Data Protection Act 2018

2018 CHAPTER 12

PART 4

INTELLIGENCE SERVICES PROCESSING

CHAPTER 4

CONTROLLER AND PROCESSOR

Obligations relating to personal data breaches

108   Communication of a personal data breach

(1) If a controller becomes aware of a serious personal data breach in relation to personal data for which the controller is responsible, the controller must notify the Commissioner of the breach without undue delay.

(2) Where the notification to the Commissioner is not made within 72 hours, the notification must be accompanied by reasons for the delay.

(3) Subject to subsection (4), the notification must include—

(a) a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) the name and contact details of the contact point from whom more information can be obtained;

(c) a description of the likely consequences of the personal data breach;

(d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

2

Data Protection Act 2018 (c. 12)
PART 4 – Intelligence services processing
CHAPTER 4 – Controller and processor
Document Generated: 2024-03-28

(4) Where and to the extent that it is not possible to provide all the information mentioned in subsection (3) at the same time, the information may be provided in phases without undue further delay.

(5) If a processor becomes aware of a personal data breach (in relation to data processed by the processor), the processor must notify the controller without undue delay.

(6) Subsection (1) does not apply in relation to a personal data breach if the breach also constitutes a relevant error within the meaning given by section 231(9) of the Investigatory Powers Act 2016.

(7) For the purposes of this section, a personal data breach is serious if the breach seriously interferes with the rights and freedoms of a data subject.