STATUTORY INSTRUMENTS

2018 No. 506

The Network and Information Systems Regulations 2018

PART 1

Introduction

Citation, commencement, interpretation and application

1.—(1) These Regulations may be cited as the Network and Information Systems Regulations 2018 and come into force on 10th May 2018.

(2) In these Regulations—

"cloud computing service" means a digital service that enables access to a scalable and elastic pool of shareable computing resources;

"the Commission" means the Commission of the European Union;

[[F1]"EU Regulation 2018/151" means Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 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;**]**

"Cooperation Group" means the group established under Article 11(1);

"CSIRTs network" means the network established under Article 12(1);

"digital service" means a service within the meaning of point (b) of Article 1(1) of Directive 2015/1535 which is of any the following kinds—

(a) online marketplace;

(b) online search engine;

(c) cloud computing service;

"digital service provider" means any person who provides a digital service;

"Directive 2013/11" means Directive 2013/11/EU of the European Parliament and of the Council on alternative dispute resolution for consumer disputes [M1], and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC, as amended from time to time;

"Directive 2015/1535" means Directive (EU) 2015/1535 of the European Parliament and of the Council laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [M2], as amended from time to time;

"Directive 2016/1148" means Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union [M3], as amended from time to time;

"Drinking Water Quality Regulator for Scotland" means the person appointed by the Scottish Ministers under section 7(1) of the Water Industry (Scotland) Act 2002 [M4];

"essential service" means a service which is essential for the maintenance of critical societal or economic activities;

[F2"First-tier Tribunal" has the meaning given by section 3(1) of the Tribunals, Courts and Enforcement Act 2007**]**;

"GCHQ" means the Government Communications Headquarters within the meaning of section 3 of the Intelligence Services Act 1994 M5;

"incident" means any event having an actual adverse effect on the security of network and information systems;

"network and information system" ("NIS") means—

(a) an electronic communications network within the meaning of section 32(1) of the Communications Act 2003 M6;

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under paragraph (a) or (b) for the purposes of their operation, use, protection and maintenance;

[F2"OES" ("operator of an essential service") means a person who is deemed to be designated as an operator of an essential service under regulation 8(1) **[**F3or (2A)**]** or is designated as an operator of an essential service under regulation 8(3);**]**

"online marketplace" means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11 to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;

"online search engine" means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;

F4…

"relevant law-enforcement authority" has the meaning given in section 63A(1A) of the Police and Criminal Evidence Act 1984 M7; and

[F5"representative" means any natural or legal person established in the United Kingdom who is able to act on behalf of a digital service provider established outside the United Kingdom with regard to its obligations under these Regulations; and**]**

"risk" means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems.

(3) In these Regulations a reference to—

[F6(a) an Article, Annex or paragraph of an Article or Annex is a reference to the Article, Annex or paragraph as numbered in Directive 2016/1148.**]**

(b) a numbered regulation, paragraph or Schedule is a reference to the regulation, paragraph or Schedule as numbered in these Regulations;

(c) "the relevant authorities in a Member State" is a reference to the designated single point of contact ("SPOC"), computer security incident response team ("CSIRT") **[**F7or**]** national competent authorities for that Member State;

(d) the "designated competent authority for **[**[F8]an OES**]**" is a reference to the competent authority that is designated under regulation 3(1) for the subsector in relation to which **[**[F9]that OES**]** provides an essential service;

(e) a "relevant digital service provider" ("RDSP") is a reference to a person who provides a digital service in the United Kingdom and satisfies the following conditions—

(i) the head office for that provider is in the United Kingdom or that provider has nominated a representative who is established in the United Kingdom;

(ii) the provider is not a micro or small enterprise as defined in Commission Recommendation 2003/361/EC [M8];

(f) the "NIS enforcement authorities" is a reference to the competent authorities designated under regulation 3(1) and the Information Commissioner;

(g) "security of network and information systems" means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

(4) Expressions and words used in these Regulations which are also used in Directive 2016/1148 have the same meaning as in Directive 2016/1148.

(5) Nothing in these Regulations prevents a person from taking an action (or not taking an action) which that person considers is necessary for the purposes of safeguarding the United Kingdom's essential State functions, in particular—

(a) safeguarding national security, including protecting information the disclosure of which the person considers is contrary to the essential interests of the United Kingdom's security; and

(b) maintaining law and order, in particular, to allow for the investigation, detection and prosecution of criminal offences [M9].

(6) These Regulations apply to—

(a) the United Kingdom, including its internal waters;

(b) the territorial sea adjacent to the United Kingdom;

(c) the sea (including the seabed and subsoil) in any area designated under section 1(7) of the Continental Shelf Act 1964 [M10].

Textual Amendments

F1 Words in reg. 1 inserted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), reg. 1(2), **Sch. para. 2**; 2020 c. 1, Sch. 5 para. 1(1)

F2 Words in reg. 1(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), **3(a)(i)** (with reg. 21)

F3 Words in reg. 1(2) inserted (1.7.2022) by Health and Care Act 2022 (c. 31), s. 186(6), **Sch. 4 para. 236**; S.I. 2022/734, reg. 2(a), Sch. (with regs. 13, 29, 30)

F4 Words in reg. 1(2) 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), **3(a)(ii)** (with reg. 21)

F5 Words in reg. 1(2) inserted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) (No. 2) Regulations 2019 (S.I. 2019/1444), regs. 1(2), **2(2)**; 2020 c. 1, Sch. 5 para. 1(1)

F6 Reg. 1(3)(a) substituted (20.6.2018) by The Network and Information Systems (Amendment) Regulations 2018 (S.I. 2018/629), regs. 1, **2(2)**

F7 Word in reg. 1(3)(c) substituted (20.6.2018) by The Network and Information Systems (Amendment) Regulations 2018 (S.I. 2018/629), regs. 1, **2(3)**

F8 Words in reg. 1(3)(d) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **3(b)(i)** (with reg. 21)

F9 Words in reg. 1(3)(d) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **3(b)(ii)** (with reg. 21)

Marginal Citations

M1 OJ No L 165, 18.6.2013, p63.

M2 OJ No L 241, 17.9.2015, p1.

M3 OJ No L 194, 19.7.2016, p1.

M4 2002 asp 3.

M5 1994 c.13. Section 3 was amended by section 251(1) and (2) of the Investigatory Powers Act 2016 (c. 25).

M6 2003 c.21. Section 32(1) was amended by regulation 2(1) of, and paragraphs 4 and 9(a) of Schedule 1 to, S.I. 2011/1210.

M7 1984 c.60. Section 63A(1A) and (1B) were substituted by section 81(2) of the Criminal Justice and Police Act 2001 (c.16). Subsection (1A) was amended by sections 117(5)(b) and 59 of, and paragraphs 43 and 46 of Schedule 4 to, the Serious and Organised Crime and Police Act 2005 (c. 15); and section 15(3) of, and paragraph 186 of Schedule 8 to, the Crime and Courts Act 2013 (c. 22).

M8 Commission Recommendation concerning the definition of micro, small and medium-sized enterprises (OJ No. L 124, 20.5.2003, p. 36).

M9 See Article 1(6) of Directive 2016/1148.

M10 1964 c. 29. Section 1(7) of the Continental Shelf Act 1964 was amended by section 37 of, and Schedule 3 to, the Oil and Gas (Enterprise) Act 1982 (c. 23), and section 103 of the Energy Act 2011 (c. 16).

PART 2

The National Framework

The NIS national strategy

2.—(1) A Minister of the Crown must designate and publish a strategy to provide strategic objectives and priorities on the security of network and information systems in the United Kingdom ("the NIS national strategy").

(2) The strategic objectives and priorities set out in the NIS national strategy must be aimed at achieving and maintaining a high level of security of network and information systems in—

(a) the sectors specified in column 1 of the table in Schedule 1 ("the relevant sectors"); and

(b) digital services.

(3) The NIS national strategy may be published in such form and manner as the Minister considers appropriate.

(4) The NIS national strategy may be reviewed by the Minister at any time and, if it is revised following such a review, the Minister must designate and publish a revised NIS national strategy as soon as reasonably practicable following that review.

(5) The NIS national strategy must, in particular, address the following matters—

(a) the regulatory measures and enforcement framework to secure the objectives and priorities of the strategy;

(b) the roles and responsibilities of the key persons responsible for implementing the strategy;

(c) the measures relating to preparedness, response and recovery, including cooperation between public and private sectors;

(d) education, awareness-raising and training programmes relating to the strategy;

(e) research and development plans relating to the strategy;

(f) a risk assessment plan identifying any risks; and

(g) a list of the persons involved in the implementation of the strategy.

F10(6) . . . . . .

(7) Before publishing the NIS national strategy F11..., the Minister may redact any part of it which relates to national security.

(8) In this regulation "a Minister of the Crown" has the same meaning as in section 8(1) of the Ministers of the Crown Act 1975 M11.

Textual Amendments

F10 Reg. 2(6) 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. 3(a)**; 2020 c. 1, Sch. 5 para. 1(1)

F11 Words in reg. 2(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. 3(b)**; 2020 c. 1, Sch. 5 para. 1(1)

Marginal Citations

M11 1975 c. 26.

Designation of national competent authorities

3.—(1) The person specified in column 3 of the table in Schedule 1 is designated as the competent authority, for the territorial jurisdiction indicated in that column, and for the subsector specified in column 2 of that table ("the designated competent authorities").

(2) The Information Commissioner is designated as the competent authority for the United Kingdom for RDSPs.

(3) In relation to the subsector for which it is designated under paragraph (1), the competent authority must—

(a) review the application of these Regulations;

(b) prepare and publish guidance;

(c) keep a list of all the operators of essential services who are designated, or deemed to be designated, under regulation 8 F12...;

(d) keep a list of all the revocations made under regulation 9;

(e) send a copy of the lists mentioned in sub-paragraphs (c) and (d) to GCHQ, as the SPOC designated under regulation 4, to enable it to prepare the report mentioned in regulation 4(3);

(f) consult and co-operate with the Information Commissioner when addressing incidents that result in breaches of personal data; and

(g) in order to fulfil the requirements of these Regulations, consult and co-operate with—

(i) relevant law-enforcement authorities;

F13(ii) . . . . . .

(iii) other competent authorities in the United Kingdom;

(iv) the SPOC that is designated under regulation 4; and

(v) the CSIRT that is designated under regulation 5.

[F14(3A) In relation to the subsector for which it is designated under paragraph (1), the competent authority may consult and co-operate with a public authority in the EU if it is in the interests of effective regulation of that subsector (whether inside or outside the United Kingdom).**]**

(4) In relation to digital services, the Information Commissioner must—

(a) review the application of these Regulations;

(b) prepare and publish guidance; and

(c) consult and co-operate with the persons mentioned in paragraph (3)(g), in order to fulfil the requirements of these Regulations.

(5) The guidance that is published F15... under paragraph (3)(b) or (4)(b) may be—

(a) published in such form and manner as the competent authority or Information Commissioner considers appropriate; and

(b) reviewed at any time, and if it is revised following such a review, the competent authority or Information Commissioner must publish revised guidance as soon as reasonably practicable.

(6) The competent authorities designated under paragraph (1) and the Information Commissioner must have regard to the national strategy that is published under regulation 2(1) when carrying out their duties under these Regulations.

Textual Amendments

F12 Words in reg. 3(3)(c) 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. 4(a)**; 2020 c. 1, Sch. 5 para. 1(1)

F13 Reg. 3(3)(g)(ii) 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. 4(b)**; 2020 c. 1, Sch. 5 para. 1(1)

F14 Reg. 3(3A) inserted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), reg. 1(2), **Sch. para. 4(c)**; 2020 c. 1, Sch. 5 para. 1(1)

F15 Word in reg. 3(5) omitted (20.6.2018) by virtue of The Network and Information Systems (Amendment) Regulations 2018 (S.I. 2018/629), regs. 1, **2(4)**

Designation of the single point of contact

4.—(1) GCHQ is designated as the SPOC on the security of network and information systems for the United Kingdom.

[F16(2) The SPOC may liaise with the relevant authorities in any Member State of the EU, the Cooperation Group and the CSIRTs network if it considers it appropriate.**]**

[F17(2A) The SPOC must—

(a) consult and co-operate, as it considers appropriate, with relevant law enforcement authorities;

(b) co-operate with the NIS enforcement authorities to enable the enforcement authorities to fulfil their obligations under these Regulations.**]**

(3) The SPOC **[**F18may, if it considers it appropriate to do so**]** submit reports to—

(a) the Cooperation Group based on the incident reports it received under regulation 11(9) and 12(15), including the number of notifications and the nature of notified incidents; and

(b) the Commission identifying the number of operators of essential services for each subsector listed in Schedule 2 [F19]....

[F20](4) . . . . . .

[F20](5) . . . . . .

Textual Amendments

F16 Reg. 4(2) 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. 5(a)**; 2020 c. 1, Sch. 5 para. 1(1)

F17 Reg. 4(2A) inserted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), reg. 1(2), **Sch. para. 5(b)**; 2020 c. 1, Sch. 5 para. 1(1)

F18 Words in reg. 4(3) 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. 5(c)(i)**; 2020 c. 1, Sch. 5 para. 1(1)

F19 Words in reg. 4(3)(b) 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. 5(c)(ii)**; 2020 c. 1, Sch. 5 para. 1(1)

F20 Reg. 4(4)(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. 5(d)**; 2020 c. 1, Sch. 5 para. 1(1)

Designation of computer security incident response team

5.—(1) GCHQ is designated as the CSIRT for the United Kingdom in respect of the relevant sectors and digital services.

(2) The CSIRT must—

(a) monitor incidents in the United Kingdom;

(b) provide early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

(c) respond to any incident notified to it under regulation 11(5)(b) or regulation 12(8);

(d) provide dynamic risk and incident analysis and situational awareness;

[F21](e) . . . . . .

(f) establish relationships with the private sector to facilitate co-operation with that sector;

(g) promote the adoption and use of common or standardised practices for—

(i) incident and risk handling procedures, and

(ii) incident, risk and information classification schemes; and

(h) co-operate with NIS enforcement authorities to enable the enforcement authorities to fulfil their obligations under these Regulations.

[[F22](3) The CSIRT may co-operate with or participate in international co-operation networks (including the CSIRTs network) if the CSIRT considers it appropriate to do so.**]**

Textual Amendments

F21 Reg. 5(2)(e) 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. 6(a)**; 2020 c. 1, Sch. 5 para. 1(1)

F22 Reg. 5(3) 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. 6(b)**; 2020 c. 1, Sch. 5 para. 1(1)

Information sharing – enforcement authorities

6.—(1) The NIS enforcement authorities may share information with **[**F23each other, relevant law-enforcement authorities,**]** the CSIRT, **[**F24and public authorities in the EU**]** if that information sharing is—

[F25(a) necessary for—

(i) the purposes of these Regulations or of facilitating the performance of any functions of a NIS enforcement authority under or by virtue of these Regulations or any other enactment;

(ii) national security purposes; or

(iii) purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution;**]**

(b) limited to information which is relevant and proportionate to the purpose of the information sharing.

[F26(1A) Information shared under paragraph (1) may not be further shared by the person with whom it is shared under that paragraph for any purpose other than a purpose mentioned in that paragraph unless otherwise agreed by the NIS enforcement authority.**]**

(2) When sharing information with **[**F27a public authority in the EU**]** under paragraph (1), the NIS enforcement authorities are not required to share—

(a) confidential information, or

(b) information which may prejudice the security or commercial interests of operators of essential services or digital service providers.

Textual Amendments

F23 Words in reg. 6(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), **4(a)(i)** (with reg. 21)

F24 Words in reg. 6(1) 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. 7(a)**; 2020 c. 1, Sch. 5 para. 1(1)

F25 Reg. 6(1)(a) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **4(a)(ii)** (with reg. 21)

F26 Reg. 6(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), **4(b)** (with reg. 21)

F27 Words in reg. 6(2) 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. 7(b)**; 2020 c. 1, Sch. 5 para. 1(1)

Information sharing – Northern Ireland

7.—(1) In order to facilitate the exercise of the Northern Ireland competent authority's functions under these Regulations—

(a) a Northern Ireland Department may share information with the Northern Ireland competent authority; and

(b) the Northern Ireland competent authority may share information with a Northern Ireland Department.

(2) In this regulation—

(a) "the Northern Ireland competent authority" means the competent authority that is specified for Northern Ireland in column 3 of the table in Schedule 1 in relation to the subsectors specified in column 2 of that table; and

(b) "a Northern Ireland Department" means a department mentioned in Schedule 1 to the Departments Act (Northern Ireland) 2016 [M12].

Marginal Citations

M12 2016 c. 5.

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 [F28]... 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.

[[F29](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 **[**[F30]in writing**]** of that fact before the notification date.

[[F31](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 [F32]... 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—

F33(a) . . . . . .

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

F34(7) . . . . . .

[F35(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) **[**F36or (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 **[**F37the "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.

Textual Amendments

F28 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)**

F29 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)

F30 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)

F31 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)

F32 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)**

F33 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)

F34 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)

F35 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)

F36 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)

F37 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)**

[F38Nomination 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

(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.**]**

Textual Amendments

F38 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 **[**F39is deemed to be designated as an OES under regulation 8(1), the designated competent authority for the OES**]** may revoke the deemed designation **[**F40, 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) **[**F41The designated competent authority for an OES may revoke the designation of that OES**]** under regulation 8(3), by notice **[**F42in writing**]**, if the conditions mentioned in that regulation are no longer met by that person.

(3) Before revoking a deemed designation of a person **[**F43as an OES**]** under regulation 8(1), or a designation of a person **[**F43as 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).

F44(5) . . . . . .

Textual Amendments

F39 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)

F40 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)

F41 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)

F42 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)

F43 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)

F44 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 **[**[F45]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.

[F46(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

(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).

Textual Amendments

F45 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)

F46 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)

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 **[**F47United Kingdom**]**, 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 **[**F48in writing**]** 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—

[F49(a) the RDSP's name and the digital services that it provides;**]**

(b) the time the F50... incident occurred;

(c) the duration of the F50... incident;

(d) information concerning the nature and impact of the F50... incident;

(e) information concerning any, or any likely, cross-border impact of the F50... incident; and

(f) any other information that may be helpful to the **[**F51Information Commissioner**]**.

(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 **[**F52first**]** 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

[F53(b) have regard to any relevant guidance published by the Information Commissioner.**]**

(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 **[**F54designated competent authority for the OES in writing**]** in relation to it about any significant impact on the continuity of the service it provides caused by an incident affecting the RDSP **[**F55without undue delay**]**.

F56(10) . . . . . .

(11) The Information Commissioner is not required to share information under **[**F57these Regulations**]** 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 **[**F58the Commissioner may**]** 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 **[**F59a Member State of the EU**]** 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 **[**F60paragraph (12)(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.

F61(17) . . . . . .

Textual Amendments

F47 Words in reg. 12(1) 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. 11(a)**; 2020 c. 1, Sch. 5 para. 1(1)

F48 Words in reg. 12(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), **9(a)** (with reg. 21)

F49 Reg. 12(5)(a) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **9(b)(i)** (with reg. 21)

F50 Word in reg. 12(5)(b)-(e) 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), **9(b)(ii)** (with reg. 21)

F51 Words in reg. 12(5)(f) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **9(b)(iii)** (with reg. 21)

F52 Word in reg. 12(6)(a) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **9(c)** (with reg. 21)

F53 Reg. 12(7)(b) substituted (12.1.2022) by The Network and Information Systems (EU Exit) (Amendment) Regulations 2021 (S.I. 2021/1461), regs. 1, **3(2)**

F54 Words in reg. 12(9) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **9(d)(i)** (with reg. 21)

F55 Words in reg. 12(9) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **9(d)(ii)** (with reg. 21)

F56 Reg. 12(10) 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. 11(b)** (as amended by S.I. 2019/1444, regs. 1(2), 4); 2020 c. 1, Sch. 5 para. 1(1)

F57 Words in reg. 12(11) 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. 11(c)**; 2020 c. 1, Sch. 5 para. 1(1)

F58 Words in reg. 12(12) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **9(e)** (with reg. 21)

F59 Words in reg. 12(14) 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. 11(d)**; 2020 c. 1, Sch. 5 para. 1(1)

F60 Words in reg. 12(14)(c) substituted (20.6.2018) by The Network and Information Systems (Amendment) Regulations 2018 (S.I. 2018/629), regs. 1, **2(7)(c)**

F61 Reg. 12(17) 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. 11(e)**; 2020 c. 1, Sch. 5 para. 1(1)

[F62Co-operation with the European Union

13. The Information Commissioner may give information and assistance to, and otherwise co-operate with, a public authority in the EU if the Information Commissioner considers that to do so would be in the interests of effective supervision of digital service providers (whether inside or outside the United Kingdom), including in the event of an incident notified under regulation 12(3).**]**

Textual Amendments

F62 Reg. 13 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. 12**; 2020 c. 1, Sch. 5 para. 1(1)

Registration with the Information Commissioner

14.—(1) The Information Commissioner must maintain a register of all RDSPs that have been notified to it.

(2) A RDSP must submit the following details to the Information Commissioner before the registration date for the purpose of maintaining the register mentioned in paragraph (1)—

(a) the name of the RDSP;

(b) the address of its head office, or of its nominated representative; and

(c) up-to-date contact details (including email addresses and telephone numbers).

(3) A RDSP must notify the Information Commissioner **[**[F63]in writing**]** about any changes to the details it submitted under paragraph (2) as soon as possible, and in any event within three months of the date on which the change took effect.

(4) In this regulation, the "registration date" means—

(a) 1st November 2018, in the case of a RDSP who satisfies the conditions mentioned in regulation 1(3)(e) on the coming into force date of these Regulations, or

(b) in any other case, the date three months after the RDSP satisfies those conditions.

Textual Amendments

F63 Words in reg. 14(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), **10** (with reg. 21)

[[F64]Representatives of digital service providers established outside the United Kingdom

14A.—(1) This regulation applies to any digital service provider which—

(a) has its head office outside the United Kingdom, but which offers digital services within the United Kingdom; and

(b) is not a small or micro enterprise as defined in Commission Recommendation 2003/361/EC.

(2) The digital service provider must—

(a) nominate in writing a representative in the United Kingdom; and

(b) notify the Information Commissioner of the name and contact details of that representative.

(3) The digital service provider must comply with paragraph (2)—

(a) in the case of a provider which is offering digital services within the United Kingdom on the coming into force date of these regulations, within three months of the date on which these regulations come into force; or

(b) in any other case, within three months of the provider first offering digital services in the United Kingdom.

(4) The Information Commissioner or GCHQ may contact the representative instead of or in addition to the digital service provider for the purposes of ensuring compliance with these Regulations.

(5) A nomination under paragraph (1) is without prejudice to any legal action which could be initiated against the nominating digital service provider.**]**

Textual Amendments

F64 Reg. 14A inserted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) (No. 2) Regulations 2019 (S.I. 2019/1444), regs. 1(2), **2(3)**; 2020 c. 1, Sch. 5 para. 1(1)

PART 5

Enforcement and penalties

Information notices

15.—(1) In order to assess whether a person should be an OES, a designated competent authority may serve an information notice **[**F65in writing**]** upon any person requiring that person to provide it with **[**F66all such information as**]** it reasonably requires to establish whether—

(a) a threshold requirement described in F67... Schedule 2 is met; or

(b) the conditions mentioned in regulation 8(3) are met.

(2) A designated competent authority may serve an information notice **[**F68in writing**]** upon an OES requiring **[**F69the OES**]** to provide it with **[**F70all such information as**]** it reasonably requires **[**F71for one or more of the following purposes**]**—

[F72(a) to assess the security of the OES's network and information systems;

(b) to establish whether there have been any events that the authority has reasonable grounds to believe have had, or could have, an adverse effect on the security of network and information systems and the nature and impact of those events;

(c) to identify any failure of the OES to comply with any duty set out in these Regulations;

(d) to assess the implementation of the OES's security policies, including from the results of any inspection conducted under regulation 16 and any underlying evidence in relation to such an inspection.**]**

(3) The Information Commissioner may serve upon a RDSP an information notice **[**F73in writing**]** requiring that RDSP to provide the Information Commissioner with **[**F74all such information as**]** the Information Commissioner reasonably requires **[**F75for one or more of the following purposes**]**—

[F76(a) to assess the security of the RDSP's network and information systems;

(b) to establish whether there have been any events that the Commissioner has reasonable grounds to believe have had, or could have, an adverse effect on the security of network and information systems and the nature and impact of those events;

(c) to identify any failure of the RDSP to comply with any duty set out in these Regulations;

(d) to assess the implementation of the RDSP's security policies, including from the results of any inspection conducted under regulation 16 and any underlying evidence in relation to such an inspection.**]**

F77(4) . . . . . .

(5) An information notice must—

(a) describe the information that is required by the designated competent authority or the Information Commissioner;

(b) provide the reasons for requesting such information;

(c) specify the form and manner in which the requested information is to be provided; and

(d) specify the time period within which the information must be provided.

[F78(5A) A person upon whom an information notice has been served under this regulation must comply with the requirements of the notice.**]**

(6) In a case falling within paragraph (1) the information notice may—

(a) be served by publishing it in such manner as the designated competent authority considers appropriate in order to bring it to the attention of any persons who are described in the notice as the persons from whom the information is required; and

(b) take the form of a general request for a certain category of persons to provide the information that is specified in the notice.

(7) A competent authority or the Information Commissioner may withdraw an information notice by written notice to the person on whom it was served.

(8) An information notice under paragraph (1) may not be served upon the SPOC or CSIRT.

Textual Amendments

F65 Words in reg. 15(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), **11(a)(i)** (with reg. 21)

F66 Words in reg. 15(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), **11(a)(ii)** (with reg. 21)

F67 Words in reg. 15(1)(a) omitted (20.6.2018) by virtue of The Network and Information Systems (Amendment) Regulations 2018 (S.I. 2018/629), regs. 1, **2(8)**

F68 Words in reg. 15(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), **11(b)(i)(aa)** (with reg. 21)

F69 Words in reg. 15(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), **11(b)(i)(bb)** (with reg. 21)

F70 Words in reg. 15(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), **11(b)(i)(cc)** (with reg. 21)

F71 Words in reg. 15(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), **11(b)(i)(dd)** (with reg. 21)

F72 Reg. 15(2)(a)-(d) substituted for reg. 15(2)(a)(b) (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **11(b)(ii)** (with reg. 21)

F73 Words in reg. 15(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), **11(c)(i)(aa)** (with reg. 21)

F74 Words in reg. 15(3) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **11(c)(i)(bb)** (with reg. 21)

F75 Words in reg. 15(3) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **11(c)(i)(cc)** (with reg. 21)

F76 Reg. 15(3)(a)-(d) substituted for reg. 15(3)(a)(b) (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **11(c)(ii)** (with reg. 21)

F77 Reg. 15(4) 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), **11(d)** (with reg. 21)

F78 Reg. 15(5A) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **11(e)** (with reg. 21)

Power of inspection

16.—(1) **[**F79The designated competent authority for an OES may—**]**

(a) conduct **[**F80all or any part of**]** an inspection;

(b) appoint a person to conduct **[**F81all or any part of**]** an inspection on its behalf; F82...

(c) direct the OES to appoint a person who is approved by that authority to conduct **[**F83all or any part of**]** an inspection on its behalf,

F84....

(2) The Information Commissioner may—

(a) conduct **[**F85all or any part of**]** an inspection;

(b) appoint a person to conduct **[**F86all or any part of**]** an inspection on its behalf; F87...

(c) direct that a RDSP appoint a person who is approved by the Information Commissioner to conduct **[**F88all or any part of**]** an inspection on its behalf,

F89....

(3) For the purposes of carrying out the inspection under paragraph (1) or (2), the OES or RDSP (as the case may be) must—

(a) pay the reasonable costs of the inspection **[**F90if so required by the relevant competent authority or the Information Commissioner**]**;

(b) co-operate with the **[**F91inspector**]**;

(c) provide the inspector with F92... access to their premises **[**F93in accordance with paragraph (5)(a)**]**;

[F94(d) allow the inspector to examine, print, copy or remove any document or information, and examine or remove any material or equipment, in accordance with paragraph (5)(d);**]**

(e) allow the inspector access to any person from whom the inspector seeks relevant information for the purposes of the inspection;

[F95(f) not intentionally obstruct an inspector performing their functions under these Regulations; and

(g) comply with any request made by, or requirement of, an inspector performing their functions under these Regulations.**]**

(4) The **[**F96relevant**]** competent authority or Information Commissioner may appoint a person to **[**F97conduct all or any part of**]** an inspection under paragraph (1)(b) or (2)(b) on its behalf on such terms and in such a manner as it considers appropriate.

[F98(5) An inspector may—

(a) at any reasonable time enter the premises of an OES or RDSP (except any premises used wholly or mainly as a private dwelling) if the inspector has reasonable grounds to believe that entry to those premises may be necessary or helpful for the purpose of the inspection;

(b) require an OES or RDSP to leave undisturbed and not to dispose of, render inaccessible or alter in any way any material, document, information, in whatever form and wherever it is held (including where it is held remotely), or equipment which is, or which the inspector

considers to be, relevant for such period as is, or as the inspector considers to be, necessary for the purposes of the inspection;

(c) require an OES or RDSP to produce and provide the inspector with access, for the purposes of the inspection, to any such material, document, information or equipment which is, or which the inspector considers to be, relevant to the inspection, either immediately or within such period as the inspector may specify;

(d) examine, print, copy or remove any document or information, and examine or remove any material or equipment (including for the purposes of printing or copying any document or information) which is, or which the inspector considers to be, relevant for such period as is, or as the inspector considers to be, necessary for the purposes of the inspection;

(e) take a statement or statements from any person;

(f) conduct, or direct the OES or RDSP to conduct, tests;

(g) take any other action that the inspector considers appropriate and reasonably required for the purposes of the inspection.

(6) The inspector must—

(a) produce proof of the inspector's identity if requested by any person present at the premises; and

(b) take appropriate and proportionate measures to ensure that any material, document, information or equipment removed in accordance with paragraph (5)(d) is kept secure from unauthorised access, interference and physical damage.

(7) Before exercising any power under paragraph (5)(b) to (d) or (g), the inspector—

(a) must take such measures as appear to the inspector appropriate and proportionate to ensure that the ability of the OES or RDSP, as the case may be, to comply with any duty set out in these Regulations will not be affected; and

(b) may consult such persons as appear to the inspector appropriate for the purpose of ascertaining the risks, if any, there may be in doing anything which the inspector proposes to do under that power.

(8) Where under paragraph (5)(d) an inspector removes any document, material or equipment, the inspector must provide, to the extent practicable, a notice giving—

(a) sufficient particulars of that document, material or equipment for it to be identifiable; and

(b) details of any procedures in relation to the handling or return of the document, material or equipment.

(9) In this regulation—

(a) a reference to a "test" is a reference to any process which is—

(i) employed to verify assertions about the security of a network or information system; and

(ii) based on interacting with that system, including components of that system,

and includes the exercising of any relevant security or resilience management process;

(b) "inspection" means any activity carried out (including any steps mentioned in paragraph (5)) for the purpose of—

(i) verifying compliance with the requirements of these Regulations; or

(ii) assessing or gathering evidence of potential or alleged failures to comply with the requirements of these Regulations,

including any necessary follow-up activity for either purpose;

(c) "inspector" means any person conducting all or any part of an inspection in accordance with paragraph (1) or (2).**]**

Textual Amendments

F79 Words in reg. 16(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), **12(a)(i)** (with reg. 21)

F80 Words in reg. 16(1)(a) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(a)(ii)** (with reg. 21)

F81 Words in reg. 16(1)(b) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(a)(ii)** (with reg. 21)

F82 Word in reg. 16(1) 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), **12(a)(iii)** (with reg. 21)

F83 Words in reg. 16(1)(c) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(a)(iv)** (with reg. 21)

F84 Words in reg. 16(1) 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), **12(a)(v)** (with reg. 21)

F85 Words in reg. 16(2)(a) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(b)(i)** (with reg. 21)

F86 Words in reg. 16(2)(b) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(b)(i)** (with reg. 21)

F87 Word in reg. 16(2) 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), **12(b)(ii)** (with reg. 21)

F88 Words in reg. 16(2)(c) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(b)(iii)** (with reg. 21)

F89 Words in reg. 16(2) 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), **12(b)(iv)** (with reg. 21)

F90 Words in reg. 16(3)(a) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(c)(i)** (with reg. 21)

F91 Word in reg. 16(3)(b) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(c)(ii)** (with reg. 21)

F92 Word in reg. 16(3)(c) 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), **12(c)(iii)(aa)** (with reg. 21)

F93 Words in reg. 16(3)(c) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(c)(iii)(bb)** (with reg. 21)

F94 Reg. 16(3)(d) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(c)(iv)** (with reg. 21)

F95 Reg. 16(3)(f)(g) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(c)(v)** (with reg. 21)

F96 Word in reg. 16(4) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(d)(i)** (with reg. 21)

F97 Words in reg. 16(4) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(d)(ii)** (with reg. 21)

F98 Reg. 16(5)-(9) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **12(e)** (with reg. 21)

Enforcement [F99notices] for breach of duties

17.—(1) **[**F100Subject to paragraph (2A),**]** the designated competent authority for an OES may serve an enforcement notice upon that OES if the F101... authority has reasonable grounds to believe that the OES has failed to—

[F102(za) notify it under regulation 8(2);

(zb) comply with the requirements stipulated in regulation 8A;**]**

(a) fulfil the security duties under regulation 10(1) and (2);

(b) notify a NIS incident under regulation 11(1);

(c) comply with the notification requirements stipulated in regulation 11(3);

(d) notify an incident as required by regulation 12(9);

(e) comply with an information notice issued under regulation 15; or

(f) comply with—

(i) a direction given under regulation 16(1)(c), or

(ii) the requirements stipulated in regulation 16(3).

(2) **[**F103Subject to paragraph (2A),**]** the Information Commissioner may serve an enforcement notice upon a RDSP if the Commissioner has reasonable grounds to believe that the RDSP has failed to—

(a) fulfil its duties under regulation 12(1) or (2);

(b) notify an incident under regulation 12(3);

(c) comply with the notification requirements stipulated in regulation 12(5);

(d) comply with a direction made by the Information Commissioner under regulation 12(12);

[F104(da) comply with the requirements stipulated in regulation 14A;**]**

(e) comply with an information notice issued under regulation 15; or

(f) comply with—

(i) a direction given under regulation 16(2)(c), or

(ii) the requirements stipulated in regulation 16(3).

[F105(2A) Before serving an enforcement notice under paragraph (1) or (2), the relevant competent authority or the Information Commissioner must inform the OES or RDSP, in such form and manner as it considers appropriate having regard to the facts and circumstances of the case, of—

(a) the alleged failure; and

(b) how and by when representations may be made in relation to the alleged failure and any related matters.

(2B) When the relevant competent authority or the Information Commissioner informs the OES or RDSP in accordance with paragraph (2A), it may also provide notice of its intention to serve an enforcement notice.

(2C) The relevant competent authority or the Information Commissioner may serve an enforcement notice on the OES or RDSP within a reasonable time, irrespective of whether it has provided any notice in accordance with paragraph (2B), having regard to the facts and circumstances of the case, after it has informed the OES or RDSP in accordance with paragraph (2A).

(2D) The relevant competent authority or the Information Commissioner must have regard to any representations made under paragraph (2A)(b).**]**

(3) An enforcement notice that is served under paragraph (1) or (2) must be in writing and must specify the following—

(a) the reasons for serving the notice;

(b) the alleged failure which is the subject of the notice; **[**F106and**]**

(c) what steps, if any, must be taken to rectify the alleged failure and the time period during which such steps must be taken; F107...

F107(d) . . . . . .

[F108(3A) An OES or RDSP upon whom an enforcement notice has been served under paragraph (1) or (2) must comply with the requirements, if any, of the notice regardless of whether the OES or RDSP has paid any penalty imposed on it under regulation 18.**]**

(4) If the relevant competent authority or Information Commissioner is satisfied that no further action is required, having considered—

(a) **[**F109any**]** representations submitted in accordance with paragraph **[**F110(2A)**]**; or

(b) any steps taken to rectify the alleged failure;

it must inform the OES or the RDSP, as the case may be, in writing, as soon as reasonably practicable.

(5) The OES or RDSP may request reasons for a decision to take no further action under paragraph (4) within 28 days of being informed of that decision.

(6) Upon receipt of a request under paragraph (5), the relevant competent authority or Information Commissioner must provide written reasons for a decision under paragraph (4) within a reasonable time and in any event no later than 28 days.

Textual Amendments

F99 Word in reg. 17 heading inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **13(a)** (with reg. 21)

F100 Words in reg. 17(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), **13(b)(i)(aa)** (with reg. 21)

F101 Word in reg. 17(1) 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), **13(b)(i)(bb)** (with reg. 21)

F102 Reg. 17(1)(za)(zb) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **13(b)(ii)** (with reg. 21)

F103 Words in reg. 17(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), **13(c)(i)** (with reg. 21)

F104 Reg. 17(2)(da) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **13(c)(ii)** (with reg. 21)

F105 Reg. 17(2A)-(2D) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **13(d)** (with reg. 21)

F106 Word in reg. 17(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), **13(e)(i)** (with reg. 21)

F107 Reg. 17(3)(d) 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), **13(e)(ii)** (with reg. 21)

F108 Reg. 17(3A) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **13(f)** (with reg. 21)

F109 Word in reg. 17(4)(a) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **13(g)(i)** (with reg. 21)

F110 Word in reg. 17(4)(a) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **13(g)(ii)** (with reg. 21)

Penalties

18.—**[**F111(1) The designated competent authority for an OES may serve a notice of intention to impose a penalty on the OES if it has reasonable grounds to believe that the OES has failed to comply with a duty referred to in regulation 17(1) or the duty set out in regulation 17(3A) and considers that a penalty is warranted having regard to the facts and circumstances of the case.

(2) The Information Commissioner may serve a notice of intention to impose a penalty on a RDSP if it has reasonable grounds to believe that the RDSP has failed to comply with a duty referred to in regulation 17(2) or the duty set out in regulation (3A) and considers that a penalty is warranted having regard to the facts and circumstances of the case.**]**

(3) A **[**F112notice of intention to impose a penalty**]** must be in writing and must specify the following—

(a) the reasons for imposing a penalty;

(b) the sum that is **[**F113intended**]** to be imposed as a penalty and how it is to be paid;

(c) the date on which the notice **[**F114of intention to impose a penalty**]** is given;

[F115(d) the period within which a penalty will be required to be paid if a penalty notice is served;

(e) that the payment of a penalty under a penalty notice (if any) is without prejudice to the requirements of any enforcement notice (if any); and

(f) how and when representations may be made about the content of the notice of intention to impose a penalty and any related matters.**]**

[F116(3A) The relevant competent authority may, after considering any representations submitted in accordance with paragraph (3)(f), serve a penalty notice on the OES with a final penalty decision if the authority is satisfied that a penalty is warranted having regard to the facts and circumstances of the case.

(3B) The Information Commissioner may, after considering any representations submitted in accordance with paragraph (3)(f), serve a penalty notice on the RDSP with a final penalty decision if the Commissioner is satisfied that a penalty is warranted having regard to the facts and circumstances of the case.

(3C) The relevant competent authority or the Information Commissioner may serve a notice of intention to impose a penalty or a penalty notice irrespective of whether it has served or is contemporaneously serving an enforcement notice on the OES or RDSP under regulation 17(1) or (2).

(3D) A penalty notice must—

(a) be given in writing to the OES or RDSP;

(b) include reasons for the final penalty decision;

(c) require the OES or RDSP to pay—

(i) the penalty specified in the notice of intention to impose a penalty; or

(ii) such penalty as the relevant competent authority or the Information Commissioner considers appropriate in the light of any representations made by the OES or RDSP and any steps taken by the OES or RDSP to rectify the failure or to do one or more of the things required by an enforcement notice under regulation 17(3);

(d) specify the period within which the penalty must be paid ("the payment period") and the date on which the payment period is to commence;

(e) provide details of the appeal process under regulation 19A; and

(f) specify the consequences of failing to make payment within the payment period.

(3E) It is the duty of the OES or RDSP to comply with any requirement imposed by a penalty notice.**]**

(4) A competent authority or the Information Commissioner may withdraw a penalty notice by informing the person upon whom it was served in writing.

(5) The sum **[**F117of any penalty imposed**]** under this regulation must be an amount that—

(a) the competent authority or Information Commissioner determines is appropriate and proportionate to the failure in respect of which it is imposed; and

(b) is in accordance with paragraph (6).

(6) The amount F118... must—

(a) not exceed £1,000,000 for any contravention which the **[**F119NIS**]** enforcement authority determines **[**F120was not a material contravention**]**;

F121(b) . . . . . .

(c) not exceed £8,500,000 for a material contravention which the **[**F122NIS**]** enforcement authority determines **[**F123does not meet the criteria set out in sub-paragraph (d)**]**; and

(d) not exceed £17,000,000 for a material contravention which the **[**F124NIS**]** enforcement authority determines **[**F125has or could have created a significant risk to, or significant impact on, or in relation to, the service provision by the OES or RDSP.**]**

(7) In this regulation—

[F126(a) "a material contravention" means—

(i) **[**F127a failure to take, or adequately take, one or more of the steps required under an enforcement notice within the period specified in that notice to rectify a failure described in one or more of—

(aa) sub-paragraphs (a) to (d) of regulation 17(1); or

(bb) sub- paragraphs (a) to (d) of regulation 17(2); or

(ii) where an enforcement notice was not served or where no steps were required to be taken under an enforcement notice, a failure described in one or more of—

(aa) sub-paragraphs (a) to (d) of regulation 17(1); or

(bb) sub-paragraphs (a) to (d) of regulation 17(2).**]]**

F128(b) . . . . . .

Textual Amendments

F111 Reg. 18(1)(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), **14(a)** (with reg. 21)

F112 Words in reg. 18(3) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(b)(i)** (with reg. 21)

F113 Word in reg. 18(3)(b) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(b)(ii)** (with reg. 21)

F114 Words in reg. 18(3)(c) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(b)(iii)** (with reg. 21)

F115 Reg. 18(3)(d)-(f) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(b)(iv)** (with reg. 21)

F116 Reg. 18(3A)-(3E) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(c)** (with reg. 21)
F117 Words in reg. 18(5) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(d)** (with reg. 21)
F118 Words in reg. 18(6) 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), **14(e)(i)** (with reg. 21)
F119 Word in reg. 18(6)(a) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(e)(ii)(aa)** (with reg. 21)
F120 Words in reg. 18(6)(a) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(e)(ii)(bb)** (with reg. 21)
F121 Reg. 18(6)(b) 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), **14(e)(iii)** (with reg. 21)
F122 Word in reg. 18(6)(c) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(e)(iv)(aa)** (with reg. 21)
F123 Words in reg. 18(6)(c) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(e)(iv)(bb)** (with reg. 21)
F124 Word in reg. 18(6)(d) inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(e)(v)(aa)** (with reg. 21)
F125 Words in reg. 18(6)(d) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(e)(v)(bb)** (with reg. 21)
F126 Reg. 18(7)(a) substituted (20.6.2018) by The Network and Information Systems (Amendment) Regulations 2018 (S.I. 2018/629), regs. 1, **2(9)(b)**
F127 Reg. 18(7)(a)(i)(ii) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **14(f)(i)** (with reg. 21)
F128 Reg. 18(7)(b) 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), **14(f)(ii)** (with reg. 21)

Independent review of designation decisions and penalty decisions

F129 19. . . . . . .

Textual Amendments
F129 Reg. 19 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), **15** (with reg. 21)

[F130 Appeal by an OES or RDSP to the First-tier Tribunal

19A.—(1) An OES may appeal to the First-tier Tribunal against one or more of the following decisions of the designated competent authority for the OES on one or more of the grounds specified in paragraph (3)—

(a) a decision under regulation 8(3) to designate that person as an OES;

(b) a decision under regulation 9(1) or (2) to revoke the designation of that OES;

(c) a decision under regulation 17(1) to serve an enforcement notice on that OES;

(d) a decision under regulation 18(3A) to serve a penalty notice on that OES.

(2) A RDSP may appeal to the First-Tier Tribunal against one or both of the following decisions of the Information Commissioner on one or more of the grounds specified in paragraph (3)—

(a) a decision under regulation 17(2) to serve an enforcement notice on that RDSP;

(b) a decision under regulation 18(3B) to serve a penalty notice on that RDSP.

(3) The grounds of appeal referred to in paragraphs (1) and (2) are—

(a) that the decision was based on a material error as to the facts;

(b) that any of the procedural requirements under these Regulations in relation to the decision have not been complied with and the interests of the OES or RDSP have been substantially prejudiced by the non-compliance;

(c) that the decision was wrong in law;

(d) that there was some other material irrationality, including unreasonableness or lack of proportionality, which has substantially prejudiced the interests of the OES or RDSP.**]**

Textual Amendments

F130 Regs. 19A-A20 inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **16** (with reg. 21)

[F130Decision of the First-tier Tribunal

19B.—(1) The First-tier Tribunal must determine the appeal after considering the grounds of appeal referred to in regulation 19A(3) and by applying the same principles as would be applied by a court on an application for judicial review.

(2) The Tribunal may, until it has determined the appeal in accordance with paragraph (1) and unless the appeal is withdrawn, suspend the effect of the whole or part of any of the following decisions to which the appeal relates—

(a) a decision under regulation 8(3) to designate a person as an OES;

(b) a decision under regulation 9(1) or (2) to revoke the designation of a person as an OES;

(c) a decision under regulation 17(1) to serve an enforcement notice;

(d) a decision under regulation 17(2) to serve an enforcement notice;

(e) a decision under regulation 18(3A) to serve a penalty notice; or

(f) a decision under regulation 18(3B) to serve a penalty notice.

(3) The Tribunal may—

(a) confirm any decision to which the appeal relates; or

(b) quash the whole or part of any decision to which the appeal relates.

(4) Where the Tribunal quashes the whole or part of a decision to which the appeal relates, it must remit the matter back to the designated competent authority for the OES or, as the case may be, the Information Commissioner, with a direction to that authority or the Commissioner to reconsider the matter and make a new decision having regard to the ruling of the Tribunal.

(5) The relevant competent authority or, as the case may be, the Information Commissioner, must have regard to a direction under paragraph (4).

(6) Where the relevant competent authority or, as the case may be, the Information Commissioner, makes a new decision in accordance with a direction under paragraph (4), that decision is to be considered final.**]**

Textual Amendments

F130 Regs. 19A-A20 inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **16** (with reg. 21)

[F130Enforcement by civil proceedings

A20.—(1) This regulation applies where—

(a) a designated competent authority for an OES has reasonable grounds to believe that the OES has failed to comply with the requirements of an enforcement notice as required by regulation 17(3A); or

(b) the Information Commissioner has reasonable grounds to believe that a RDSP has failed to comply with the requirements of an enforcement notice as required by regulation 17(3A).

(2) This regulation applies irrespective of whether the OES or RDSP has appealed to the First-tier Tribunal under regulation 19A.

(3) But where an OES or RDSP has appealed to the First-tier Tribunal under regulation 19A and the Tribunal has granted a suspension of the effect of the whole or part of the relevant decision under regulation 19B(2), the relevant competent authority or the Information Commissioner, as the case may be, may not bring or continue proceedings under this regulation in respect of that decision or that part of that decision for as long as the suspension has effect.

(4) Where paragraph (1)(a) applies, the relevant competent authority may commence civil proceedings against the OES—

(a) for an injunction to enforce the duty in regulation 17(3A);

(b) for specific performance of a statutory duty under section 45 of the Court of Session Act 1988; or

(c) for any other appropriate remedy or relief.

(5) Where paragraph (1)(b) applies, the Information Commissioner may commence civil proceedings against the RDSP—

(a) for an injunction to enforce the duty in regulation 17(3A);

(b) for specific performance of a statutory duty under section 45 of the Court of Session Act 1988; or

(c) for any other appropriate remedy or relief.

(6) No civil proceedings may be commenced under this regulation before the end of a period of 28 days beginning with the day on which the last relevant enforcement notice was served on the OES or, as the case may be, RDSP.

(7) In this regulation, a reference to civil proceedings is a reference to proceedings, other than proceedings in respect of an offence, before a civil court in the United Kingdom.**]**

Textual Amendments

F130 Regs. 19A-A20 inserted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **16** (with reg. 21)

Enforcement of penalty notices

20.—(1) This paragraph applies where a sum is payable to an enforcement authority as a penalty under regulation 18.

(2) In England and Wales the penalty is recoverable as if it were payable under an order of the county court or of the High Court.

(3) In Scotland the penalty may be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom.

(4) In Northern Ireland the penalty is recoverable as if it were payable under an order of a county court or of the High Court.

(5) Where action is taken under this paragraph for the recovery of a sum payable as a penalty under regulation 18, the penalty is —

(a) in relation to England and Wales, to be treated for the purposes of section 98 of the Courts Act 2003 [M13] (register of judgments and order etc.) as if it were a judgment entered in the county court;

(b) in relation to Northern Ireland, to be treated for the purposes of Article 116 of the Judgments Enforcement (Northern Ireland) Order 1981 [M14] (register of judgments) as if it were a judgment in respect of which an application has been accepted under Article 22 or 23(1) of that Order.

(6) No action may be taken under this paragraph for the recovery of a sum payable as a penalty under regulation 18 if **[**[F131]an appeal has been brought under regulation 19A and the appeal**]** has not been determined or withdrawn.

Textual Amendments

F131 Words in reg. 20(6) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **17** (with reg. 21)

Marginal Citations

M13 2003 c. 39. Section 98 was amended by sections 48(1) and 106(2) of, and paragraph 55(1), (2), (3)(a) and (b) of Schedule 8 and paragraph 15 of Schedule 16 to, the Tribunals, Courts and Enforcement Act 2007 (c. 15), and section 17(5) of, and paragraph 40(a) and (c) of Part 2 of Schedule 9 to, the Crime and Courts Act 2013 (c. 22). Further amendments made by the Tribunals, Courts and Enforcement Act 2007 have yet to be brought into force.

M14 S.I. 1981/226 (N.I. 6).

PART 6

Miscellaneous

Fees

21.—(1) A fee is payable by an OES or a RDSP to an enforcement authority, to recover the reasonable costs incurred by, or on behalf of, that authority in carrying out a NIS function in relation to that OES or RDSP.

(2) The fee mentioned in paragraph (1) must be paid to the enforcement authority within 30 days after receipt of the invoice sent by the authority.

(3) The invoice must state the work done and the reasonable costs incurred by, or on behalf of, the enforcement authority, including the time period to which the invoice relates.

(4) An enforcement authority may determine not to charge a fee under paragraph (1) in any particular case.

(5) A fee payable under this regulation is recoverable as a civil debt.

(6) In this regulation—

(a) a "NIS function" means a function that is carried out under these Regulations except any function under regulations 17(1) to (4) and 18 to 20; and

(b) "enforcement authority" has the same meaning as in regulation 18(7)(b).

Proceeds of penalties

22.—(1) The sum that is received by a NIS enforcement authority as a result of a penalty notice served under regulation 18 must be paid into the Consolidated Fund unless paragraph (2) applies.

(2) The sum that is received as a result of a penalty notice served under regulation 18 by—

(a) the Welsh Ministers must be paid into the Welsh Consolidated Fund established under section 117 of the Government of Wales Act 2006 [M15]; and

(b) the Scottish Ministers or the Drinking Water Quality Regulator for Scotland, must be paid into the Scottish Consolidated Fund established under section 64 of the Scotland Act 1998 [M16].

Marginal Citations

M15 2006 c. 32.

M16 1998 c. 46. Sub-section 2A of section 64 was inserted by section 16(1) and (2) of the Scotland Act 2016 (c. 11).

Enforcement action – general considerations

23.—(1) Before a NIS enforcement authority takes any action under regulation **[**[F132]17(1) or (2), 18(3A) or (3B) or A20,**]** the enforcement authority must consider whether it is reasonable and proportionate, on the facts and circumstances of the case, to take action in relation to the contravention.

(2) The NIS enforcement authority must, in particular, have regard to the following matters—

(a) any representations made by the OES or RDSP, as the case may be, about the contravention and the reasons for it, if any;

(b) any steps taken by the OES or RDSP to comply with the requirements set out in these Regulations;

(c) any steps taken by the OES or RDSP to rectify the contravention;

(d) whether the OES or RDSP had sufficient time to comply with the requirements set out in these Regulations; and

(e) whether the contravention is also liable to enforcement under another enactment.

Textual Amendments

F132 Words in reg. 23(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), **18** (with reg. 21)

Service of documents

24.—(1) Any document or notice required or authorised by these Regulations to be served on a person may be served by—

(a) delivering it to that person in person;

(b) leaving it at the person's proper address; or

(c) sending it by post or electronic means to that person's proper address.

(2) In the case of a body corporate, a document may be served on a director of that body.

(3) In the case of a partnership, a document may be served on a partner or person having control or management of the partnership business.

(4) If a person has specified an address in the United Kingdom (other than that person's proper address) at which that person or someone on that person's behalf will accept service, that address must also be treated as that person's proper address.

(5) For the purposes of this regulation "proper address" means—

(a) in the case of a body corporate or its director—

(i) the registered or principal office of that body; or

(ii) the email address of the secretary or clerk of that body;

(b) in the case of a partnership, a partner or person having control or management of the partnership business—

(i) the principal office of the partnership; or

(ii) the email address of a partner or a person having that control or management;

(c) in any other case, a person's last known address, which includes an email address.

(6) In this regulation, "partnership" includes a Scottish partnership.

Review and report

25.—(1) The Secretary of State must—

(a) carry out a review of the regulatory provision contained in these Regulations **[**F133and in EU Regulation 2018/151**]**; and

(b) publish a report setting out the conclusions of that review.

(2) The first report must be published on or before 9th May 2020 **[**F134, the second report must be published on or before 9th May 2022**]** and subsequent reports must be published at **[**F135intervals not exceeding five years**]**.

F136(3) . . . . . .

[F137(4) Section 30(4) of **[**F138the Small Business, Enterprise and Employment Act 2015**]** requires that reports published under this regulation must, in particular—

(a) set out the objectives intended to be achieved by the regulatory provision referred to in paragraph (1)(a);

(b) assess the extent to which those objectives are achieved;

(c) assess whether those objectives remain appropriate; and

(d) if those objectives remain appropriate, assess the extent to which they could be achieved in another way which involves less onerous regulatory provision.**]**

[F137(5) In this regulation "regulatory provision" has the same meaning as in sections 28 to 32 of that Act.**]**

Textual Amendments

F133 Words in reg. 25(1)(a) inserted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), reg. 1(2), **Sch. para. 13(a)**; 2020 c. 1, Sch. 5 para. 1(1)

F134 Words in reg. 25(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), **19(a)(i)** (with reg. 21)

F135 Words in reg. 25(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), **19(a)(ii)** (with reg. 21)

F136 Reg. 25(3) 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. 13(b)**; 2020 c. 1, Sch. 5 para. 1(1)

F137 Reg. 25(3)-(5) substituted (20.6.2018) by The Network and Information Systems (Amendment) Regulations 2018 (S.I. 2018/629), **reg. 2(11)**

F138 Words in reg. 25(4) substituted (31.12.2020) by The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (S.I. 2020/1245), regs. 1(1), **19(b)** (with reg. 21)

Department for Digital, Culture, Media and Sport

Matt Hancock
Secretary of State

We consent

Rebecca Harris
Paul Maynard
Two of the Lords Commissioners of Her Majesty's Treasury

Changes to legislation:
There are currently no known outstanding effects for the The Network and Information Systems Regulations 2018.