Data Protection Act 2018

2018 CHAPTER 12

PART 3

LAW ENFORCEMENT PROCESSING

CHAPTER 4

CONTROLLER AND PROCESSOR

Obligations relating to personal data breaches

67 Notification of a personal data breach to the Commissioner

(1) If a controller becomes aware of a personal data breach in relation to personal data for which the controller is responsible, the controller must notify the breach to the Commissioner—

(a) without undue delay, and

(b) where feasible, not later than 72 hours after becoming aware of it.

(2) Subsection (1) does not apply if the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals.

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

(4) Subject to subsection (5), 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 data protection officer or other 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.

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

(6) The controller must record the following information in relation to a personal data breach—

(a) the facts relating to the breach,

(b) its effects, and

(c) the remedial action taken.

(7) The information mentioned in subsection (6) must be recorded in such a way as to enable the Commissioner to verify compliance with this section.

(8) Where a personal data breach involves personal data that has been transmitted by or to a person who is a controller under the law of another member State, the information mentioned in subsection (6) must be communicated to that person without undue delay.

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

68 Communication of a personal data breach to the data subject

(1) Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must inform the data subject of the breach without undue delay.

(2) The information given to the data subject must include the following—

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

(b) the name and contact details of the data protection officer or other 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.

(3) The duty under subsection (1) does not apply where—

(a) the controller has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the breach,

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in subsection (1) is no longer likely to materialise, or

(c) it would involve a disproportionate effort.

(4) An example of a case which may fall within subsection (3)(a) is where measures that render personal data unintelligible to any person not authorised to access the data have been applied, such as encryption.

(5) In a case falling within subsection (3)(c) (but not within subsection (3)(a) or (b)), the information mentioned in subsection (2) must be made available to the data subject in another equally effective way, for example, by means of a public communication.

(6) Where the controller has not informed the data subject of the breach the Commissioner, on being notified under section 67 and after considering the likelihood of the breach resulting in a high risk, may—

(a) require the controller to notify the data subject of the breach, or

(b) decide that the controller is not required to do so because any of paragraphs (a) to (c) of subsection (3) applies.

(7) The controller may restrict, wholly or partly, the provision of information to the data subject under subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—

(a) avoid obstructing an official or legal inquiry, investigation or procedure;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

(8) Subsection (6) does not apply where the controller's decision not to inform the data subject of the breach was made in reliance on subsection (7).

(9) The duties in section 52(1) and (2) apply in relation to information that the controller is required to provide to the data subject under this section as they apply in relation to information that the controller is required to provide to the data subject under Chapter 3 .