out their responsibilities under these Regulations, contact the nominated person instead of or in addition to the OES.

(6) A nomination under paragraph (3) is without prejudice to any legal action which could be initiated against the OES.

(7) In this regulation, “relevant date” means the date three months after—

- (a) the first day (including that day) on which the OES was deemed to be designated as an OES under regulation 8(1); or

Status: Point in time view as at 01/07/2022.

Changes to legislation: There are currently no known outstanding effects for the The Network and Information Systems Regulations 2018, PART 3. (See end of Document for details)

(b) the day (including that day) on which the OES was designated as an OES under regulation 8(3),
 unless the first day referred to in sub-paragraph (a) or the day referred to in sub-paragraph (b) was before 31st December 2020 in which case it means 31st March 2021.]

F11 Reg. 8A inserted (31.12.2020) by [The Network and Information Systems \(Amendment and Transitional Provision etc.\) Regulations 2020 \(S.I. 2020/1245\)](#), regs. 1(1), **6** (with reg. 21)

Revocation

9.—(1) Even if a person [^{F12}is deemed to be designated as an OES under regulation 8(1), the designated competent authority for the OES] may revoke the deemed designation [^{F13}, by notice in writing], 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) [^{F14}The designated competent authority for an OES may revoke the designation of that OES] under regulation 8(3), by notice [^{F15}in writing], if the conditions mentioned in that regulation are no longer met by that person.

(3) Before revoking a deemed designation of a person [^{F16}as an OES] under regulation 8(1), or a designation of a person [^{F16}as an OES] 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).

^{F17}(5)

F12 Words in reg. 9(1) substituted (31.12.2020) by [The Network and Information Systems \(Amendment and Transitional Provision etc.\) Regulations 2020 \(S.I. 2020/1245\)](#), regs. 1(1), **7(a)(i)** (with reg. 21)

F13 Words in reg. 9(1) substituted (31.12.2020) by [The Network and Information Systems \(Amendment and Transitional Provision etc.\) Regulations 2020 \(S.I. 2020/1245\)](#), regs. 1(1), **7(a)(ii)** (with reg. 21)

F14 Words in reg. 9(2) substituted (31.12.2020) by [The Network and Information Systems \(Amendment and Transitional Provision etc.\) Regulations 2020 \(S.I. 2020/1245\)](#), regs. 1(1), **7(b)(i)** (with reg. 21)

F15 Words in reg. 9(2) inserted (31.12.2020) by [The Network and Information Systems \(Amendment and Transitional Provision etc.\) Regulations 2020 \(S.I. 2020/1245\)](#), regs. 1(1), **7(b)(ii)** (with reg. 21)

F16 Words in reg. 9(3) inserted (31.12.2020) by [The Network and Information Systems \(Amendment and Transitional Provision etc.\) Regulations 2020 \(S.I. 2020/1245\)](#), regs. 1(1), **7(c)** (with reg. 21)

F17 Reg. 9(5) omitted (20.1.2021) by virtue of [The Network and Information Systems \(Amendment etc.\) \(EU Exit\) Regulations 2019 \(S.I. 2019/653\)](#), reg. 1(2), **Sch. para. 9**; 2020 c. 1, Sch. 5 para. 1(1)

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 [^{F18}for the OES in writing] 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.

[^{F19}(6) After receipt of the NIS incident information under paragraph (5)(b), and based on that information, the CSIRT may inform the relevant authorities in a Member State if the CSIRT considers that 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

Status: Point in time view as at 01/07/2022.

Changes to legislation: There are currently no known outstanding effects for the The Network and Information Systems Regulations 2018, PART 3. (See end of Document for details)

- (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).

F18 Words in reg. 11(1) inserted (31.12.2020) by [The Network and Information Systems \(Amendment and Transitional Provision etc.\) Regulations 2020 \(S.I. 2020/1245\)](#), regs. 1(1), **8** (with reg. 21)

F19 Reg. 11(6) substituted (20.1.2021) by [The Network and Information Systems \(Amendment etc.\) \(EU Exit\) Regulations 2019 \(S.I. 2019/653\)](#), reg. 1(2), **Sch. para. 10**; 2020 c. 1, Sch. 5 para. 1(1)

Status:

Point in time view as at 01/07/2022.

Changes to legislation:

There are currently no known outstanding effects for the The Network and Information Systems Regulations 2018, PART 3.