STATUTORY INSTRUMENTS

2018 No. 506

The Network and Information Systems Regulations 2018

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 [M1] (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 [M2] (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.

Marginal Citations

M1 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.

M2 S.I. 1981/226 (N.I. 6).

Status:
Point in time view as at 10/05/2018.

Changes to legislation:
There are currently no known outstanding effects for the The Network and Information Systems Regulations 2018, PART 5.