STATUTORY INSTRUMENTS

2011 No. 1208

ELECTRONIC COMMUNICATIONS

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

Made - - - -	*4th May 2011*
Laid before Parliament	*5th May 2011*
Coming into force - -	*26th May 2011*

The Secretary of State, being a Minister designated(**a**) for the purposes of section 2(2) of the European Communities Act 1972(**b**) in respect of matters relating to electronic communications, in exercise of the powers conferred by that section makes the following Regulations:

Citation, commencement and interpretation

1.—(1) These Regulations may be cited as the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 and shall come into force on 26th May 2011.

(2) In these Regulations "the 2003 Regulations" means the Privacy and Electronic Communications (EC Directive) Regulations 2003(**c**).

Amendment of the 2003 Regulations

2. The 2003 Regulations are amended as set out in the following regulations.

3. In regulation 2—

(a) in the definition of "location data" after "electronic communications network" insert "or by an electronic communications service";

(b) after the definition of "OFCOM", insert ""personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service;".

4.—(1) In regulation 5, after paragraph (1) insert—

"(1A) The measures referred to in paragraph (1) shall at least—

(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;

(**a**) S.I. 2001/3495: which has been amended, but those amendments are not relevant to these regulations.
(**b**) 1972 c.68. Section 2(2) was amended by section 27 of the Legislative and Regulatory Reform Act 2006 (c.51) and section 3 of, and Part 1 of the Schedule to, the European Union (Amendment) Act 2008 (c.7).
(**c**) S.I. 2003/2426; which have been amended, but those amendments are not relevant to these regulations.

(b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and

(c) ensure the implementation of a security policy with respect to the processing of personal data."

(2) After paragraph (5) insert—

"(6) The Information Commissioner may audit the measures taken by a provider of a public electronic communications service to safeguard the security of that service.".

5. After regulation 5, insert—

"Personal data breach

5A.—(1) In this regulation and in regulations 5B and 5C, "service provider" has the meaning given in regulation 5(1).

(2) If a personal data breach occurs, the service provider shall, without undue delay, notify that breach to the Information Commissioner.

(3) Subject to paragraph (6), if a personal data breach is likely to adversely affect the personal data or privacy of a subscriber or user, the service provider shall also, without undue delay, notify that breach to the subscriber or user concerned.

(4) The notification referred to in paragraph (2) shall contain at least a description of—

(a) the nature of the breach;

(b) the consequences of the breach; and

(c) the measures taken or proposed to be taken by the provider to address the breach.

(5) The notification referred to the paragraph (3) shall contain at least—

(a) a description of the nature of the breach;

(b) information about contact points within the service provider's organisation from which more information may be obtained; and

(c) recommendations of measures to allow the subscriber to mitigate the possible adverse impacts of the breach.

(6) The notification referred to in paragraph (3) is not required if the service provider has demonstrated, to the satisfaction of the Information Commissioner that—

(a) it has implemented appropriate technological protection measures which render the data unintelligible to any person who is not authorised to access it, and

(b) that those measures were applied to the data concerned in that breach.

(7) If the service provider has not notified the subscriber or user in compliance with paragraph (3), the Information Commissioner may, having considered the likely adverse effects of the breach, require it to do so.

(8) Service providers shall maintain an inventory of personal data breaches comprising —

(a) the facts surrounding the breach,

(b) the effects of that breach, and

(c) remedial action taken

which shall be sufficient to enable the Information Commissioner to verify compliance with the provisions of this regulation. The inventory shall only include information necessary for this purpose.

Personal data breach: audit

5B. The Information Commissioner may audit the compliance of service providers with the provisions of regulation 5A.

Personal data breach: enforcement

5C.—(1) If a service provider fails to comply with the notification requirements of regulation 5A, the Information Commissioner may issue a fixed monetary penalty notice in respect of that failure.

(2) The amount of a fixed monetary penalty under this regulation shall be £1,000.

(3) Before serving such a notice, the Information Commissioner must serve the service provider with a notice of intent.

(4) The notice of intent must—

(a) state the name and address of the service provider;

(b) state the nature of the breach;

(c) indicate the amount of the fixed monetary penalty;

(d) include a statement informing the service provider of the opportunity to discharge liability for the fixed monetary penalty;

(e) indicate the date on which the Information Commissioner proposes to serve the fixed monetary penalty notice; and

(f) inform the service provider that he may make written representations in relation to the proposal to serve a fixed monetary penalty notice within the period of 21 days from the service of the notice of intent.

(5) A service provider may discharge liability for the fixed monetary penalty if he pays to the Information Commissioner the amount of £800 within 21 days of receipt of the notice of intent.

(6) The Information Commissioner may not serve a fixed monetary penalty notice until the time within which representations may be made has expired.

(7) The fixed monetary penalty notice must state—

(a) the name and address of the service provider;

(b) details of the notice of intent served on the service provider;

(c) whether there have been any written representations;

(d) details of any early payment discounts;

(e) the grounds on which the Information Commissioner imposes the fixed monetary penalty;

(f) the date by which the fixed monetary penalty is to be paid; and

(g) details of, including the time limit for, the service provider's right of appeal against the imposition of the fixed monetary penalty.

(8) A service provider on whom a fixed monetary penalty is served may appeal to the Tribunal against the issue of the fixed monetary penalty notice.

(9) Any sum received by the Information Commissioner by virtue of this regulation must be paid into the Consolidated Fund.

(10) In England and Wales and Northern Ireland, the penalty is recoverable—

(a) if a county court so orders, as if it were payable under an order of that court;

(b) if the High Court so orders, as if it were payable under an order of that court.

(11) 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 in Scotland."

6.—(1) In regulation 6—

(2) In paragraph (1) for "use an electronic communications network to store information, or to", substitute "store or".

(3) For paragraph (2)(b) substitute "(b) has given his or her consent".

(4) After paragraph (3) insert—

"(3A) For the purposes of paragraph (2), consent may be signified by a subscriber who amends or sets controls on the internet browser which the subscriber uses or by using another application or programme to signify consent."

(5) In paragraph (4)(a) omit "or facilitating".

7. In regulation 7(3)(b) for "given his consent" substitute "previously notified the provider that he consents".

8. In regulation 19(1) after "automated calling" insert "or communication".

9.—(1) In regulation 23, at the end of paragraph (a) omit "or".

(2) After paragraph (b) insert—

"(c) where that electronic mail would contravene regulation 7 of the Electronic Commerce (EC Directive) Regulations 2002(**a**); or

(d) where that electronic mail encourages recipients to visit websites which contravene that regulation."

10. After regulation 29 insert—

"**29A.**—(1) Where regulations 28 and 29 apply, communications providers must establish and maintain internal procedures for responding to requests for access to users' personal data.

(2) Communications providers shall on demand provide the Information Commissioner with information about—

(a) those procedures;

(b) the number of requests received;

(c) the legal justification for the request; and

(d) the communications provider's response."

11. In regulation 31—

(a) in paragraph (1) after "provisions of Part V" insert "and sections 55A to 55E".

(b) at the end of paragraph (2) insert "and the functions set out in regulations 31A and 31B".

12. After regulation 31 insert—

"Enforcement: third party information notices

31A.—(1) The Information Commissioner may require a communications provider (A) to provide information to the Information Commissioner by serving on A a notice ("a third party information notice").

(2) The third party information notice may require A to release information held by A about another person's use of an electronic communications network or an electronic communications service where the Information Commissioner believes that the information requested is relevant information.

(3) Relevant information is information which the Information Commissioner considers is necessary to investigate the compliance of any person with these Regulations.

(4) The notice shall set out—

(a) the information requested,

(b) the form in which the information must be provided;

(c) the time limit within which the information must be provided; and

---

(**a**) S.I. 2002/2013; which has been amended but those amendments are not relevant.

(d) information about the rights of appeal conferred by these Regulations.

(5) The time limit referred to in paragraph (4)(c) shall not expire before the end of the period in which an appeal may be brought. If an appeal is brought, the information requested need not be provided pending the determination or withdrawal of the appeal.

(6) In an urgent case, the Commissioner may include in the notice—

(a) a statement that the case is urgent; and

(b) a statement of his reasons for reaching that conclusion,

in which case paragraph (5) shall not apply.

(7) Where paragraph (6) applies, the communications provider shall have a minimum of 7 days (beginning on the day on which the notice is served) to provide the information requested.

(8) A person shall not be required by virtue of this regulation to disclose any information in respect of—

(a) any communication between a professional legal adviser and the adviser's client in connection with the giving of legal advice with respect to the client's obligations, liabilities or rights under these Regulations, or

(b) any communication between a professional legal adviser and the adviser's client, or between such an adviser or the adviser's client and any other person, made in connection with or in contemplation of proceedings under or arising out of these Regulations (including proceedings before the Tribunal) and for the purposes of such proceedings.

Enforcement: appeals

31B.—(1) A communications provider on whom a third party information notice has been served may appeal to the Tribunal against the notice.

(2) Appeals shall be determined in accordance with section 49 of and Schedule 6 to the Data Protection Act 1998 as modified by Schedule 1 to these Regulations."

13. After regulation 36 insert—

"**Review of implementation**

37.—(1) Before the end of each review period, the Secretary of State must—

(a) carry out a review of the implementation in the United Kingdom of the Directive;

(b) set out the conclusions of the review in a report; and

(c) publish the report.

(2) In carrying out the review the Secretary of State must, so far as is reasonable, have regard to how the Directive is implemented in other member States.

(3) The report must in particular—

(a) set out the objectives intended to be achieved by the implementation in the United Kingdom of the Directive;

(b) assess the extent to which those objectives are achieved; and

(c) assess whether those objectives remain appropriate and, if so, the extent to which they could be achieved with a system that imposes less regulation.

(4) "Review period" means—

(a) the period of five years beginning with the 26th May 2011; and

(b) subject to paragraph (5), each successive period of 5 years.

(5) If a report under this regulation is published before the last day of the review period to which it relates, the following review period is to being with the day on which that report is published."

14. Schedule 1 to the 2003 Regulations is amended as follows—

(a) In the title of the Schedule, after "Part V" insert "and sections 55A to 55E";

(b) After paragraph 2 insert "2A. Sections 41A to 41C shall be omitted.";

(c) In paragraph 4, at the end of the substituted subparagraph (c) for "; and" and paragraph (d) there shall be substituted—

"(d) in subsection (8), for "under this Act" there shall be substituted "under the Privacy and Electronic Communications (EC Directive) Regulations 2003";

(e) in subsection (8B), for "under this Act (other than an offence under section 47)" there shall be substituted "under the Privacy and Electronic Communications (EC Directive) Regulations 2003"; and

(f) subsection (10) shall be omitted.";

(d) For paragraph 6 there shall be substituted—

"**6.** In section 47—

(a) in subsection (1), "special information notice" there shall be substituted "third party information notice"; and

(b) in subsection (2), for "special information notice" there shall be substituted "third party information notice".";

(e) After paragraph 8, insert—

"**8A.** In section 55A—

(a) in subsection (1)—

(i) for "data controller" there shall be substituted "person", and

(ii) for "of section 4(4) by the data controller" there shall be substituted "of the requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2003";

(b) in subsection (3), for "data controller" there shall be substituted "person";

(c) subsection (3A) shall be omitted;

(d) in subsection (4), for "data controller" there shall be substituted "person";

(e) in subsection (9), the definition of "data controller" shall be omitted.

8B. In section 55B, for the words "data controller" (in subsections (1), (3) and (4)), there shall be substituted the word "person".";

(f) In paragraph 9, for "Schedule (6)" substitute "Schedule 6";

(g) In paragraph 10 at the end of subparagraph (a) omit "; and" and subparagraph (b) and replace with—

"(b) in subparagraph (1A) for "data controller" there shall be substituted "person", and for "requirement imposed by an assessment notice" there shall be substituted "the audit provisions in regulations 5 and 5B of the 2003 Regulations";

(c) in subparagraph (1B)—

(i) for "data controller" there shall be substituted "person";

(ii) for "data protection principles" there shall be substituted "the requirements of the 2003 Regulations";

(iii) for "assessment notice" there shall be substituted "audit notice"; and

(iv) the words "subparagraph (2) and" shall be omitted;

(d) subparagraph (2) shall be omitted;

(e) in subparagraphs (3)(d)(ii) and (3)(f) for the words "data controller" there shall be substituted "person", and for the words "the data protection principles" there shall be substituted "the requirements of the 2003 Regulations".";

(h) After paragraph 10 insert—

"**10A.** In paragraph 2(1A) of Schedule 9 for "assessment notice" there shall be substituted "audit notice"."

Amendment of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

15. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000(**a**) are amended as follows—

(a) in regulation 3(1) omit "or implied";

(b) at the end of regulation 3(3) insert "as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws(**b**).".

Amendment of the Enterprise Act 2002

16. The Enterprise Act 2002(**c**) is amended as follows—

(a) in section 213(5A), after paragraph (i) insert "(j) the Information Commissioner";

(b) in Schedule 13, after paragraph 11 insert—

"**12.** Article 13 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).".

Amendment of the Enterprise Act 2002 (Part 8 Community Infringements Specified UK Laws) Order 2003

17. At the end of the Schedule to the Enterprise Act 2002 (Part 8 Community Infringements Specified UK Laws) Order 2003(**d**) insert—

"Article 13 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)	Regulations 19 to 26 and 30 and 32 of the Privacy and Electronic Communications (EC Directive) Regulations 2003"

Ed Vaizey
Parliamentary Under Secretary of State
Department for Culture, Media and Sport

4th May 2011

(**a**) S.I. 2000/2699; which was amended by S.I. 2003/2426.
(**b**) O.J. L 337, 18.12.2009, p.11.
(**c**) 2002 c.40. Section 213(5A) was inserted by S.I. 2006/3363. Schedule 13 has been amended by S.I. 2004/2095, 2006/3363, 2008/1277, 2009/2999 and 2010/2960.
(**d**) S.I. 2003/1374; which has been amended but those amendments are not relevant.

EXPLANATORY NOTE

(This note is not part of the Order)

These Regulations implement Articles 2 and 3 of Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws by making amendments to the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("the 2003 Regulations").

Regulation 3 amends the definition of "location data" and inserts a new definition of "personal data breach" into the 2003 Regulations.

Regulation 4 makes provision in relation to the required measures to be taken by communications providers in ensuring that the processing of personal data is secure. Regulation 4 also gives the Information Commissioner the power to audit compliance with these requirements.

Regulation 5 inserts a new provision into the 2003 Regulations which relates to the notification of personal data breaches. In all cases, the Information Commissioner must be notified. In some cases, the subscriber or user must also be notified where there is a risk that the breach would adversely affect the personal data or privacy of that user.

Regulation 5 also inserts provision into the 2003 Regulations for the auditing and enforcement of the notification provisions. In the event of failure to comply, the Information Commissioner will be able to impose a fixed civil monetary penalty on a service provider.

Regulation 6 amends the provisions in the 2003 Regulations on the storage of or access to information on the terminal equipment of end users. It also makes provision as to the signification of consent which must be sought as a result of the changes to the Directive.

Regulation 7 makes a minor textual amendment to regulation 7 of the 2003 Regulations.

Regulation 8 makes a minor textual amendment to regulation 19(1) of the 2003 Regulations.

Regulation 9 amends regulation 23 of the 2003 Regulations, by providing for the prohibition of sending electronic mail which contravenes the information requirements in regulation 7 of the Electronic Commerce (EC Directive) Regulations 2002, or sending an e-mail which encourages recipients to visit websites which contravene that regulation.

Regulation 10 makes provision to allow police and the security services to have access to personal data of users of public electronic communications networks and services. It also makes provision to compel service providers to establish and maintain procedures to allow access to that data.

Regulation 11 makes minor amendments to regulation 31 of the 2003 Regulations. The amendments extend section 55A to 55E of the Data Protection Act 1998 to the 2003 Regulations which will allow the Information Commissioner to issue civil monetary penalties for non-compliance with the Regulations of up to £500,000.

Regulation 12 inserts new regulations 31A and 31B which make provision for third party information notices. The Information Commissioner may request information from a communications provider which relates to the use of that provider's network or service by a third party which is in contravention of any part of the Regulations. New regulation 31B makes provision for appeals against third party information notices.

Regulation 13 inserts a new regulation 37 into the 2003 Regulations which requires the Secretary of State to conduct a review of the implementation of the Directive in the United Kingdom at least every 5 years and lay a report of that review before Parliament.

Regulation 14 amends Schedule 1 to the 2003 Regulations.

Regulation 15 amends the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Regulation 16 amends the Enterprise Act 2002 to include reference to the Information Commissioner, and Article 13 of the 2002 Directive for the purposes of the enforcement of the provisions of that Article as a Community Infringement under Part 8 of the Enterprise Act 2002.

Regulation 17 inserts article 13 of the 2002 Directive into the Schedule to the Enterprise Act 2002 (Part 8 Community Infringements Specified UK Laws) Order 2003, which lists Community infringements for the purposes of the Enterprise Act 2002.

A transposition and a full impact assessment of the effect that this instrument will have on the costs of business and the voluntary sector are available from the Department for Culture, Media and Sport, 2-4 Cockspur Street, London, SW1Y 5DH and are published with the Explanatory Memorandum alongside the instrument on www.legislation.gov.uk.

Printed and published in the UK by The Stationery Office Limited under the authority and superintendence of Carol Tullo, Controller of Her Majesty's Stationery Office and Queen's Printer of Acts of Parliament.

STATUTORY INSTRUMENTS

2011 No. 1208

ELECTRONIC COMMUNICATIONS

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

£5.75

E0309 05/2011 110309T 19585