Data Protection Act 2018

2018 CHAPTER 12

PART 3

LAW ENFORCEMENT PROCESSING

CHAPTER 2

PRINCIPLES

34 Overview and general duty of controller

(1) This Chapter sets out the six data protection principles as follows—

(a) section 35(1) sets out the first data protection principle (requirement that processing be lawful and fair);

(b) section 36(1) sets out the second data protection principle (requirement that purposes of processing be specified, explicit and legitimate);

(c) section 37 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 38(1) sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

(e) section 39(1) sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 40 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) In addition—

(a) each of sections 35, 36, 38 and 39 makes provision to supplement the principle to which it relates, and

(b) sections 41 and 42 make provision about the safeguards that apply in relation to certain types of processing.

(3) The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter.

35 The first data protection principle

(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—

(a) the data subject has given consent to the processing for that purpose, or

(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4) The first case is where—

(a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and

(b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5) The second case is where—

(a) the processing is strictly necessary for the law enforcement purpose,

(b) the processing meets at least one of the conditions in Schedule 8, and

(c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(6) The Secretary of State may by regulations amend Schedule 8—

(a) by adding conditions;

(b) by omitting conditions added by regulations under paragraph (a).

(7) Regulations under subsection (6) are subject to the affirmative resolution procedure.

(8) In this section, "sensitive processing" means—

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

36 The second data protection principle

(1) The second data protection principle is that—

(a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

(2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).

(3) Personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose (whether by the controller that collected the data or by another controller) provided that—

(a) the controller is authorised by law to process the data for the other purpose, and

(b) the processing is necessary and proportionate to that other purpose.

(4) Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.

37 The third data protection principle

The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

38 The fourth data protection principle

(1) The fourth data protection principle is that—

(a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and

(b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

(2) In processing personal data for any of the law enforcement purposes, personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments.

(3) In processing personal data for any of the law enforcement purposes, a clear distinction must, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as—

(a) persons suspected of having committed or being about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) persons who are or may be victims of a criminal offence;

(d) witnesses or other persons with information about offences.

(4) All reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes.

(5) For that purpose—

(a) the quality of personal data must be verified before it is transmitted or made available,

(b) in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and

(c) if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

39 The fifth data protection principle

(1) The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

(2) Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

40 The sixth data protection principle

The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

41 Safeguards: archiving

(1) This section applies in relation to the processing of personal data for a law enforcement purpose where the processing is necessary—

(a) for archiving purposes in the public interest,

(b) for scientific or historical research purposes, or

(c) for statistical purposes.

(2) The processing is not permitted if—

(a) it is carried out for the purposes of, or in connection with, measures or decisions with respect to a particular data subject, or

(b) it is likely to cause substantial damage or substantial distress to a data subject.

42 Safeguards: sensitive processing

(1) This section applies for the purposes of section 35(4) and (5) (which require a controller to have an appropriate policy document in place when carrying out sensitive processing in reliance on the consent of the data subject or, as the case may be, in reliance on a condition specified in Schedule 8).

(2) The controller has an appropriate policy document in place in relation to the sensitive processing if the controller has produced a document which—

(a) explains the controller's procedures for securing compliance with the data protection principles (see section 34(1)) in connection with sensitive processing in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, and

(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained.

(3) Where personal data is processed on the basis that an appropriate policy document is in place, the controller must during the relevant period—

(a) retain the appropriate policy document,

(b) review and (if appropriate) update it from time to time, and

(c) make it available to the Commissioner, on request, without charge.

(4) The record maintained by the controller under section 61(1) and, where the sensitive processing is carried out by a processor on behalf of the controller, the record maintained by the processor under section 61(3) must include the following information—

(a) whether the sensitive processing is carried out in reliance on the consent of the data subject or, if not, which condition in Schedule 8 is relied on,

(b) how the processing satisfies section 35 (lawfulness of processing), and

(c) whether the personal data is retained and erased in accordance with the policies described in subsection (2)(b) and, if it is not, the reasons for not following those policies.

(5) In this section, "relevant period", in relation to sensitive processing in reliance on the consent of the data subject or in reliance on a condition specified in Schedule 8, means a period which—

(a) begins when the controller starts to carry out the sensitive processing in reliance on the data subject's consent or (as the case may be) in reliance on that condition, and

(b) ends at the end of the period of 6 months beginning when the controller ceases to carry out the processing.