Communications Act 2003

2003 CHAPTER 21

PART 2

NETWORKS, SERVICES AND THE RADIO SPECTRUM

CHAPTER 1

ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES

[F1 Security of public electronic communications networks and services

Textual Amendments

F1 Ss. 105A-105D and cross-heading inserted (26.5.2011) by The Electronic Communications and Wireless Telegraphy Regulations 2011 (S.I. 2011/1210), reg. 1(2), **Sch. 1 para. 65** (with Sch. 3 para. 2)

[F2 105A. Duty to take security measures

(1) The provider of a public electronic communications network or a public electronic communications service must take such measures as are appropriate and proportionate for the purposes of—

(a) identifying the risks of security compromises occurring;

(b) reducing the risks of security compromises occurring; and

(c) preparing for the occurrence of security compromises.

(2) In this Chapter "security compromise", in relation to a public electronic communications network or a public electronic communications service, means—

(a) anything that compromises the availability, performance or functionality of the network or service;

(b) any unauthorised access to, interference with or exploitation of the network or service or anything that enables such access, interference or exploitation;

(c) anything that compromises the confidentiality of signals conveyed by means of the network or service;

(d) anything that causes signals conveyed by means of the network or service to be—

(i) lost;

(ii) unintentionally altered; or

(iii) altered otherwise than by or with the permission of the provider of the network or service;

(e) anything that occurs in connection with the network or service and compromises the confidentiality of any data stored by electronic means;

(f) anything that occurs in connection with the network or service and causes any data stored by electronic means to be—

(i) lost;

(ii) unintentionally altered; or

(iii) altered otherwise than by or with the permission of the person holding the data; or

(g) anything that occurs in connection with the network or service and causes a connected security compromise.

(3) But in this Chapter "security compromise" does not include anything that occurs as a result of conduct that—

(a) is required or authorised by or under an enactment mentioned in subsection (4);

(b) is undertaken for the purpose of providing a person with assistance in giving effect to a warrant or authorisation that has been issued or given under an enactment mentioned in subsection (4);

(c) is undertaken for the purpose of providing a person with assistance in exercising any power conferred by or under prison rules; or

(d) is undertaken for the purpose of providing assistance to a constable or a member of a service police force (acting in either case in that capacity).

(4) The enactments are—

(a) the Investigatory Powers Act 2016;

(b) Part 1 of the Crime and Courts Act 2013;

(c) the Prisons (Interference with Wireless Telegraphy) Act 2012;

(d) the Regulation of Investigatory Powers Act 2000;

(e) the Regulation of Investigatory Powers (Scotland) Act 2000;

(f) the Intelligence Services Act 1994;

(g) any other enactment (whenever passed or made) so far as it—

(i) makes provision which is in the interests of national security;

(ii) has effect for the purpose of preventing or detecting crime or of preventing disorder; or

(iii) makes provision which is in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security.

(5) In this section—

"connected security compromise" means—

(a) in relation to a public electronic communications network, a security compromise that occurs in relation to another public electronic communications network or a public electronic communications service;

(b) in relation to a public electronic communications service, a security compromise that occurs in relation to a public electronic communications network or another public electronic communications service;

"crime" and "detecting crime" have the same meanings as in the Investigatory Powers Act 2016;

"prison rules" means any rules made under—

(a) section 47 of the Prison Act 1952;

(b) section 39 of the Prisons (Scotland) Act 1989; or

(c) section 13 of the Prison Act (Northern Ireland) 1953;

"service police force" means—

(a) the Royal Navy Police;

(b) the Royal Military Police; or

(c) the Royal Air Force Police;

"signal" has the same meaning as in section 32.**]**

Textual Amendments

F2 Ss. 105A, 105B substituted for ss. 105A-105D and ss. 105C, 105D re-inserted (17.11.2021 for specified purposes, 1.10.2022 in so far as not already in force) by Telecommunications (Security) Act 2021 (c. 31), **ss. 1(2)**, 2, 28(1)(a)

[F2105B. Duty to take specified security measures

(1) The Secretary of State may by regulations provide that the provider of a public electronic communications network or a public electronic communications service must take specified measures or measures of a specified description.

(2) A measure or description of measure may be specified only if the Secretary of State considers that taking that measure or a measure of that description would be appropriate and proportionate for a purpose mentioned in section 105A(1).

(3) In this section "specified" means specified in the regulations.

(4) Nothing in this section or regulations under it affects the duty imposed by section 105A.**]**

Textual Amendments

F2 Ss. 105A, 105B substituted for ss. 105A-105D and ss. 105C, 105D re-inserted (17.11.2021 for specified purposes, 1.10.2022 in so far as not already in force) by Telecommunications (Security) Act 2021 (c. 31), **ss. 1(2)**, 2, 28(1)(a)

[

Duty to take measures in response to security compromises

F3105C.

(1) This section applies where a security compromise occurs in relation to a public electronic communications network or a public electronic communications service.

(2) The provider of the network or service must take such measures as are appropriate and proportionate for the purpose of preventing adverse effects (on the network or service or otherwise) arising from the security compromise.

(3) If the security compromise has an adverse effect on the network or service, the provider of the network or service must take such measures as are appropriate and proportionate for the purpose of remedying or mitigating that adverse effect.**]**

Textual Amendments

F3 Ss. 105A, 105B substituted for ss. 105A-105D and ss. 105C, 105D re-inserted (17.11.2021 for specified purposes, 1.10.2022 in so far as not already in force) by Telecommunications (Security) Act 2021 (c. 31), **ss. 1(2)**, 2, 28(1)(a)

[

Duty to take specified measures in response to security compromise

F4105D.

(1) The Secretary of State may by regulations provide that, where a security compromise of a specified description occurs in relation to a public electronic communications network or a public electronic communications service, the provider of the network or service must take specified measures or measures of a specified description.

(2) A measure or description of measure may be specified under subsection (1) only if the Secretary of State considers that taking that measure or a measure of that description would be appropriate and proportionate for the purpose of preventing adverse effects (on the network or service or otherwise) arising from a security compromise of the specified description.

(3) The Secretary of State may by regulations provide that, where a security compromise occurs in relation to a public electronic communications network or a public electronic communications service and has an adverse effect of a specified description on the network or service, the provider of the network or service must take specified measures or measures of a specified description.

(4) A measure or description of measure may be specified under subsection (3) only if the Secretary of State considers that taking that measure or a measure of that description would be appropriate and proportionate for the purpose of remedying or mitigating an adverse effect of the specified description.

(5) In this section "specified" means specified in the regulations.

(6) Nothing in this section or regulations under it affects the duty imposed by section 105C.**]**

Textual Amendments

F4 Ss. 105A, 105B substituted for ss. 105A-105D and ss. 105C, 105D re-inserted (17.11.2021 for specified purposes, 1.10.2022 in so far as not already in force) by Telecommunications (Security) Act 2021 (c. 31), **ss. 1(2)**, 2, 28(1)(a); S.I. 2022/931, **reg. 2(a)**

[F5 105E Codes of practice about security measures etc

The Secretary of State may—

(a) issue codes of practice giving guidance as to the measures to be taken under sections 105A to 105D by the provider of a public electronic communications network or a public electronic communications service;

(b) revise a code of practice issued under this section and issue the code as revised;

(c) withdraw a code of practice issued under this section.

Textual Amendments

F5 Ss. 105E-105I inserted (17.11.2021 for specified purposes) by Telecommunications (Security) Act 2021 (c. 31), **ss. 3**, 28(1)(b)

105F Issuing codes of practice about security measures

(1) Before issuing a code of practice under section 105E the Secretary of State—

(a) must publish a draft of—

(i) the code; or

(ii) where relevant, the revisions of the existing code;

(b) must consult the following about the draft—

(i) OFCOM;

(ii) providers of public electronic communications networks to whom the draft would apply;

(iii) providers of public electronic communications services to whom the draft would apply; and

(iv) such other persons as the Secretary of State considers appropriate; and

(c) may make such alterations to the draft as the Secretary of State considers appropriate following the consultation.

(2) Before issuing a code of practice under section 105E the Secretary of State must also lay a draft of the code before Parliament.

(3) If, within the 40-day period, either House of Parliament resolves not to approve the draft of the code, the code may not be issued.

(4) If no such resolution is made within that period, the code may be issued.

(5) If the code is issued, the Secretary of State must publish it.

(6) A code of practice comes into force at the time of its publication under subsection (5), unless it specifies a different commencement time.

(7) A code of practice may—

(a) specify different commencement times for different purposes;

(b) include transitional provisions and savings.

(8) In this section, the "40-day period", in relation to a draft of a code, means the period of 40 days beginning with the day on which the draft is laid before Parliament (or, if it is not laid before each House of Parliament on the same day, the later of the 2 days on which it is laid).

(9) For the purposes of calculating the 40-day period, no account is to be taken of any period during which—

(a) Parliament is dissolved or prorogued, or

(b) both Houses are adjourned for more than 4 days.

Textual Amendments

F5 Ss. 105E-105I inserted (17.11.2021 for specified purposes) by Telecommunications (Security) Act 2021 (c. 31), **ss. 3**, 28(1)(b)

105G Withdrawing codes of practice about security measures

(1) Before withdrawing a code of practice under section 105E the Secretary of State must—

(a) publish notice of the proposal to withdraw the code; and

(b) consult the following about the proposal—

(i) OFCOM;

(ii) providers of public electronic communications networks to whom the code applies;

(iii) providers of public electronic communications services to whom the code applies; and

(iv) such other persons as the Secretary of State considers appropriate.

(2) Where the Secretary of State withdraws a code of practice under section 105E the Secretary of State must—

(a) publish notice of the withdrawal of the code; and

(b) lay a copy of the notice before Parliament.

(3) A withdrawal of a code of practice has effect at the time of the publication of the notice of withdrawal under subsection (2), unless the notice specifies a different withdrawal time.

(4) A notice of withdrawal may—

(a) specify different withdrawal times for different purposes;

(b) include savings.

Textual Amendments

F5 Ss. 105E-105I inserted (17.11.2021 for specified purposes) by Telecommunications (Security) Act 2021 (c. 31), **ss. 3**, 28(1)(b)

105H Effects of codes of practice about security measures

(1) A failure by the provider of a public electronic communications network or a public electronic communications service to act in accordance with a provision of a code of practice does not of itself make the provider liable to legal proceedings before a court or tribunal.

(2) In any legal proceedings before a court or tribunal, the court or tribunal must take into account a provision of a code of practice in determining any question arising in the proceedings if—

(a) the question relates to a time when the provision was in force; and

(b) the provision appears to the court or tribunal to be relevant to the question.

(3) OFCOM must take into account a provision of a code of practice in determining any question arising in connection with the carrying out by them of a relevant function if—

(a) the question relates to a time when the provision was in force; and

(b) the provision appears to OFCOM to be relevant to the question.

(4) In this section—

"code of practice" means a code of practice issued under section 105E;

"relevant function" means a function conferred on OFCOM by any of the following provisions—

(a) section 105M (general duty of OFCOM to ensure compliance with security duties);

(b) section 105N (power of OFCOM to assess compliance with security duties);

(c) section 105O (power of OFCOM to give assessment notices);

(d) section 105S (enforcement of security duties);

(e) section 105U (enforcement of security duties: proposal for interim steps);

(f) section 105V (enforcement of security duties: direction to take interim steps).

Textual Amendments

F5 Ss. 105E-105I inserted (17.11.2021 for specified purposes) by Telecommunications (Security) Act 2021 (c. 31), **ss. 3**, 28(1)(b)

105I Duty to explain failure to act in accordance with code of practice

(1) This section applies where OFCOM have reasonable grounds for suspecting that the provider of a public electronic communications network or a public electronic communications service is failing, or has failed, to act in accordance with a provision of a code of practice issued under section 105E.

(2) OFCOM may give a notification to the provider that—

(a) specifies the provision of the code of practice;

(b) specifies the respects in which the provider is suspected to be failing, or to have failed, to act in accordance with it; and

(c) directs the provider to give to OFCOM a statement under subsection (3) or (4).

(3) A statement under this subsection is a statement that—

(a) confirms that the provider is failing, or has failed, in the respects specified in the notification to act in accordance with the provision of the code of practice; and

(b) explains the reasons for the failure.

(4) A statement under this subsection is a statement that—

(a) states that the provider is not failing, or has not failed, in the respects specified in the notification to act in accordance with the provision of the code of practice; and

(b) explains the reasons for that statement.

(5) The provider must comply with a direction given under subsection (2)(c) within such reasonable period as may be specified in the notification.**]]**

Textual Amendments

F5 Ss. 105E-105I inserted (17.11.2021 for specified purposes) by Telecommunications (Security) Act 2021 (c. 31), **ss. 3**, 28(1)(b)

[F6105J Duty to inform users of risk of security compromise

(1) This section applies where there is a significant risk of a security compromise occurring in relation to a public electronic communications network or a public electronic communications service.

(2) The provider of the network or service must take such steps as are reasonable and proportionate for the purpose of bringing the relevant information, expressed in clear and plain language, to the attention of persons who use the network or service and may be adversely affected by the security compromise.

(3) The relevant information is—

(a) the existence of the risk of the security compromise occurring;

(b) the nature of the security compromise;

(c) the technical measures that it may be reasonably practicable for persons who use the network or service to take for the purposes of—

(i) preventing the security compromise adversely affecting them;

(ii) remedying or mitigating the adverse effect that the security compromise has on them; and

(d) the name and contact details of a person from whom further information may be obtained about the security compromise.

Textual Amendments

F6 Ss. 105J-105L inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 4(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

105K Duty to inform OFCOM of security compromise

(1) The provider of a public electronic communications network or a public electronic communications service must inform OFCOM as soon as reasonably practicable of—

(a) any security compromise that has a significant effect on the operation of the network or service;

(b) any security compromise within section 105A(2)(b) that puts any person in a position to be able to bring about a further security compromise that would have a significant effect on the operation of the network or service.

(2) In determining for the purposes of this section whether the effect that a security compromise has, or would have, on the operation of a network or service is significant, the following matters in particular are to be taken into account—

(a) the length of the period during which the operation of the network or service is or would be affected;

(b) the number of persons who use the network or service that are or would be affected by the effect on the operation of the network or service;

(c) the size and location of the geographical area within which persons who use the network or service are or would be affected by the effect on the operation of the network or service;

(d) the extent to which activities of persons who use the network or service are or would be affected by the effect on the operation of the network or service.

Textual Amendments

F6 Ss. 105J-105L inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 4(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

105L Powers of OFCOM to inform others of security compromise

(1) This section applies where OFCOM consider that—

(a) there is a risk of a security compromise occurring in relation to a public electronic communications network or public electronic communications service; or

(b) a security compromise has occurred in relation to a public electronic communications network or public electronic communications service.

(2) OFCOM must inform the Secretary of State of the risk of or (as the case may be) the occurrence of the security compromise if they consider that the security compromise could result in or has resulted in—

(a) a serious threat to the safety of the public, to public health or to national security;

(b) serious economic or operational problems for persons who are communications providers or persons who make associated facilities available; or

(c) serious economic or operational problems for persons who use electronic communications networks, electronic communications services or associated facilities.

(3) OFCOM may inform the Secretary of State of the risk of or (as the case may be) the occurrence of the security compromise in a case where the duty in subsection (2) does not arise.

(4) OFCOM may inform any of the following about the risk of or (as the case may be) the occurrence of the security compromise—

(a) any person who uses or has used the network or service;

(b) any communications provider;

(c) any person who makes associated facilities available;
(d) any overseas regulator;
(e) the European Union Agency for Cybersecurity.

(5) OFCOM may inform any person who uses or has used the network or service of the technical measures that may be taken by the person for the purposes of—
(a) preventing the security compromise adversely affecting them; or
(b) remedying or mitigating the adverse effect that the security compromise has on them.

(6) OFCOM may direct the provider of the network or service to take steps specified in the direction for the purposes of—
(a) informing persons who use or have used the network or service of the risk of or (as the case may be) the occurrence of the security compromise;
(b) informing persons who use or have used the network or service of the technical measures that may be taken by them for a purpose mentioned in subsection (5)(a) or (b).

(7) OFCOM may if they consider it to be in the public interest—
(a) inform the public of the risk of or (as the case may be) the occurrence of the security compromise;
(b) inform the public of the technical measures that may be taken by members of the public for a purpose mentioned in subsection (5)(a) or (b);
(c) direct the provider of the network or service to do anything that OFCOM could do under paragraph (a) or (b).

(8) It is the duty of the provider of the network or service to comply with a direction given under this section within such reasonable period as may be specified in the direction.

(9) In this section "overseas regulator" means a person who, under the law of a country or territory outside the United Kingdom, has functions in relation to public electronic communications networks or public electronic communications services that correspond to functions that OFCOM have in relation to such networks or services.**]**

Textual Amendments

F6 Ss. 105J-105L inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 4(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

[F7 105M General duty of OFCOM to ensure compliance with security duties

OFCOM must seek to ensure that providers of public electronic communications networks and public electronic communications services comply with the duties imposed on them by or under sections 105A to 105D, 105J and 105K.**]**

Textual Amendments

F7 S. 105M inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 5**, 28(2)(b); S.I. 2022/931, reg. 2(b)

[F8105N Power of OFCOM to assess compliance with security duties

(1) OFCOM may carry out, or arrange for another person to carry out, an assessment of whether the provider of a public electronic communications network or a public electronic communications service is complying or has complied with a duty imposed on the provider by or under any of sections 105A to 105D, 105J and 105K.

(2) Where an assessment under this section is carried out, the provider of the network or service concerned must—

(a) co-operate with the assessment; and

(b) pay the costs reasonably incurred by OFCOM in connection with the assessment.

Textual Amendments

F8 Ss. 105N-105R inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 6(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

105O Power of OFCOM to give assessment notices

(1) This section applies for the purposes of an assessment under section 105N in respect of the provider of a public electronic communications network or a public electronic communications service.

(2) OFCOM may by notice ("an assessment notice") impose on the provider a duty to do any of the following things—

(a) carry out specified tests or tests of a specified description in relation to the network or service;

(b) make arrangements of a specified description for another person to carry out specified tests or tests of a specified description in relation to the network or service;

(c) make available for interview a specified number of persons of a specified description who are involved in the provision of the network or service (not exceeding the number who are willing to be interviewed);

(d) permit an authorised person to enter specified premises;

(e) permit an authorised person to observe any operation taking place on the premises that relates to the network or service;

(f) direct an authorised person to equipment or other material on the premises that is of a specified description;

(g) direct an authorised person to documents on the premises that are of a specified description;

(h) assist an authorised person to view information of a specified description that is capable of being viewed using equipment on the premises;

(i) comply with a request from an authorised person for a copy of the documents to which the person is directed and the information the person is assisted to view;

(j) permit an authorised person to inspect or examine the documents, information, equipment or material to which the person is directed or which the person is assisted to view;

(k) provide an authorised person with an explanation of such documents, information, equipment or material.

(3) The references in subsection (2)(a) and (b) to tests in relation to the network or service include references to—

(a) tests in relation to premises used in connection with the provision of the network or service;

(b) tests in relation to persons involved in the provision of the network or service.

(4) An assessment notice may impose on the provider a duty to carry out, or to make arrangements for another person to carry out, a test in relation to the network or service that risks causing a security compromise, loss to a person or damage to property only if the test consists of the use of techniques that might be expected to be used by a person seeking to cause a security compromise.

(5) An assessment notice may not impose on the provider a duty to permit an authorised person to enter domestic premises.

(6) An assessment notice may not impose on the provider a duty to do anything that would result in the disclosure of documents or information in respect of which a claim to legal professional privilege (or, in Scotland, to confidentiality of communications) could be maintained in legal proceedings.

(7) An assessment notice must, in relation to each duty imposed by the notice, specify the time or times at which, or period or periods within which, the duty must be complied with.

(8) A time or period specified under subsection (7) must not be a time that falls or a period that begins before the end of the period within which an appeal under section 192 can be brought in respect of the assessment notice (ignoring any power to extend the period within which an appeal could be brought).

(9) If an appeal under section 192 is brought in respect of an assessment notice or any provision of an assessment notice, the provider need not comply with any duty imposed by the notice or the provision pending the determination or withdrawal of the appeal.

(10) An assessment notice must provide information about—

(a) the consequences of failing to comply with a duty imposed by the notice; and

(b) the right of appeal in respect of the notice under section 192.

(11) An assessment notice may by further notice—

(a) be revoked by OFCOM;

(b) be varied by OFCOM so as to make it less onerous.

(12) In this section—

"authorised person" means an employee of, or person authorised by, OFCOM;

"domestic premises" means premises, or a part of premises, used as a dwelling;

"specified" means specified in the assessment notice.

Textual Amendments

F8 Ss. 105N-105R inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 6(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

105P Assessment notices: urgency statements

(1) This section applies where—

(a) an assessment notice is given under section 105O to the provider of a public electronic communications network or a public electronic communications service;

(b) the notice states that, in OFCOM's opinion, it is necessary for the provider to comply with a duty imposed by the notice urgently;

(c) the notice gives OFCOM's reasons for reaching that opinion; and

(d) the notice provides information about the right of the provider to make an application under section 105Q.

(2) Subsections (8) and (9) of section 105O do not apply in relation to the duty mentioned in subsection (1)(b).

(3) A time or period specified under subsection (7) of section 105O in relation to the duty mentioned in subsection (1)(b) must not be a time that falls or a period that begins before the end of the period of 14 days beginning with the day the notice is given.

(4) In a case where—

(a) the duty mentioned in subsection (1)(b) is a duty to do something mentioned in section 105O(2)(d) to (k), and

(b) within the period of 14 days beginning with the day the notice is given an appeal under section 192 is brought in respect of the notice or the provision of the notice that imposes the duty,

the provider of the network or service need not comply with the duty pending the determination or withdrawal of the appeal.

Textual Amendments

F8 Ss. 105N-105R inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 6(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

105Q Assessment notices: applications in respect of urgency statements

(1) This section applies where an assessment notice given under section 105O to a provider of a public electronic communications network or a public electronic communications service contains a statement under section 105P(1)(b).

(2) The provider may apply to the court for either or both of the following—

(a) the disapplication of the statement in relation to some or all of the duties imposed by the notice;

(b) a change to the time at which, or period within which, a duty imposed by the notice must be complied with.

(3) On an application under this section, the court may do any of the following—

(a) direct that the notice is to have effect as if it did not contain the statement;

(b) direct that the inclusion of the statement is not to have effect in relation to a duty imposed by the notice;

(c) vary the notice by changing the time at which, or the period within which, a duty imposed by the notice must be complied with;

(d) vary the notice by making other changes required to give effect to a direction under paragraph (a) or (b) or in consequence of a variation under paragraph (c).

(4) The decision of the court on an application under this section is final.

(5) In this section "the court" means the High Court or, in Scotland, the Court of Session.

Textual Amendments

F8 Ss. 105N-105R inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 6(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

105R Assessment notices: information about entering premises

Every report under paragraph 12 of the Schedule to the Office of Communications Act 2002 (OFCOM's annual report) must include a statement of the number of occasions during the financial year to which the report relates on which premises have been entered in pursuance of a duty imposed under section 105O(2)(d).**]**

Textual Amendments

F8 Ss. 105N-105R inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 6(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

[F9105S Enforcement of security duties

(1) Sections 96A to 100, 102 and 103 apply in relation to a contravention of a security duty as they apply in relation to a contravention of a condition set under section 45, other than an SMP apparatus condition.

(2) This section is subject to section 105T (enforcement of security duties: amount of penalties).

(3) In this section "security duty" means a duty imposed by or under any of sections 105A to 105D, 105I to 105K, 105L(6), (7)(c) and (8), 105N(2)(a) and 105O.

Textual Amendments

F9 Ss. 105S-105V inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 7(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

105T Enforcement of security duties: amount of penalties

(1) In its application in relation to a contravention of a security duty, other than a security duty imposed by section 105I, section 96B(5) has effect as if the maximum penalty specified were £100,000 per day.

(2) In its application in relation to a contravention of a security duty imposed by section 105I, section 96B(5) has effect as if the maximum penalty specified were £50,000 per day.

(3) In its application in relation to a contravention of a security duty imposed by section 105I, section 97(1) has effect as if the maximum penalty specified were £10 million.

(4) The Secretary of State may by regulations amend this section so as to substitute a different amount for the amount for the time being specified in subsection (1), (2) or (3).

(5) No regulations are to be made containing provision authorised by subsection (4) unless a draft of the regulations has been laid before Parliament and approved by a resolution of each House.

(6) In this section "security duty" has the same meaning as in section 105S.

Textual Amendments

F9 Ss. 105S-105V inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 7(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

105U Enforcement of security duties: proposal for interim steps

(1) This section applies where—

(a) OFCOM determine that there are reasonable grounds for believing that the provider of a public electronic communications network or a public electronic communications service is contravening or has contravened a duty imposed by or under any of sections 105A to 105D;

(b) OFCOM either have not commenced, or have commenced but not completed, enforcement action in connection with the contravention;

(c) OFCOM determine that there are reasonable grounds for believing that either or both of the following conditions are met—

(i) a security compromise has occurred as a result of the contravention;

(ii) there is an imminent risk of a security compromise or (as the case may be) a further security compromise occurring as a result of the contravention; and

(d) OFCOM determine that, having regard to the seriousness or likely seriousness of the security compromise or security compromises mentioned in paragraph (c), it is reasonable to require the provider to take interim steps pending the completion by OFCOM of enforcement action in connection with the contravention.

(2) OFCOM may give a notification to the provider that—

(a) sets out the determinations mentioned in subsection (1);

(b) specifies the interim steps that OFCOM think the provider should be required to take pending the completion by OFCOM of enforcement action in connection with the contravention; and

(c) specifies the period during which the provider has an opportunity to make representations about the matters notified.

(3) In this section and section 105V—

(a) references to the commencement by OFCOM of enforcement action in connection with a contravention are to the giving of a notification under section 96A (as applied by section 105S) in respect of the contravention; and

(b) references to the completion by OFCOM of enforcement action in connection with a contravention are to the taking of action under section 96C(2)(a) or (b) (as applied by section 105S) in connection with the contravention.

(4) In this section "interim steps" means—

(a) in a case where OFCOM determine that there are reasonable grounds for believing that the condition in subsection (1)(c)(i) is met, steps to—

(i) prevent adverse effects (on the network or service or otherwise) arising from the security compromise;

(ii) remedy or mitigate any adverse effects on the network or service arising from the security compromise;

(b) in a case where OFCOM determine that there are reasonable grounds for believing that the condition in subsection (1)(c)(ii) is met, steps to—

(i) eliminate or reduce the risk of the security compromise or (as the case may be) the further security compromise occurring;

(ii) prevent adverse effects (on the network or service or otherwise) arising from the security compromise or (as the case may be) the further security compromise in the event it occurs.

Textual Amendments

F9 Ss. 105S-105V inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 7(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

105V Enforcement of security duties: direction to take interim steps

(1) This section applies where—

(a) the provider of a public electronic communications network or a public electronic communications service has been given a notification under section 105U;

(b) OFCOM have allowed the provider an opportunity to make representations about the matters notified; and

(c) the period allowed for the making of representations has expired.

(2) OFCOM may—

(a) direct the provider to take the interim steps or any of the interim steps specified in the notification; or

(b) inform the provider that a direction under paragraph (a) will not be given.

(3) OFCOM may give a direction under subsection (2)(a) only if (after considering any representations) they are satisfied—

(a) that there are reasonable grounds for believing that the contravention on the basis of which the notification was given occurred;

(b) that there are reasonable grounds for believing that either or both of the following conditions are met—

(i) a security compromise has occurred as a result of the contravention;

(ii) there is an imminent risk of a security compromise or (as the case may be) a further security compromise occurring as a result of the contravention; and

(c) that, having regard to the seriousness or likely seriousness of the security compromise or security compromises mentioned in paragraph (b), it is reasonable to give the direction.

(4) A direction under subsection (2)(a) must include a statement of OFCOM's reasons for giving the direction.

(5) A direction under subsection (2)(a) must, in relation to each interim step, specify the period within which the step must be taken.

(6) A direction under subsection (2)(a) is ineffective in so far as it would require interim steps to be taken after the completion by OFCOM of enforcement action in connection with the contravention concerned.

(7) Where a direction under subsection (2)(a) has been given and has not been revoked, OFCOM must as soon as reasonably practicable—

(a) commence enforcement action in connection with the contravention concerned (unless enforcement action was commenced by OFCOM before the direction was given); and

(b) complete enforcement action in connection with the contravention concerned.

(8) A direction under subsection (2)(a) may at any time—

(a) be revoked by OFCOM; or

(b) be varied by OFCOM so as to make it less onerous.

(9) A provider of a public electronic communications network or a public electronic communications service who is given a direction under subsection (2)(a) must comply with it.

(10) That duty is enforceable in civil proceedings by OFCOM—

(a) for an injunction;

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

(c) for any other appropriate remedy or relief.**]**

Textual Amendments

F9 Ss. 105S-105V inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 7(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

[F10 105W Civil liability for breach of security duties

(1) A duty imposed by or under any of sections 105A to 105D and 105J on a provider of a public electronic communications network or a public electronic communications service is a duty owed to every person who may be affected by a contravention of the duty.

(2) Subsections (3) and (4) apply where a duty is owed by virtue of subsection (1) to a person.

(3) A breach of the duty that causes that person to sustain loss or damage is actionable at the suit or instance of that person.

(4) An act which—

(a) by inducing a breach of the duty or interfering with its performance, causes that person to sustain loss or damage, and

(b) is done wholly or partly for achieving that result,

is actionable at the suit or instance of that person.

(5) In proceedings brought against a provider of a public electronic communications network or a public electronic communications service by virtue of subsection (3), it is a defence for the provider to show that they took all reasonable steps and exercised all due diligence to avoid contravening the duty in question.

(6) The consent of OFCOM is required for the bringing of proceedings by virtue of this section.

(7) If OFCOM give their consent subject to conditions relating to the conduct of the proceedings, the proceedings are not to be carried on except in compliance with those conditions.**]**

Textual Amendments

F10 S. 105W inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 8**, 28(2)(b); S.I. 2022/931, reg. 2(b)

[F11 105X Relationship between security duties and certain other duties etc

(1) A security duty imposed on a provider of a public electronic communications network or a public electronic communications service does not apply in so far as compliance with the duty would—

(a) result in a failure by the provider to comply with a duty or prohibition imposed by or under an enactment mentioned in section 105A(4);

(b) prevent the provider from giving effect to a warrant or authorisation that has been issued or given under an enactment mentioned in section 105A(4);

(c) prevent the provider from providing a person with assistance in giving effect to a warrant or authorisation that has been issued or given under an enactment mentioned in section 105A(4); or

(d) prevent the provider from providing a person with assistance in exercising any power conferred by or under prison rules.

(2) In this section—

"prison rules" has the same meaning as in section 105A;

"security duty" means a duty imposed by or under—

(a) section 96C as applied by section 105S; or

(b) any of sections 105A to 105D, 105I to 105K, 105L(6), (7)(c) and (8), 105N(2)(a), 105O and 105V.**]**

Textual Amendments

F11 S. 105X inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 9**, 28(2)(b); S.I. 2022/931, reg. 2(b)

[F12 105Y Statement of policy on ensuring compliance with security duties

(1) OFCOM must prepare and publish a statement of their general policy with respect to the exercise of their functions under sections 105I and 105M to 105V.

(2) OFCOM may from time to time revise that statement as they think fit.

(3) Where OFCOM make or revise their statement of policy under this section, they must publish that statement or (as the case may be) the revised statement in such manner as they consider appropriate for bringing it to the attention of the persons who, in their opinion, are likely to be affected by it.

(4) In exercising their functions under sections 105I and 105M to 105V OFCOM must have regard to the statement for the time being in force under this section.**]**

Textual Amendments

F12 S. 105Y inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 10(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

[F13 105Z OFCOM reports on security

(1) As soon as practicable after the end of each reporting period OFCOM must prepare and send to the Secretary of State a report for the period (a "security report").

(2) A security report must contain such information and advice as OFCOM consider may best serve the purpose mentioned in subsection (3).

(3) The purpose is to assist the Secretary of State in the formulation of policy in relation to the security of public electronic communications networks and public electronic communications services.

(4) A security report must in particular include—

(a) information about the extent to which providers of public electronic communications networks and public electronic communications services have complied during the reporting period with the duties imposed on them by or under sections 105A to 105D, 105I to 105K, 105N(2)(a) and 105O;

(b) information about the extent to which providers of public electronic communications networks and public electronic communications services have acted during the reporting period in accordance with codes of practice issued under section 105E;

(c) information about the security compromises that OFCOM have been informed of during the reporting period under section 105K;

(d) information about the action taken by OFCOM during the reporting period in response to security compromises they have been informed of under section 105K;

(e) information about the extent to which and manner in which OFCOM have exercised the functions conferred on them by sections 105I and 105L to 105V during the reporting period;

(f) information about any particular risks to the security of public electronic communications networks and public electronic communications services of which OFCOM have become aware during the reporting period;

(g) any other information of a kind specified in a direction given by the Secretary of State.

(5) A security report must not include personal data (within the meaning of Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2) and (14) of that Act).

(6) The Secretary of State may—

(a) publish a security report or any part of it; or

(b) disclose a security report or any part of it to any person or body performing functions of a public nature for the purpose of enabling or assisting the performance of those functions.

(7) In publishing or disclosing a security report or any part of a security report, the Secretary of State must have regard to the need to exclude from publication or disclosure, so far as is practicable, the matters which are confidential in accordance with subsection (8).

(8) A matter is confidential under this subsection if—

(a) it relates to the affairs of a particular body; and

(b) publication or disclosure of that matter would or might, in the Secretary of State's opinion, seriously and prejudicially affect the interests of that body.

(9) In this section "reporting period" means—

(a) the period of 2 years beginning with the day on which section 11 of the Telecommunications (Security) Act 2021 comes into force; and

(b) each successive period of 12 months.**]**

Textual Amendments

F13 S. 105Z inserted (1.10.2022) by Telecommunications (Security) Act 2021 (c. 31), **ss. 11(2)**, 28(2)(b); S.I. 2022/931, reg. 2(b)

Changes to legislation:
Communications Act 2003, Cross Heading: Security of public electronic communications networks and services is up to date with all changes known to be in force on or before 08 May 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations.
View outstanding changes

Changes and effects yet to be applied to :

- specified provision(s) amendment to earlier commencing SI 2003/1900, art. 3(2) by S.I. 2003/3142 art. 1(3)
- specified provision(s) amendment to earlier commencing SI 2003/3142 by S.I. 2004/1492 art. 2
- specified provision(s) amendment to earlier commencing SI 2003/3142 by S.I. 2004/697 art. 2
- specified provision(s) amendment to earlier commencing SI 2003/3142 art. 4 Sch. 2 by S.I. 2004/545 art. 2

Changes and effects yet to be applied to the whole Act associated Parts and Chapters:
Whole provisions yet to be inserted into this Act (including any effects on those provisions):

- s. 124Q(7)(a) words substituted by 2013 c. 22 Sch. 9 para. 52
- s. 148A and cross-heading inserted by 2022 c. 46 s. 73(2)
- s. 368E(5)(d)(e) inserted by 2017 c. 30 s. 94(3)
- s. 402(2A)(za)(zb) inserted by 2022 c. 46 Sch. para. 2
- Sch. 3A para. 21(6) inserted by 2022 c. 46 Sch. para. 3(5)(b)
- Sch. 3A para. 37(3)(aza) inserted by 2022 c. 46 Sch. para. 3(9)
- Sch. 3A para. 84(1)(aza) inserted by 2022 c. 46 Sch. para. 3(10)
- Sch. 3A para. 103(1)(ca) inserted by 2022 c. 46 s. 70
- Sch. 3A para. 119A inserted by 2022 c. 46 s. 72
- Sch. 3A Pt. 4ZA inserted by 2022 c. 46 s. 67(1)