STATUTORY INSTRUMENTS

2003 No. 2426

The Privacy and Electronic Communications (EC Directive) Regulations 2003

[F1Personal 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.

[

F2(9) This regulation does not apply in relation to any personal data breach which is to be notified to the Investigatory Powers Commissioner in accordance with a code of practice made under the Investigatory Powers Act 2016.**]]**

F1 Regs. 5A-5C inserted (26.5.2011) by The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (S.I. 2011/1208), regs. 1(1), **5**

F2 Reg. 5A(9) inserted (27.6.2018) by Investigatory Powers Act 2016 (c. 25), s. 272(1), **Sch. 10 para. 14** (with Sch. 9 paras. 7, 8, 10); S.I. 2018/652, reg. 12(g)(iii)

Changes to legislation:
There are currently no known outstanding effects for the The Privacy and Electronic Communications (EC Directive) Regulations 2003, Section 5A.