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;

"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(**1**), 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(**2**), 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(**3**), 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(**4**);

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

(**1**) OJ No L 165, 18.6.2013, p63.
(**2**) OJ No L 241, 17.9.2015, p1.
(**3**) OJ No L 194, 19.7.2016, p1.
(**4**) 2002 asp 3.

"GCHQ" means the Government Communications Headquarters within the meaning of section 3 of the Intelligence Services Act 1994(**5**);

"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(**6**);

(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;

"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;

"operator of an essential service" ("OES") means a person who is deemed to be designated as an operator of an essential service under regulation 8(1) or is designated as an operator of an essential service under regulation 8(3);

"relevant law-enforcement authority" has the meaning given in section 63A(1A) of the Police and Criminal Evidence Act 1984(**7**); 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—

(a) an Article, Annex, paragraph of an Article or Annex is a reference to the Article, Annex of 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") and national competent authorities for that Member State;

(d) the "designated competent authority for an operator of an essential service" is a reference to the competent authority that is designated under regulation 3(1) for the subsector in relation to which that operator 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—

(**5**) 1994 c.13. Section 3 was amended by section 251(1) and (2) of the Investigatory Powers Act 2016 (c. 25).
(**6**) 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.
(**7**) 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).

(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(**8**);

(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(**9**).

(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(**10**).

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.

(**8**) Commission Recommendation concerning the definition of micro, small and medium-sized enterprises (OJ No. L 124, 20.5.2003, p. 36).
(**9**) See Article 1(6) of Directive 2016/1148.
(**10**) 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).

(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.

(6) The Minister must communicate the NIS national strategy, including any revised NIS national strategy, to the Commission within three months after the date on which the strategy is designated under paragraph (1).

(7) Before publishing the NIS national strategy or communicating it to the Commission, 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(**11**).

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, including an indication of the importance of each operator in relation to the subsector in relation to which it provides an essential service;

(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;

(ii) competent authorities in other Member States;

(**11**) 1975 c. 26.

(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.

(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 by 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.

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.

(2) The SPOC must—

(a) liaise with the relevant authorities in other Member States, the Cooperation Group and the CSIRTs network to ensure cross-border co-operation;

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

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

(3) The SPOC must 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, indicating their importance in relation to that sector.

(4) The first report mentioned in paragraph (3)(a) must be submitted on or before 9th August 2018 and subsequent reports must be submitted at annual intervals.

(5) The first report mentioned in paragraph (3)(b) must be submitted on or before 9th November 2018 and subsequent reports must be submitted at biennial intervals.

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;

(e) participate and co-operate in the CSIRTs network;

(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.

(3) The CSIRT may participate in international co-operation networks if the CSIRT considers it appropriate to do so.

Information sharing – enforcement authorities

6.—(1) The NIS enforcement authorities may share information with the CSIRT, the Commission and the relevant authorities in other Member States if that information sharing is—

(a) necessary for the requirements of these Regulations, and

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

(2) When sharing information with the Commission or the relevant authorities in other Member States 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.

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(**12**).

(**12**) 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 paragraphs 1 to 9 of Schedule 2 and that service—

(a) relies on network and information systems; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Revocation

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

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

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

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

(b) provide reasons for the proposed decision;

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

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

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

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

The security duties of operators of essential services

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

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

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

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

The duty to notify incidents

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

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

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

(b) the duration of the incident; and

(c) the geographical area affected by the incident.

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

(a) provide the following—

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

(ii) the time the NIS incident occurred;

(iii) the duration of the NIS incident;

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

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

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

(b) be provided to the competent authority—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) confidential information; or

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

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

PART 4

Digital Services

Relevant digital service providers

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

(a) online marketplace;

(b) online search engine; or

(c) cloud computing service.

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

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

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

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

(i) the security of systems and facilities;

(ii) incident handling;

(iii) business continuity management;

(iv) monitoring auditing and testing; and

(v) compliance with international standards.

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

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

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

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

(b) the time the NIS incident occurred;

(c) the duration of the NIS incident;

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

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

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

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

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

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

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

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

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

(ii) the duration of the incident;

(iii) the geographical area affected by the incident;

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

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

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

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

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

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

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

(a) confidential information; or

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

(12) If the Information Commissioner or CSIRT—

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

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

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

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

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

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

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

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

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

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

(17) In this regulation "EU Regulation 2018/151" means Commission Implementing Regulation (EU) 2018/151 laying down rules for the application of Directive (EU) 2016/148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact(**13**).

Co-operation and action across Member State boundaries

13.—(1) The Information Commissioner must co-operate with, and assist, competent authorities in other Member States, if the Commissioner considers that is appropriate to secure the effective supervision of—

(a) RDSPs who have network and information systems located in another Member State; or

(b) digital service providers who do not meet the condition mentioned in regulation 1(3)(e)(i) but have network and information systems located in the United Kingdom.

(2) The co-operation and assistance referred to in paragraph (1) may include—

(a) sharing information with, and receiving information from, a competent authority in another Member State to the extent that the Information Commissioner considers it necessary and appropriate;

(b) receiving a request from a competent authority in another Member State for the Information Commissioner to take enforcement action with respect to a RDSP mentioned in paragraph (1)(a); and

(c) making a request to a competent authority in another Member State for enforcement action to be taken with respect to a digital service provider mentioned in paragraph (1)(b).

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).

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

(3) A RDSP must notify the Information Commissioner 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.

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 upon any person requiring that person to provide it with information that it reasonably requires to establish whether—

(a) a threshold requirement described in paragraphs 1 to 9 of 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 upon an OES requiring that person to provide it with information that it reasonably requires to assess—

(a) the security of the OES's network and information systems; and

(b) the implementation of the operator's security policies, including any about inspections 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 requiring that RDSP to provide the Information Commissioner with information that the Information Commissioner reasonably requires to assess—

(a) the security of the RDSP's network and information systems; and

(b) the implementation of the RDSP's security policies, including any about inspections conducted under regulation 16 and any underlying evidence in relation to such an inspection.

(4) Before a person is to be designated as an OES under regulation 8(3), a designated competent authority may serve an information notice upon that person requiring the person to provide it with information in order to assess whether to designate it.

(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.

(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.

Power of inspection

16.—(1) A relevant competent authority in relation to an OES may—

(a) conduct an inspection;

(b) appoint a person to conduct an inspection on its behalf; or

(c) direct the OES to appoint a person who is approved by that authority to conduct an inspection on its behalf,

to assess if the OES has fulfilled the duties imposed on it by regulations 10 and 11.

(2) The Information Commissioner may—

(a) conduct an inspection;

(b) appoint a person to conduct an inspection on its behalf; or

(c) direct that a RDSP appoint a person who is approved by the Information Commissioner to conduct an inspection on its behalf,

to assess if a RDSP has fulfilled the requirements set out in regulation 12.

(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;

(b) co-operate with the person who is conducting the inspection ("the inspector");

(c) provide the inspector with reasonable access to their premises;

(d) allow the inspector to inspect, copy or remove such documents and information, including information that is held electronically, as the inspector considers to be relevant to the inspection; and

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

(4) The competent authority or Information Commissioner may appoint a person to carry out an inspection under paragraph (1)(b) or (2)(b) on its behalf on such terms and in such a manner as it considers appropriate.

Enforcement for breach of duties

17.—(1) The designated competent authority for an OES may serve an enforcement notice upon that OES if the competent authority has reasonable grounds to believe that the OES has failed to—

(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) 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);

(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).

(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;

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

(d) how and when representations may be made about the content of the notice and any related matters.

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

(a) the representations submitted in accordance with paragraph (3)(d); 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.

Penalties

18.—(1) The relevant competent authority for an OES may serve a penalty notice upon that OES if the OES was served with an enforcement notice under regulation 17(1) and the OES—

(a) was required to take steps to rectify a failure within a time period stipulated in the enforcement notice but the operator failed to take any steps or any adequate steps; or

(b) was not required to take steps to rectify a failure but the competent authority is not satisfied with the representations submitted by the OES in accordance with regulation 17(3)(d).

(2) The Information Commissioner may serve a penalty notice upon a RDSP if the RDSP was served with an enforcement notice under regulation 17(2) and the RDSP—

(a) was required to take steps to rectify a failure within a time period stipulated in the enforcement notice but the RDSP failed to take any steps or any adequate steps; or

(b) was not required to take steps to rectify a failure but the Information Commissioner is not satisfied with the representations submitted by the RDSP in accordance with regulation 17(3)(d).

(3) A penalty notice must be in writing and must specify the following—

(a) the reasons for imposing a penalty;

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

(c) the date on which the notice is given;

(d) the date, at least 30 days after the date specified in sub-paragraph (c), before which the penalty must be paid ("the payment period");

(e) details about the independent review process set up under regulation 19 and how the right to review may be exercised; and

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

(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 that is to be imposed under a penalty notice served 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 that is to be imposed under a penalty notice must—

(a) not exceed £1,000,000 for any contravention which the enforcement authority determines could not cause a NIS incident;

(b) not exceed £3,400,000 for a material contravention which the enforcement authority determines has caused, or could cause, an incident resulting in a reduction of service provision by the OES or RDSP for a significant period of time;

(c) not exceed £8,500,000 for a material contravention which the enforcement authority determines has caused, or could cause, an incident resulting in a disruption of service provision by the OES or RDSP for a significant period of time; and

(d) not exceed £17,000,000 for a material contravention which the enforcement authority determines has caused, or could cause, an incident resulting in an immediate threat to life or significant adverse impact on the United Kingdom economy.

(7) In this regulation—

(a) "a material contravention" means a failure to take steps, or any adequate steps, within the stipulated time period to rectify a failing that is described in regulation 17(1)(a) to (d) or (2)(a) to (e);

(b) "enforcement authority" means the designated competent authority for an OES or the Information Commissioner for RDSPs.

Independent review of designation decisions and penalty decisions

19.—(1) If an OES so requests, the relevant competent authority for an OES must appoint an independent person ("the reviewer") to conduct reviews of a designation or penalty decision made by that authority in relation to that OES.

(2) The Information Commissioner must appoint an independent person ("the reviewer") to conduct a review of a penalty decision made by the Commissioner in relation to an RDSP, if the RDSP requests a review to be conducted.

(3) An OES may request the reviewer to review a designation or penalty decision made in relation to that OES in order to challenge any of the following matters—

(a) the basis upon which the designation decision was made;

(b) the grounds for imposing a penalty notice;

(c) the sum that is imposed by way of a penalty notice;

(d) the time period within which the penalty notice must be paid.

(4) A RDSP may request the reviewer to conduct a review of a penalty decision made in relation to that RDSP in order to challenge any of the following matters—

(a) the grounds for imposing a penalty notice;

(b) the sum that is imposed by way of a penalty notice;

(c) the time period within which the penalty notice must be paid.

(5) Any request to conduct a review must—

(a) be made in writing, and copied to the relevant competent authority or the Information Commissioner, as the case may be;

(b) set out the reasons for requesting a review and provide any relevant evidence; and

(c) be made within 30 days of receipt of the designation decision or penalty decision.

(6) The relevant competent authority or the Information Commissioner must respond to a request, including to any reasons provided under regulation 19(5)(b), to conduct a review—

(a) in writing to the reviewer, copied to the person who made the request for a review; and

(b) within 30 days of receipt of that request.

(7) The reviewer may extend the time limits mentioned in paragraph (5)(c) or (6)(b) if the reviewer considers it necessary to do so in the interests of fairness and having regard to the facts and circumstances of the particular case.

(8) A request for a review suspends the effect of a designation decision or penalty decision until the review is decided or withdrawn.

(9) The reviewer must uphold or set aside a designation decision or a penalty decision after consideration of the following matters—

(a) the basis upon which the designation decision or penalty decision is challenged;

(b) the response submitted under paragraph (6); and

(c) any relevant evidence.

(10) The reviewer must provide reasons for the decision made under paragraph (9).

(11) In this regulation—

(a) "designation decision" means a decision to designate an operator of essential services made under regulation 8(3); and

(b) "penalty decision" means a decision to serve a penalty notice under regulation 18(1) or (2).

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(**14**) (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(**15**) (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 a review has been requested under regulation 19(3) or (4) and the review has not been determined or withdrawn.

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—

(**14**) 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.

(**15**) S.I. 1981/226 (N.I. 6).

(a) the Welsh Ministers must be paid into the Welsh Consolidated Fund established under section 117 of the Government of Wales Act 2006(**16**); 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(**17**).

Enforcement action – general considerations

23.—(1) Before a NIS enforcement authority takes any action under regulation 17 or 18 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.

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.

(**16**) 2006 c. 32.
(**17**) 1998 c. 46. Sub-section 2A of section 64 was inserted by section 16(1) and (2) of the Scotland Act 2016 (c. 11).

(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; 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 and subsequent reports must be published at biennial intervals.

(3) Section 30(3) of the Small Business, Enterprise and Employment Act 2016 requires that a review carried out under this regulation must, so far as is reasonable, have regard to how the 2015 Directive is implemented in other Member States.

(4) Section 30(4) of Small Business, Enterprise and Employment Act 2015(**18**) requires that the 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.

(5) In this regulation, "regulatory provision" has the same meaning as in sections 28 to 32 of the 2015 Act.

Matt Hancock
Secretary of State
Department for Digital, Culture, Media and Sport

19th April 2018

We consent

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

19th April 2018

(**18**) 2015 c. 26.