STATUTORY INSTRUMENTS

2011 No. 1208

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

Amendment of the 2003 Regulations

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."

Commencement Information

I1 Reg. 5 in force at 26.5.2011, see **reg. 1(1)**

Changes to legislation:
There are currently no known outstanding effects for the The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, Section 5.