STATUTORY INSTRUMENTS

2018 No. 506

ELECTRONIC COMMUNICATIONS

The Network and Information Systems Regulations 2018

Made - - - -	*19th April 2018*
Laid before Parliament	*20th April 2018*
Coming into force - -	*10th May 2018*

The Secretary of State is a Minister designated [F1] for the purposes of section 2(2) of the European Communities Act 1972 [F2] ("the 1972 Act") in relation to electronic communications.

These Regulations make provision for a purpose mentioned in section 2(2) of the 1972 Act and it appears to the Secretary of State that it is expedient for certain references to provisions of EU instruments to be construed as references to those provisions as amended from time to time.

The Secretary of State makes the following Regulations in exercise of the powers conferred by section 2(2) of, and paragraph 1A [F3] of Schedule 2 to, the 1972 Act and by section 56 of the Finance Act 1973 [F4] ("the 1973 Act") and, in the case of section 56 of the 1973 Act, with the consent of the Treasury.

F1 S.I. 2001/3495. See article 2 of, and Schedule 1 to, these Regulations. There are amendments not relevant to these Regulations.

F2 1972 c.68. Section 2(2) was amended by section 27(1)(a) of the Legislative and Regulatory Reform Act 2006 (c.51) and by Part 1 of the Schedule to the European Union (Amendment) Act 2008 (c.7). In so far as these Regulations deal with matters that are within the devolved competence of Scottish Ministers, the power of the Secretary of State to make regulations in relation to those matters in or as regards Scotland is preserved by section 57(1) of the Scotland Act 1998 (c.46).

F3 Paragraph 1A of Schedule 2 was inserted by section 28 of the Legislative and Regulatory Reform Act 2006 and amended by Part 1 of the Schedule to the European Union (Amendment) Act 2008 and by article 3 of and paragraph 1 of Schedule 1 to SI 2007/1388.

F4 1973 c.51. Section 56 was amended by S.I. 2011/1043; there are other amendments not relevant to these Regulations.

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;

[[F5]"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 [F6], 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 [F7], 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 [F8], 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 [F9];

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

[[F10]"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 [F11];

"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 [F12];

(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;

[[F10]"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) 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;

[F13]…

"relevant law-enforcement authority" has the meaning given in section 63A(1A) of the Police and Criminal Evidence Act 1984 [F14]; and

[[F15]"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—

[[F16](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") **[**[F17]or**]** national competent authorities for that Member State;

(d) the "designated competent authority for **[**[F18]an OES**]**" is a reference to the competent authority that is designated under regulation 3(1) for the subsector in relation to which **[**[F19]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 [F20];

(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 [F21].

(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 [F22].

F5 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)

F6 OJ No L 165, 18.6.2013, p63.

F7 OJ No L 241, 17.9.2015, p1.

F8 OJ No L 194, 19.7.2016, p1.

F9 2002 asp 3.

F10 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)

F11 1994 c.13. Section 3 was amended by section 251(1) and (2) of the Investigatory Powers Act 2016 (c. 25).

F12 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.

F13 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)

F14 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).

F15 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)

F16 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)**

F17 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)**

F18 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)

F19 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)

F20 Commission Recommendation concerning the definition of micro, small and medium-sized enterprises (OJ No. L 124, 20.5.2003, p. 36).

F21 See Article 1(6) of Directive 2016/1148.

F22 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.

F23(6) . . . . . .

(7) Before publishing the NIS national strategy F24..., 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 F25.