Data Protection Act 2018

2018 CHAPTER 12

PART 3

LAW ENFORCEMENT PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

VALID FROM 25/05/2018

Scope

29 Processing to which this Part applies

(1) This Part applies to—

(a) the processing by a competent authority of personal data wholly or partly by automated means, and

(b) the processing by a competent authority otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system.

(2) Any reference in this Part to the processing of personal data is to processing to which this Part applies.

(3) For the meaning of "competent authority", see section 30.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

Definitions

30 Meaning of "competent authority"

(1) In this Part, "competent authority" means—

(a) a person specified or described in Schedule 7, and

(b) any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.

(2) But an intelligence service is not a competent authority within the meaning of this Part.

(3) The Secretary of State may by regulations amend Schedule 7—

(a) so as to add or remove a person or description of person;

(b) so as to reflect any change in the name of a person specified in the Schedule.

(4) Regulations under subsection (3) which make provision of the kind described in subsection (3)(a) may also make consequential amendments of section 73(4)(b).

(5) Regulations under subsection (3) which make provision of the kind described in subsection (3)(a), or which make provision of that kind and of the kind described in subsection (3)(b), are subject to the affirmative resolution procedure.

(6) Regulations under subsection (3) which make provision only of the kind described in subsection (3)(b) are subject to the negative resolution procedure.

(7) In this section—

"intelligence service" means—

(a) the Security Service;

(b) the Secret Intelligence Service;

(c) the Government Communications Headquarters;

"statutory function" means a function under or by virtue of an enactment.

Commencement Information

I1 S. 30 in force at Royal Assent for specified purposes, see s. 212(2)(f)

VALID FROM 25/05/2018

31 "The law enforcement purposes"

For the purposes of this Part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

VALID FROM 25/05/2018

32 Meaning of "controller" and "processor"

(1) In this Part, "controller" means the competent authority which, alone or jointly with others—

(a) determines the purposes and means of the processing of personal data, or

(b) is the controller by virtue of subsection (2).

(2) Where personal data is processed only—

(a) for purposes for which it is required by an enactment to be processed, and

(b) by means by which it is required by an enactment to be processed,

the competent authority on which the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller.

(3) In this Part, "processor" means any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).

VALID FROM 25/05/2018

33 Other definitions

(1) This section defines certain other expressions used in this Part.

(2) "Employee", in relation to any person, includes an individual who holds a position (whether paid or unpaid) under the direction and control of that person.

(3) "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

(4) "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

(5) "Recipient", in relation to any personal data, means any person to whom the data is disclosed, whether a third party or not, but it does not include a public authority to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the law.

(6) "Restriction of processing" means the marking of stored personal data with the aim of limiting its processing for the future.

(7) "Third country" means a country or territory other than a member State.

(8) Sections 3 and 205 include definitions of other expressions used in this Part.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

CHAPTER 2

PRINCIPLES

VALID FROM 25/05/2018

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

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(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.

Commencement Information

I2 S. 35 in force at Royal Assent for specified purposes, see s. 212(2)(f)

VALID FROM 25/05/2018

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.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

VALID FROM 25/05/2018

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.

VALID FROM 25/05/2018

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.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

VALID FROM 25/05/2018

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.

VALID FROM 25/05/2018

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).

VALID FROM 25/05/2018

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.

VALID FROM 25/05/2018

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).

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(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.

CHAPTER 3

RIGHTS OF THE DATA SUBJECT

VALID FROM 25/05/2018

Overview and scope

43 Overview and scope

(1) This Chapter—

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(a) imposes general duties on the controller to make information available (see section 44);

(b) confers a right of access by the data subject (see section 45);

(c) confers rights on the data subject with respect to the rectification of personal data and the erasure of personal data or the restriction of its processing (see sections 46 to 48);

(d) regulates automated decision-making (see sections 49 and 50);

(e) makes supplementary provision (see sections 51 to 54).

(2) This Chapter applies only in relation to the processing of personal data for a law enforcement purpose.

(3) But sections 44 to 48 do not apply in relation to the processing of relevant personal data in the course of a criminal investigation or criminal proceedings, including proceedings for the purpose of executing a criminal penalty.

(4) In subsection (3), "relevant personal data" means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority.

(5) In this Chapter, "the controller", in relation to a data subject, means the controller in relation to personal data relating to the data subject.

VALID FROM 25/05/2018

Information: controller's general duties

44 Information: controller's general duties

(1) The controller must make available to data subjects the following information (whether by making the information generally available to the public or in any other way)—

(a) the identity and the contact details of the controller;

(b) where applicable, the contact details of the data protection officer (see sections 69 to 71);

(c) the purposes for which the controller processes personal data;

(d) the existence of the rights of data subjects to request from the controller—

(i) access to personal data (see section 45),

(ii) rectification of personal data (see section 46), and

(iii) erasure of personal data or the restriction of its processing (see section 47);

(e) the existence of the right to lodge a complaint with the Commissioner and the contact details of the Commissioner.

(2) The controller must also, in specific cases for the purpose of enabling the exercise of a data subject's rights under this Part, give the data subject the following—

(a) information about the legal basis for the processing;

(b) information about the period for which the personal data will be stored or, where that is not possible, about the criteria used to determine that period;

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(c) where applicable, information about the categories of recipients of the personal data (including recipients in third countries or international organisations);

(d) such further information as is necessary to enable the exercise of the data subject's rights under this Part.

(3) An example of where further information may be necessary as mentioned in subsection (2)(d) is where the personal data being processed was collected without the knowledge of the data subject.

(4) The controller may restrict, wholly or partly, the provision of information to the data subject under subsection (2) 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.

(5) Where the provision of information to a data subject under subsection (2) is restricted, wholly or partly, the controller must inform the data subject in writing without undue delay—

(a) that the provision of information has been restricted,

(b) of the reasons for the restriction,

(c) of the data subject's right to make a request to the Commissioner under section 51,

(d) of the data subject's right to lodge a complaint with the Commissioner, and

(e) of the data subject's right to apply to a court under section 167.

(6) Subsection (5)(a) and (b) do not apply to the extent that complying with them would undermine the purpose of the restriction.

(7) The controller must—

(a) record the reasons for a decision to restrict (whether wholly or partly) the provision of information to a data subject under subsection (2), and

(b) if requested to do so by the Commissioner, make the record available to the Commissioner.

VALID FROM 25/05/2018

Data subject's right of access

45 Right of access by the data subject

(1) A data subject is entitled to obtain from the controller—

(a) confirmation as to whether or not personal data concerning him or her is being processed, and

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(b) where that is the case, access to the personal data and the information set out in subsection (2).

(2) That information is—

(a) the purposes of and legal basis for the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data has been disclosed (including recipients or categories of recipients in third countries or international organisations);

(d) the period for which it is envisaged that the personal data will be stored or, where that is not possible, the criteria used to determine that period;

(e) the existence of the data subject's rights to request from the controller—

(i) rectification of personal data (see section 46), and

(ii) erasure of personal data or the restriction of its processing (see section 47);

(f) the existence of the data subject's right to lodge a complaint with the Commissioner and the contact details of the Commissioner;

(g) communication of the personal data undergoing processing and of any available information as to its origin.

(3) Where a data subject makes a request under subsection (1), the information to which the data subject is entitled must be provided in writing —

(a) without undue delay, and

(b) in any event, before the end of the applicable time period (as to which see section 54).

(4) The controller may restrict, wholly or partly, the rights conferred by 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.

(5) Where the rights of a data subject under subsection (1) are restricted, wholly or partly, the controller must inform the data subject in writing without undue delay—

(a) that the rights of the data subject have been restricted,

(b) of the reasons for the restriction,

(c) of the data subject's right to make a request to the Commissioner under section 51,

(d) of the data subject's right to lodge a complaint with the Commissioner, and

(e) of the data subject's right to apply to a court under section 167.

(6) Subsection (5)(a) and (b) do not apply to the extent that the provision of the information would undermine the purpose of the restriction.

(7) The controller must—

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(a) record the reasons for a decision to restrict (whether wholly or partly) the rights of a data subject under subsection (1), and

(b) if requested to do so by the Commissioner, make the record available to the Commissioner.

VALID FROM 25/05/2018

Data subject's rights to rectification or erasure etc

46 Right to rectification

(1) The controller must, if so requested by a data subject, rectify without undue delay inaccurate personal data relating to the data subject.

(2) Where personal data is inaccurate because it is incomplete, the controller must, if so requested by a data subject, complete it.

(3) The duty under subsection (2) may, in appropriate cases, be fulfilled by the provision of a supplementary statement.

(4) Where the controller would be required to rectify personal data under this section but the personal data must be maintained for the purposes of evidence, the controller must (instead of rectifying the personal data) restrict its processing.

47 Right to erasure or restriction of processing

(1) The controller must erase personal data without undue delay where—

(a) the processing of the personal data would infringe section 35, 36(1) to (3), 37, 38(1), 39(1), 40, 41 or 42, or

(b) the controller has a legal obligation to erase the data.

(2) Where the controller would be required to erase personal data under subsection (1) but the personal data must be maintained for the purposes of evidence, the controller must (instead of erasing the personal data) restrict its processing.

(3) Where a data subject contests the accuracy of personal data (whether in making a request under this section or section 46 or in any other way), but it is not possible to ascertain whether it is accurate or not, the controller must restrict its processing.

(4) A data subject may request the controller to erase personal data or to restrict its processing (but the duties of the controller under this section apply whether or not such a request is made).

48 Rights under section 46 or 47: supplementary

(1) Where a data subject requests the rectification or erasure of personal data or the restriction of its processing, the controller must inform the data subject in writing—

(a) whether the request has been granted, and

(b) if it has been refused—

(i) of the reasons for the refusal,

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(ii) of the data subject's right to make a request to the Commissioner under section 51,

(iii) of the data subject's right to lodge a complaint with the Commissioner, and

(iv) of the data subject's right to apply to a court under section 167.

(2) The controller must comply with the duty under subsection (1)—

(a) without undue delay, and

(b) in any event, before the end of the applicable time period (see section 54).

(3) The controller may restrict, wholly or partly, the provision of information to the data subject under subsection (1)(b)(i) 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.

(4) Where the rights of a data subject under subsection (1) are restricted, wholly or partly, the controller must inform the data subject in writing without undue delay—

(a) that the rights of the data subject have been restricted,

(b) of the reasons for the restriction,

(c) of the data subject's right to lodge a complaint with the Commissioner, and

(d) of the data subject's right to apply to a court under section 167.

(5) Subsection (4)(a) and (b) do not apply to the extent that the provision of the information would undermine the purpose of the restriction.

(6) The controller must—

(a) record the reasons for a decision to restrict (whether wholly or partly) the provision of information to a data subject under subsection (1)(b)(i), and

(b) if requested to do so by the Commissioner, make the record available to the Commissioner.

(7) Where the controller rectifies personal data, it must notify the competent authority (if any) from which the inaccurate personal data originated.

(8) In subsection (7), the reference to a competent authority includes (in addition to a competent authority within the meaning of this Part) any person that is a competent authority for the purposes of the Law Enforcement Directive in a member State other than the United Kingdom.

(9) Where the controller rectifies, erases or restricts the processing of personal data which has been disclosed by the controller—

(a) the controller must notify the recipients, and

(b) the recipients must similarly rectify, erase or restrict the processing of the personal data (so far as they retain responsibility for it).

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(10) Where processing is restricted in accordance with section 47(3), the controller must inform the data subject before lifting the restriction.

Automated individual decision-making

VALID FROM 25/05/2018

49 Right not to be subject to automated decision-making

(1) A controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law.

(2) A decision is a "significant decision" for the purpose of this section if, in relation to a data subject, it—

(a) produces an adverse legal effect concerning the data subject, or

(b) significantly affects the data subject.

50 Automated decision-making authorised by law: safeguards

(1) A decision is a "qualifying significant decision" for the purposes of this section if—

(a) it is a significant decision in relation to a data subject, and

(b) it is required or authorised by law.

(2) Where a controller takes a qualifying significant decision in relation to a data subject based solely on automated processing—

(a) the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing, and

(b) the data subject may, before the end of the period of 1 month beginning with receipt of the notification, request the controller to—

(i) reconsider the decision, or

(ii) take a new decision that is not based solely on automated processing.

(3) If a request is made to a controller under subsection (2), the controller must, before the end of the period of 1 month beginning with receipt of the request—

(a) consider the request, including any information provided by the data subject that is relevant to it,

(b) comply with the request, and

(c) by notice in writing inform the data subject of—

(i) the steps taken to comply with the request, and

(ii) the outcome of complying with the request.

(4) The Secretary of State may by regulations make such further provision as the Secretary of State considers appropriate to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with the taking of qualifying significant decisions based solely on automated processing.

(5) Regulations under subsection (4)—

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(a) may amend this section, and

(b) are subject to the affirmative resolution procedure.

(6) In this section "significant decision" has the meaning given by section 49(2).

Commencement Information

I3 S. 50 in force at Royal Assent for specified purposes, see s. 212(2)(f)

Supplementary

VALID FROM 25/05/2018

51 Exercise of rights through the Commissioner

(1) This section applies where a controller—

(a) restricts under section 44(4) the information provided to the data subject under section 44(2) (duty of the controller to give the data subject additional information),

(b) restricts under section 45(4) the data subject's rights under section 45(1) (right of access), or

(c) refuses a request by the data subject for rectification under section 46 or for erasure or restriction of processing under section 47.

(2) The data subject may—

(a) where subsection (1)(a) or (b) applies, request the Commissioner to check that the restriction imposed by the controller was lawful;

(b) where subsection (1)(c) applies, request the Commissioner to check that the refusal of the data subject's request was lawful.

(3) The Commissioner must take such steps as appear to the Commissioner to be appropriate to respond to a request under subsection (2) (which may include the exercise of any of the powers conferred by sections 142 and 146).

(4) After taking those steps, the Commissioner must inform the data subject—

(a) where subsection (1)(a) or (b) applies, whether the Commissioner is satisfied that the restriction imposed by the controller was lawful;

(b) where subsection (1)(c) applies, whether the Commissioner is satisfied that the controller's refusal of the data subject's request was lawful.

(5) The Commissioner must also inform the data subject of the data subject's right to apply to a court under section 167.

(6) Where the Commissioner is not satisfied as mentioned in subsection (4)(a) or (b), the Commissioner may also inform the data subject of any further steps that the Commissioner is considering taking under Part 6 .

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

VALID FROM 25/05/2018

52 Form of provision of information etc

(1) The controller must take reasonable steps to ensure that any information that is required by this Chapter to be provided to the data subject is provided in a concise, intelligible and easily accessible form, using clear and plain language.

(2) Subject to subsection (3), the information may be provided in any form, including electronic form.

(3) Where information is provided in response to a request by the data subject under section 45, 46, 47 or 50, the controller must provide the information in the same form as the request where it is practicable to do so.

(4) Where the controller has reasonable doubts about the identity of an individual making a request under section 45, 46 or 47, the controller may—

(a) request the provision of additional information to enable the controller to confirm the identity, and

(b) delay dealing with the request until the identity is confirmed.

(5) Subject to section 53, any information that is required by this Chapter to be provided to the data subject must be provided free of charge.

(6) The controller must facilitate the exercise of the rights of the data subject under sections 45 to 50.

53 Manifestly unfounded or excessive requests by the data subject

(1) Where a request from a data subject under section 45, 46, 47 or 50 is manifestly unfounded or excessive, the controller may—

(a) charge a reasonable fee for dealing with the request, or

(b) refuse to act on the request.

(2) An example of a request that may be excessive is one that merely repeats the substance of previous requests.

(3) In any proceedings where there is an issue as to whether a request under section 45, 46, 47 or 50 is manifestly unfounded or excessive, it is for the controller to show that it is.

(4) The Secretary of State may by regulations specify limits on the fees that a controller may charge in accordance with subsection (1)(a).

(5) Regulations under subsection (4) are subject to the negative resolution procedure.

Commencement Information

I4 S. 53 in force at Royal Assent for specified purposes, see s. 212(2)(f)

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

54 Meaning of "applicable time period"

(1) This section defines "the applicable time period" for the purposes of sections 45(3)(b) and 48(2)(b).

(2) "The applicable time period" means the period of 1 month, or such longer period as may be specified in regulations, beginning with the relevant time.

(3) "The relevant time" means the latest of the following—

(a) when the controller receives the request in question;

(b) when the controller receives the information (if any) requested in connection with a request under section 52(4);

(c) when the fee (if any) charged in connection with the request under section 53 is paid.

(4) The power to make regulations under subsection (2) is exercisable by the Secretary of State.

(5) Regulations under subsection (2) may not specify a period which is longer than 3 months.

(6) Regulations under subsection (2) are subject to the negative resolution procedure.

Commencement Information
I5 S. 54 in force at Royal Assent for specified purposes, see s. 212(2)(f)

VALID FROM 25/05/2018

CHAPTER 4

CONTROLLER AND PROCESSOR

Overview and scope

55 Overview and scope

(1) This Chapter—

(a) sets out the general obligations of controllers and processors (see sections 56 to 65);

(b) sets out specific obligations of controllers and processors with respect to security (see section 66);

(c) sets out specific obligations of controllers and processors with respect to personal data breaches (see sections 67 and 68);

(d) makes provision for the designation, position and tasks of data protection officers (see sections 69 to 71).

(2) This Chapter applies only in relation to the processing of personal data for a law enforcement purpose.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(3) Where a controller is required by any provision of this Chapter to implement appropriate technical and organisational measures, the controller must (in deciding what measures are appropriate) take into account—

(a) the latest developments in technology,

(b) the cost of implementation,

(c) the nature, scope, context and purposes of processing, and

(d) the risks for the rights and freedoms of individuals arising from the processing.

General obligations

56 General obligations of the controller

(1) Each controller must implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of this Part.

(2) Where proportionate in relation to the processing, the measures implemented to comply with the duty under subsection (1) must include appropriate data protection policies.

(3) The technical and organisational measures implemented under subsection (1) must be reviewed and updated where necessary.

57 Data protection by design and default

(1) Each controller must implement appropriate technical and organisational measures which are designed—

(a) to implement the data protection principles in an effective manner, and

(b) to integrate into the processing itself the safeguards necessary for that purpose.

(2) The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing itself.

(3) Each controller must implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

(4) The duty under subsection (3) applies to—

(a) the amount of personal data collected,

(b) the extent of its processing,

(c) the period of its storage, and

(d) its accessibility.

(5) In particular, the measures implemented to comply with the duty under subsection (3) must ensure that, by default, personal data is not made accessible to an indefinite number of people without an individual's intervention.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

58 Joint controllers

(1) Where two or more competent authorities jointly determine the purposes and means of processing personal data, they are joint controllers for the purposes of this Part.

(2) Joint controllers must, in a transparent manner, determine their respective responsibilities for compliance with this Part by means of an arrangement between them, except to the extent that those responsibilities are determined under or by virtue of an enactment.

(3) The arrangement must designate the controller which is to be the contact point for data subjects.

59 Processors

(1) This section applies to the use by a controller of a processor to carry out processing of personal data on behalf of the controller.

(2) The controller may use only a processor who provides guarantees to implement appropriate technical and organisational measures that are sufficient to secure that the processing will—

(a) meet the requirements of this Part, and

(b) ensure the protection of the rights of the data subject.

(3) The processor used by the controller may not engage another processor ("a sub-processor") without the prior written authorisation of the controller, which may be specific or general.

(4) Where the controller gives a general written authorisation to a processor, the processor must inform the controller if the processor proposes to add to the number of sub-processors engaged by it or to replace any of them (so that the controller has the opportunity to object to the proposal).

(5) The processing by the processor must be governed by a contract in writing between the controller and the processor setting out the following—

(a) the subject-matter and duration of the processing;

(b) the nature and purpose of the processing;

(c) the type of personal data and categories of data subjects involved;

(d) the obligations and rights of the controller and processor.

(6) The contract must, in particular, provide that the processor must—

(a) act only on instructions from the controller,

(b) ensure that the persons authorised to process personal data are subject to an appropriate duty of confidentiality,

(c) assist the controller by any appropriate means to ensure compliance with the rights of the data subject under this Part,

(d) at the end of the provision of services by the processor to the controller—

(i) either delete or return to the controller (at the choice of the controller) the personal data to which the services relate, and

(ii) delete copies of the personal data unless subject to a legal obligation to store the copies,

(e) make available to the controller all information necessary to demonstrate compliance with this section, and

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(f) comply with the requirements of this section for engaging sub-processors.

(7) The terms included in the contract in accordance with subsection (6)(a) must provide that the processor may transfer personal data to a third country or international organisation only if instructed by the controller to make the particular transfer.

(8) If a processor determines, in breach of this Part, the purposes and means of processing, the processor is to be treated for the purposes of this Part as a controller in respect of that processing.

60 Processing under the authority of the controller or processor

A processor, and any person acting under the authority of a controller or processor, who has access to personal data may not process the data except—

(a) on instructions from the controller, or

(b) to comply with a legal obligation.

61 Records of processing activities

(1) Each controller must maintain a record of all categories of processing activities for which the controller is responsible.

(2) The controller's record must contain the following information—

(a) the name and contact details of the controller;

(b) where applicable, the name and contact details of the joint controller;

(c) where applicable, the name and contact details of the data protection officer;

(d) the purposes of the processing;

(e) the categories of recipients to whom personal data has been or will be disclosed (including recipients in third countries or international organisations);

(f) a description of the categories of—

(i) data subject, and

(ii) personal data;

(g) where applicable, details of the use of profiling;

(h) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(i) an indication of the legal basis for the processing operations, including transfers, for which the personal data is intended;

(j) where possible, the envisaged time limits for erasure of the different categories of personal data;

(k) where possible, a general description of the technical and organisational security measures referred to in section 66.

(3) Each processor must maintain a record of all categories of processing activities carried out on behalf of a controller.

(4) The processor's record must contain the following information—

(a) the name and contact details of the processor and of any other processors engaged by the processor in accordance with section 59(3);

(b) the name and contact details of the controller on behalf of which the processor is acting;

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(c) where applicable, the name and contact details of the data protection officer;

(d) the categories of processing carried out on behalf of the controller;

(e) where applicable, details of transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of that third country or international organisation;

(f) where possible, a general description of the technical and organisational security measures referred to in section 66.

(5) The controller and the processor must make the records kept under this section available to the Commissioner on request.

62 Logging

(1) A controller (or, where personal data is processed on behalf of the controller by a processor, the processor) must keep logs for at least the following processing operations in automated processing systems—

(a) collection;

(b) alteration;

(c) consultation;

(d) disclosure (including transfers);

(e) combination;

(f) erasure.

(2) The logs of consultation must make it possible to establish—

(a) the justification for, and date and time of, the consultation, and

(b) so far as possible, the identity of the person who consulted the data.

(3) The logs of disclosure must make it possible to establish—

(a) the justification for, and date and time of, the disclosure, and

(b) so far as possible—

(i) the identity of the person who disclosed the data, and

(ii) the identity of the recipients of the data.

(4) The logs kept under subsection (1) may be used only for one or more of the following purposes—

(a) to verify the lawfulness of processing;

(b) to assist with self-monitoring by the controller or (as the case may be) the processor, including the conduct of internal disciplinary proceedings;

(c) to ensure the integrity and security of personal data;

(d) the purposes of criminal proceedings.

(5) The controller or (as the case may be) the processor must make the logs available to the Commissioner on request.

63 Co-operation with the Commissioner

Each controller and each processor must co-operate, on request, with the Commissioner in the performance of the Commissioner's tasks.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

64 Data protection impact assessment

(1) Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.

(2) A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.

(3) A data protection impact assessment must include the following—

(a) a general description of the envisaged processing operations;

(b) an assessment of the risks to the rights and freedoms of data subjects;

(c) the measures envisaged to address those risks;

(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

(4) In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing.

65 Prior consultation with the Commissioner

(1) This section applies where a controller intends to create a filing system and process personal data forming part of it.

(2) The controller must consult the Commissioner prior to the processing if a data protection impact assessment prepared under section 64 indicates that the processing of the data would result in a high risk to the rights and freedoms of individuals (in the absence of measures to mitigate the risk).

(3) Where the controller is required to consult the Commissioner under subsection (2), the controller must give the Commissioner—

(a) the data protection impact assessment prepared under section 64, and

(b) any other information requested by the Commissioner to enable the Commissioner to make an assessment of the compliance of the processing with the requirements of this Part.

(4) Where the Commissioner is of the opinion that the intended processing referred to in subsection (1) would infringe any provision of this Part, the Commissioner must provide written advice to the controller and, where the controller is using a processor, to the processor.

(5) The written advice must be provided before the end of the period of 6 weeks beginning with receipt of the request for consultation by the controller or the processor.

(6) The Commissioner may extend the period of 6 weeks by a further period of 1 month, taking into account the complexity of the intended processing.

(7) If the Commissioner extends the period of 6 weeks, the Commissioner must—

(a) inform the controller and, where applicable, the processor of any such extension before the end of the period of 1 month beginning with receipt of the request for consultation, and

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(b) provide reasons for the delay.

Obligations relating to security

66 Security of processing

(1) Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data.

(2) In the case of automated processing, each controller and each processor must, following an evaluation of the risks, implement measures designed to—

(a) prevent unauthorised processing or unauthorised interference with the systems used in connection with it,

(b) ensure that it is possible to establish the precise details of any processing that takes place,

(c) ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored, and

(d) ensure that stored personal data cannot be corrupted if a system used in connection with the processing malfunctions.

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.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(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.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(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 .

Data protection officers

69 Designation of a data protection officer

(1) The controller must designate a data protection officer, unless the controller is a court, or other judicial authority, acting in its judicial capacity.

(2) When designating a data protection officer, the controller must have regard to the professional qualities of the proposed officer, in particular—

(a) the proposed officer's expert knowledge of data protection law and practice, and

(b) the ability of the proposed officer to perform the tasks mentioned in section 71.

(3) The same person may be designated as a data protection officer by several controllers, taking account of their organisational structure and size.

(4) The controller must publish the contact details of the data protection officer and communicate these to the Commissioner.

70 Position of data protection officer

(1) The controller must ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(2) The controller must provide the data protection officer with the necessary resources and access to personal data and processing operations to enable the data protection officer to—

(a) perform the tasks mentioned in section 71, and

(b) maintain his or her expert knowledge of data protection law and practice.

(3) The controller—

(a) must ensure that the data protection officer does not receive any instructions regarding the performance of the tasks mentioned in section 71;

(b) must ensure that the data protection officer does not perform a task or fulfil a duty other than those mentioned in this Part where such task or duty would result in a conflict of interests;

(c) must not dismiss or penalise the data protection officer for performing the tasks mentioned in section 71.

(4) A data subject may contact the data protection officer with regard to all issues relating to—

(a) the processing of that data subject's personal data, or

(b) the exercise of that data subject's rights under this Part.

(5) The data protection officer, in the performance of this role, must report to the highest management level of the controller.

71 Tasks of data protection officer

(1) The controller must entrust the data protection officer with at least the following tasks—

(a) informing and advising the controller, any processor engaged by the controller, and any employee of the controller who carries out processing of personal data, of that person's obligations under this Part,

(b) providing advice on the carrying out of a data protection impact assessment under section 64 and monitoring compliance with that section,

(c) co-operating with the Commissioner,

(d) acting as the contact point for the Commissioner on issues relating to processing, including in relation to the consultation mentioned in section 65, and consulting with the Commissioner, where appropriate, in relation to any other matter,

(e) monitoring compliance with policies of the controller in relation to the protection of personal data, and

(f) monitoring compliance by the controller with this Part.

(2) In relation to the policies mentioned in subsection (1)(e), the data protection officer's tasks include—

(a) assigning responsibilities under those policies,

(b) raising awareness of those policies,

(c) training staff involved in processing operations, and

(d) conducting audits required under those policies.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(3) In performing the tasks set out in subsections (1) and (2), the data protection officer must have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

VALID FROM 25/05/2018

CHAPTER 5

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES ETC

Overview and interpretation

72 Overview and interpretation

(1) This Chapter deals with the transfer of personal data to third countries or international organisations, as follows—

(a) sections 73 to 76 set out the general conditions that apply;

(b) section 77 sets out the special conditions that apply where the intended recipient of personal data is not a relevant authority in a third country or an international organisation;

(c) section 78 makes special provision about subsequent transfers of personal data.

(2) In this Chapter, "relevant authority", in relation to a third country, means any person based in a third country that has (in that country) functions comparable to those of a competent authority.

General principles for transfers

73 General principles for transfers of personal data

(1) A controller may not transfer personal data to a third country or to an international organisation unless—

(a) the three conditions set out in subsections (2) to (4) are met, and

(b) in a case where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a member State other than the United Kingdom, that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State.

(2) Condition 1 is that the transfer is necessary for any of the law enforcement purposes.

(3) Condition 2 is that the transfer—

(a) is based on an adequacy decision (see section 74),

(b) if not based on an adequacy decision, is based on there being appropriate safeguards (see section 75), or

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(c) if not based on an adequacy decision or on there being appropriate safeguards, is based on special circumstances (see section 76).

(4) Condition 3 is that—

(a) the intended recipient is a relevant authority in a third country or an international organisation that is a relevant international organisation, or

(b) in a case where the controller is a competent authority specified in any of paragraphs 5 to 17, 21, 24 to 28, 34 to 51, 54 and 56 of Schedule 7—

(i) the intended recipient is a person in a third country other than a relevant authority, and

(ii) the additional conditions in section 77 are met.

(5) Authorisation is not required as mentioned in subsection (1)(b) if—

(a) the transfer is necessary for the prevention of an immediate and serious threat either to the public security of a member State or a third country or to the essential interests of a member State, and

(b) the authorisation cannot be obtained in good time.

(6) Where a transfer is made without the authorisation mentioned in subsection (1)(b), the authority in the member State which would have been responsible for deciding whether to authorise the transfer must be informed without delay.

(7) In this section, "relevant international organisation" means an international organisation that carries out functions for any of the law enforcement purposes.

74 Transfers on the basis of an adequacy decision

A transfer of personal data to a third country or an international organisation is based on an adequacy decision where—

(a) the European Commission has decided, in accordance with Article 36 of the Law Enforcement Directive, that—

(i) the third country or a territory or one or more specified sectors within that third country, or

(ii) (as the case may be) the international organisation,

ensures an adequate level of protection of personal data, and

(b) that decision has not been repealed or suspended, or amended in a way that demonstrates that the Commission no longer considers there to be an adequate level of protection of personal data.

75 Transfers on the basis of appropriate safeguards

(1) A transfer of personal data to a third country or an international organisation is based on there being appropriate safeguards where—

(a) a legal instrument containing appropriate safeguards for the protection of personal data binds the intended recipient of the data, or

(b) the controller, having assessed all the circumstances surrounding transfers of that type of personal data to the third country or international organisation, concludes that appropriate safeguards exist to protect the data.

(2) The controller must inform the Commissioner about the categories of data transfers that take place in reliance on subsection (1)(b).

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(3) Where a transfer of data takes place in reliance on subsection (1)—

(a) the transfer must be documented,

(b) the documentation must be provided to the Commissioner on request, and

(c) the documentation must include, in particular—

(i) the date and time of the transfer,

(ii) the name of and any other pertinent information about the recipient,

(iii) the justification for the transfer, and

(iv) a description of the personal data transferred.

76 Transfers on the basis of special circumstances

(1) A transfer of personal data to a third country or international organisation is based on special circumstances where the transfer is necessary—

(a) to protect the vital interests of the data subject or another person,

(b) to safeguard the legitimate interests of the data subject,

(c) for the prevention of an immediate and serious threat to the public security of a member State or a third country,

(d) in individual cases for any of the law enforcement purposes, or

(e) in individual cases for a legal purpose.

(2) But subsection (1)(d) and (e) do not apply if the controller determines that fundamental rights and freedoms of the data subject override the public interest in the transfer.

(3) Where a transfer of data takes place in reliance on subsection (1)—

(a) the transfer must be documented,

(b) the documentation must be provided to the Commissioner on request, and

(c) the documentation must include, in particular—

(i) the date and time of the transfer,

(ii) the name of and any other pertinent information about the recipient,

(iii) the justification for the transfer, and

(iv) a description of the personal data transferred.

(4) For the purposes of this section, a transfer is necessary for a legal purpose if—

(a) it is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) relating to any of the law enforcement purposes,

(b) it is necessary for the purpose of obtaining legal advice in relation to any of the law enforcement purposes, or

(c) it is otherwise necessary for the purposes of establishing, exercising or defending legal rights in relation to any of the law enforcement purposes.

Transfers to particular recipients

77 Transfers of personal data to persons other than relevant authorities

(1) The additional conditions referred to in section 73(4)(b)(ii) are the following four conditions.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(2) Condition 1 is that the transfer is strictly necessary in a specific case for the performance of a task of the transferring controller as provided by law for any of the law enforcement purposes.

(3) Condition 2 is that the transferring controller has determined that there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer.

(4) Condition 3 is that the transferring controller considers that the transfer of the personal data to a relevant authority in the third country would be ineffective or inappropriate (for example, where the transfer could not be made in sufficient time to enable its purpose to be fulfilled).

(5) Condition 4 is that the transferring controller informs the intended recipient of the specific purpose or purposes for which the personal data may, so far as necessary, be processed.

(6) Where personal data is transferred to a person in a third country other than a relevant authority, the transferring controller must inform a relevant authority in that third country without undue delay of the transfer, unless this would be ineffective or inappropriate.

(7) The transferring controller must—

(a) document any transfer to a recipient in a third country other than a relevant authority, and

(b) inform the Commissioner about the transfer.

(8) This section does not affect the operation of any international agreement in force between member States and third countries in the field of judicial co-operation in criminal matters and police co-operation.

Subsequent transfers

78 Subsequent transfers

(1) Where personal data is transferred in accordance with section 73, the transferring controller must make it a condition of the transfer that the data is not to be further transferred to a third country or international organisation without the authorisation of the transferring controller or another competent authority.

(2) A competent authority may give an authorisation under subsection (1) only where the further transfer is necessary for a law enforcement purpose.

(3) In deciding whether to give the authorisation, the competent authority must take into account (among any other relevant factors)—

(a) the seriousness of the circumstances leading to the request for authorisation,

(b) the purpose for which the personal data was originally transferred, and

(c) the standards for the protection of personal data that apply in the third country or international organisation to which the personal data would be transferred.

(4) In a case where the personal data was originally transmitted or otherwise made available to the transferring controller or another competent authority by a member State other than the United Kingdom, an authorisation may not be given under

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

subsection (1) unless that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State.

(5) Authorisation is not required as mentioned in subsection (4) if—

(a) the transfer is necessary for the prevention of an immediate and serious threat either to the public security of a member State or a third country or to the essential interests of a member State, and

(b) the authorisation cannot be obtained in good time.

(6) Where a transfer is made without the authorisation mentioned in subsection (4), the authority in the member State which would have been responsible for deciding whether to authorise the transfer must be informed without delay.

VALID FROM 25/05/2018

CHAPTER 6

SUPPLEMENTARY

79 National security: certificate

(1) A Minister of the Crown may issue a certificate certifying, for the purposes of section 44(4), 45(4), 48(3) or 68(7), that a restriction is a necessary and proportionate measure to protect national security.

(2) The certificate may—

(a) relate to a specific restriction (described in the certificate) which a controller has imposed or is proposing to impose under section 44(4), 45(4), 48(3) or 68(7), or

(b) identify any restriction to which it relates by means of a general description.

(3) Subject to subsection (6), a certificate issued under subsection (1) is conclusive evidence that the specific restriction or (as the case may be) any restriction falling within the general description is, or at any time was, a necessary and proportionate measure to protect national security.

(4) A certificate issued under subsection (1) may be expressed to have prospective effect.

(5) Any person directly affected by the issuing of a certificate under subsection (1) may appeal to the Tribunal against the certificate.

(6) If, on an appeal under subsection (5), the Tribunal finds that, applying the principles applied by a court on an application for judicial review, the Minister did not have reasonable grounds for issuing the certificate, the Tribunal may —

(a) allow the appeal, and

(b) quash the certificate.

(7) Where in any proceedings under or by virtue of this Act, it is claimed by a controller that a restriction falls within a general description in a certificate issued under subsection (1), any other party to the proceedings may appeal to the Tribunal on the ground that the restriction does not fall within that description.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(8) But, subject to any determination under subsection (9), the restriction is to be conclusively presumed to fall within the general description.

(9) On an appeal under subsection (7), the Tribunal may determine that the certificate does not so apply.

(10) A document purporting to be a certificate under subsection (1) is to be—

(a) received in evidence, and

(b) deemed to be such a certificate unless the contrary is proved.

(11) A document which purports to be certified by or on behalf of a Minister of the Crown as a true copy of a certificate issued by that Minister under subsection (1) is—

(a) in any legal proceedings, evidence of that certificate, and

(b) in any legal proceedings in Scotland, sufficient evidence of that certificate.

(12) The power conferred by subsection (1) on a Minister of the Crown is exercisable only by—

(a) a Minister who is a member of the Cabinet, or

(b) the Attorney General or the Advocate General for Scotland.

(13) No power conferred by any provision of Part 6 may be exercised in relation to the imposition of—

(a) a specific restriction in a certificate under subsection (1), or

(b) a restriction falling within a general description in such a certificate.

80 Special processing restrictions

(1) Subsections (3) and (4) apply where, for a law enforcement purpose, a controller transmits or otherwise makes available personal data to an EU recipient or a non-EU recipient.

(2) In this section—

"EU recipient" means—

(a) a recipient in a member State other than the United Kingdom, or

(b) an agency, office or body established pursuant to Chapters 4 and 5 of Title V of the Treaty on the Functioning of the European Union;

"non-EU recipient" means—

(a) a recipient in a third country, or

(b) an international organisation.

(3) The controller must consider whether, if the personal data had instead been transmitted or otherwise made available within the United Kingdom to another competent authority, processing of the data by the other competent authority would have been subject to any restrictions by virtue of any enactment or rule of law.

(4) Where that would be the case, the controller must inform the EU recipient or non-EU recipient that the data is transmitted or otherwise made available subject to compliance by that person with the same restrictions (which must be set out in the information given to that person).

(5) Except as provided by subsection (4), the controller may not impose restrictions on the processing of personal data transmitted or otherwise made available by the controller to an EU recipient.

Status: *Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.*
Changes to legislation: *Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(6) Subsection (7) applies where—

(a) a competent authority for the purposes of the Law Enforcement Directive in a member State other than the United Kingdom transmits or otherwise makes available personal data to a controller for a law enforcement purpose, and

(b) the competent authority in the other member State informs the controller, in accordance with any law of that member State which implements Article 9(3) and (4) of the Law Enforcement Directive, that the data is transmitted or otherwise made available subject to compliance by the controller with restrictions set out by the competent authority.

(7) The controller must comply with the restrictions.

81 Reporting of infringements

(1) Each controller must implement effective mechanisms to encourage the reporting of an infringement of this Part.

(2) The mechanisms implemented under subsection (1) must provide that an infringement may be reported to any of the following persons—

(a) the controller;

(b) the Commissioner.

(3) The mechanisms implemented under subsection (1) must include—

(a) raising awareness of the protections provided by Part 4A of the Employment Rights Act 1996 and Part 5A of the Employment Rights (Northern Ireland) Order 1996 (S.I. 1996/1919 (N.I. 16)), and

(b) such other protections for a person who reports an infringement of this Part as the controller considers appropriate.

(4) A person who reports an infringement of this Part does not breach—

(a) an obligation of confidence owed by the person, or

(b) any other restriction on the disclosure of information (however imposed).

(5) Subsection (4) does not apply if or to the extent that the report includes a disclosure which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

(6) Until the repeal of Part 1 of the Regulation of Investigatory Powers Act 2000 by paragraphs 45 and 54 of Schedule 10 to the Investigatory Powers Act 2016 is fully in force, subsection (5) has effect as if it included a reference to that Part.

Status:
Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.

Changes to legislation:
Data Protection Act 2018, PART 3 is up to date with all changes known to be in force on or before 02 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations.