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**).

(**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).