Data Protection Bill [HL]

[AS AMENDED IN PUBLIC BILL COMMITTEE]

CONTENTS

PART 3

LAW ENFORCEMENT PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

Scope

Definitions

CHAPTER 2

PRINCIPLES

CHAPTER 3

RIGHTS OF THE DATA SUBJECT

Overview and scope

Information: controller's general duties

Data subject's right of access

Data subject's rights to rectification or erasure etc

CHAPTER 6

EXEMPTIONS

PART 5

THE INFORMATION COMMISSIONER

The Commissioner

General functions

International role

Codes of practice

Consensual audits

Records of national security certificates

Information provided to the Commissioner

PART 7

SUPPLEMENTARY AND FINAL PROVISION

Regulations under this Act

Changes to the Data Protection Convention

Rights of the data subject

Representation of data subjects

Framework for Data Processing by Government

Offences

The Tribunal

Definitions

A

B I L L

[AS AMENDED IN PUBLIC BILL COMMITTEE]

TO

Make provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes.

BE IT ENACTED by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

PART 1

PRELIMINARY

1 Overview

(1) This Act makes provision about the processing of personal data.

(2) Most processing of personal data is subject to the GDPR.

(3) Part 2 supplements the GDPR (see Chapter 2) and applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply (see Chapter 3).

(4) Part 3 makes provision about the processing of personal data by competent authorities for law enforcement purposes and implements the Law Enforcement Directive.

(5) Part 4 makes provision about the processing of personal data by the intelligence services.

(6) Part 5 makes provision about the Information Commissioner.

(7) Part 6 makes provision about the enforcement of the data protection legislation.

(8) Part 7 makes supplementary provision, including provision about the application of this Act to the Crown and to Parliament.

2 Protection of personal data

(1) The GDPR, the applied GDPR and this Act protect individuals with regard to the processing of personal data, in particular by—

(a) requiring personal data to be processed lawfully and fairly, on the basis of the data subject's consent or another specified basis,

(b) conferring rights on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and

(c) conferring functions on the Commissioner, giving the holder of that office responsibility for monitoring and enforcing their provisions.

(2) When carrying out functions under the GDPR, the applied GDPR and this Act, the Commissioner must have regard to the importance of securing an appropriate level of protection for personal data, taking account of the interests of data subjects, controllers and others and matters of general public interest.

3 Terms relating to the processing of personal data

(1) This section defines some terms used in this Act.

(2) "Personal data" means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)).

(3) "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to—

(a) an identifier such as a name, an identification number, location data or an online identifier, or

(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

(4) "Processing", in relation to ~~personal data~~information, means an operation or set of operations which is performed on ~~personal data~~information, or on sets of ~~personal data~~information, such as—

(a) collection, recording, organisation, structuring or storage,

(b) adaptation or alteration,

(c) retrieval, consultation or use,

(d) disclosure by transmission, dissemination or otherwise making available,

(e) alignment or combination, or

(f) restriction, erasure or destruction,

(subject to subsection (14)(c) and sections 5(7), 29(2) and 82(3), which make provision about references to processing in the different Parts of this Act).

(5) "Data subject" means the identified or identifiable living individual to whom personal data relates.

(6) "Controller" and "processor", in relation to the processing of personal data to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies, have the same meaning as in that Chapter or Part (see sections 5, 6, 32 and ~~83~~83 and see also subsection (14)(c)).

(7) "Filing system" means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.

(8) "The Commissioner" means the Information Commissioner (see section 114).

(9) "The data protection legislation" means—
- (a) the GDPR,
- (b) the applied GDPR,
- (c) this Act,
- (d) regulations made under this Act, and
- (e) regulations made under section 2(2) of the European Communities Act 1972 which relate to the GDPR or the Law Enforcement Directive.

(10) "The GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

(11) "The applied GDPR" means the GDPR as applied by Chapter 3 of Part 2.

(12) "The Law Enforcement Directive" means Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

(13) "The Data Protection Convention" means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data which was opened for signature on 28 January 1981, as amended up to the day on which this Act is passed.

(14) In Parts 5 to 7, except where otherwise provided—
- (a) references to the GDPR are to the GDPR read with Chapter 2 of Part 2 and include the applied GDPR read with Chapter 3 of Part 2;
- (b) references to Chapter 2 of Part 2, or to a provision of that Chapter, include that Chapter or that provision as applied by Chapter 3 of Part 2;
- (c) references to personal data, and the processing of personal data, are to personal data and processing to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies;
- (d) references to ~~processing and personal data~~ a controller or processor are to a controller or processor in relation to the processing ~~and~~ of personal data to which Chapter ~~2~~ 2 or ~~3~~ 3 of Part ~~2~~2, Part ~~3~~ 3 or Part ~~4~~ 4 applies.

(15) There is an index of defined expressions in section ~~199~~197.

PART 2

GENERAL PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

4 Processing to which this Part applies

(1) This Part is relevant to most processing of personal data.

(2) Chapter 2 of this Part—

(a) applies to the types of processing of personal data to which the GDPR applies by virtue of Article 2 of the GDPR, and

(b) supplements, and must be read with, the GDPR.

(3) Chapter 3 of this Part—

(a) applies to certain types of processing of personal data to which the GDPR does not apply (see section 21), and

(b) makes provision for a regime broadly equivalent to the GDPR to apply to such processing.

5 Definitions

(1) Terms used in Chapter 2 of this Part and in the GDPR have the same meaning in Chapter 2 as they have in the GDPR.

(2) In subsection (1), the reference to a term's meaning in the GDPR is to its meaning in the GDPR read with any provision of Chapter 2 which modifies the term's meaning for the purposes of the GDPR.

(3) Subsection (1) is subject to any provision in Chapter 2 which provides expressly for the term to have a different meaning and to section ~~197~~195.

(4) Terms used in Chapter 3 of this Part and in the applied GDPR have the same meaning in Chapter 3 as they have in the applied GDPR.

(5) In subsection (4), the reference to a term's meaning in the applied GDPR is to its meaning in the GDPR read with any provision of Chapter 2 (as applied by Chapter 3) or Chapter 3 which modifies the term's meaning for the purposes of the applied GDPR.

(6) Subsection (4) is subject to any provision in Chapter 2 (as applied by Chapter 3) or Chapter 3 which provides expressly for the term to have a different meaning.

(7) A reference in Chapter 2 or Chapter 3 of this Part to the processing of personal data is to processing to which the Chapter applies.

(8) Sections 3 and ~~198~~ 196 include definitions of other expressions used in this Part.

CHAPTER 2

THE GDPR

Meaning of certain terms used in the GDPR

6 Meaning of "controller"

(1) The definition of "controller" in Article 4(7) of the GDPR has effect subject to—

(a) subsection (2),

(b) section ~~202~~200, and

(c) section ~~203~~201.

(2) For the purposes of the GDPR, 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 person on whom the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller.

7 Meaning of "public authority" and "public body"

(1) For the purposes of the GDPR, the following (and only the following) are "public authorities" and "public bodies" under the law of the United Kingdom—

(a) a public authority as defined by the Freedom of Information Act 2000,

(b) a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002 (asp 13), and

(c) an authority or ~~a~~ body specified or described by the Secretary of State in regulations,

subject to subsections (2) and (3).

(2) An authority or body that falls within subsection (1) is only a "public authority" or "public body" when performing a task carried out in the public interest or in the exercise of official authority vested in it.

(3) The Secretary of State may by regulations provide that a person specified or described in the regulations that is a public authority described in subsection (1)(a) or (b) is not a "public authority" or "public body" for the purposes of the GDPR.

(4) Regulations under this section are subject to the affirmative resolution procedure.

Lawfulness of processing

8 Lawfulness of processing: public interest etc

In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority includes processing of personal data that is necessary for—

(a) the administration of justice,

(b) the exercise of a function of either House of Parliament,

(c) the exercise of a function conferred on a person by an enactment or rule of law~~, or~~,

(d) the exercise of a function of the Crown, a Minister of the Crown or a government department~~.~~, or

(e) an activity that supports or promotes democratic engagement.

9 Child's consent in relation to information society services

In Article 8(1) of the GDPR (conditions applicable to child's consent in relation to information society services)—

(a) references to "16 years" are to be read as references to "13 years", and

(b) the reference to "information society services" does not include preventive or counselling services.

Special categories of personal data

10 Special categories of personal data and criminal convictions etc data

(1) Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2)—

(a) point (b) (employment, social security and social protection);

(b) point (g) (substantial public interest);

(c) point (h) (health and social care);

(d) point (i) (public health);

(e) point (j) (archiving, research and statistics).

(2) The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the GDPR for authorisation by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part ~~1~~1 of Schedule 1.

(3) The processing meets the requirement in point (g) of Article 9(2) of the GDPR for a basis in the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part ~~2~~2 of Schedule 1.

(4) Subsection (5) makes provision about the processing of personal data relating to criminal convictions and offences or related security measures that is not carried out under the control of official authority.

(5) The processing meets the requirement in Article 10 of the GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part ~~1~~1, ~~2~~2 or ~~3~~3 of Schedule 1.

(6) The Secretary of State may by regulations—

(a) amend Schedule 1—

(i) by adding or varying conditions or safeguards, and

(ii) by omitting conditions or safeguards added by regulations under this section, and

(b) consequentially amend this section.

(7) Regulations under this section are subject to the affirmative resolution procedure.

11 Special categories of personal data etc: supplementary

(1) For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of secrecy) include circumstances in which it is carried out—

(a) by or under the responsibility of a health professional or a social work professional, or

(b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

(2) In Article 10 of the GDPR and section 10, references to personal data relating to criminal convictions and offences or related security measures include personal data relating to—

(a) the alleged commission of offences by the data subject, or

(b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

Rights of the data subject

12 Limits on fees that may be charged by controllers

(1) The Secretary of State may by regulations specify limits on the fees that a controller may charge in reliance on—

(a) Article 12(5) of the GDPR (reasonable fees when responding to manifestly unfounded or excessive requests), or

(b) Article 15(3) of the GDPR (reasonable fees for provision of further copies).

(2) The Secretary of State may by regulations—

(a) require controllers of a description specified in the regulations to produce and publish guidance about the fees that they charge in reliance on those provisions, and

(b) specify what the guidance must include.

(3) Regulations under this section are subject to the negative resolution procedure.

13 Obligations of credit reference agencies

(1) This section applies where a controller is a credit reference agency (within the meaning of section 145(8) of the Consumer Credit Act 1974).

(2) The controller's obligations under Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) are taken to apply only to personal data relating to the data subject's financial standing, unless the data subject has indicated a contrary intention.

(3) Where the controller discloses personal data in pursuance of Article 15(1) to (3) of the GDPR, the disclosure must be accompanied by a statement informing the

data subject of the data subject's rights under section 159 of the Consumer Credit Act 1974 (correction of wrong information).

14 Automated decision-making authorised by law: safeguards

(1) This section makes provision for the purposes of Article 22(2)(b) of the GDPR (exception from Article 22(1) of the GDPR for significant decisions based solely on automated processing that are authorised by law and subject to safeguards for the data subject's rights, freedoms and legitimate interests).

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

(a) produces legal effects concerning the data subject, or

(b) similarly significantly affects the data subject.

(3) 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,

(b) it is required or authorised by law, and

(c) it does not fall within Article 22(2)(a) or (c) of the GDPR (decisions necessary to a contract or made with the data subject's consent).

(4) 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 ~~21 days~~ 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.

(5) If a request is made to a controller under subsection (4), the controller must, ~~before the end of~~ within the period ~~of 21 days beginning with receipt~~ described in Article 12(3) of the ~~request~~GDPR—

(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.

(6) In connection with this section, a controller has the powers and obligations under Article 12 of the GDPR (transparency, procedure for extending time for acting on request, fees, manifestly unfounded or excessive requests etc) that apply in connection with Article 22 of the GDPR.

(7) 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.

(8) Regulations under subsection (7)—

(a) may amend this section, and
(b) are subject to the affirmative resolution procedure.

Restrictions on data subject's rights

15 Exemptions etc

(1) Schedules 2, 3 and 4 make provision for exemptions from, and restrictions and adaptations of the application of, rules of the GDPR.

(2) In Schedule 2—
(a) Part ~~1~~1 makes provision adapting or restricting the application of rules contained in Articles 13 to 21 and 34 of the GDPR in specified circumstances, as allowed for by Article 6(3) and Article 23(1) of the GDPR;
(b) Part ~~2~~2 makes provision restricting the application of rules contained in Articles 13 to 21 and 34 of the GDPR in specified circumstances, as allowed for by Article 23(1) of the GDPR;
(c) Part ~~3~~3 makes provision restricting the application of Article 15 of the GDPR where this is necessary to protect the rights of others, as allowed for by Article 23(1) of the GDPR;
(d) Part ~~4~~4 makes provision restricting the application of rules contained in Articles 13 to 15 of the GDPR in specified circumstances, as allowed for by Article 23(1) of the GDPR;
(e) Part ~~5~~5 makes provision containing exemptions or derogations from Chapters II, III, IV, V and VII of the GDPR for reasons relating to freedom of expression, as allowed for by Article 85(2) of the GDPR;
(f) Part ~~6~~6 makes provision containing derogations from rights contained in Articles 15, 16, 18, 19, 20 and 21 of the GDPR for scientific or historical research purposes, statistical purposes and archiving purposes, as allowed for by Article 89(2) and (3) of the GDPR.

(3) Schedule 3 makes provision restricting the application of rules contained in Articles 13 to 21 of the GDPR to health, social work, education and child abuse data, as allowed for by Article 23(1) of the GDPR.

(4) Schedule 4 makes provision restricting the application of rules contained in Articles 13 to 21 of the GDPR to information the disclosure of which is prohibited or restricted by an enactment, as allowed for by Article 23(1) of the GDPR.

(5) In connection with the safeguarding of national security and with defence, see Chapter 3 of this Part and the exemption in section 26.

16 Power to make further exemptions etc by regulations

(1) The following powers to make provision altering the application of the GDPR may be exercised by way of regulations made by the Secretary of State under this section—
(a) the power in Article 6(3) for Member State law to lay down a legal basis containing specific provisions to adapt the application of rules of the GDPR where processing is necessary for compliance with a legal obligation, for the performance of a task in the public interest or in the exercise of official authority;

(b) the power in Article 23(1) to make a legislative measure restricting the scope of the obligations and rights mentioned in that Article where necessary and proportionate to safeguard certain objectives of general public interest;

(c) the power in Article 85(2) to provide for exemptions or derogations from certain Chapters of the GDPR where necessary to reconcile the protection of personal data with the freedom of expression and information.

(2) Regulations under this section may—

(a) amend Schedules 2 to 4—

(i) by adding or varying provisions, and

(ii) by omitting provisions added by regulations under this section, and

(b) consequentially amend section 15.

(3) Regulations under this section are subject to the affirmative resolution procedure.

Accreditation of certification providers

17 Accreditation of certification providers

(1) Accreditation of a person as a certification provider is only valid when carried out by—

(a) the Commissioner, or

(b) the national accreditation body.

(2) The Commissioner may only accredit a person as a certification provider where the Commissioner—

(a) has published a statement that the Commissioner will carry out such accreditation, and

(b) has not published a notice withdrawing that statement.

(3) The national accreditation body may only accredit a person as a certification provider where the Commissioner—

(a) has published a statement that the body may carry out such accreditation, and

(b) has not published a notice withdrawing that statement.

(4) The publication of a notice under subsection (2)(b) or (3)(b) does not affect the validity of any accreditation carried out before its publication.

(5) Schedule 5 makes provision about reviews of, and appeals from, a decision relating to accreditation of a person as a certification provider.

(6) The national accreditation body may charge a reasonable fee in connection with, or incidental to, the carrying out of the body's functions under this section, Schedule 5 and Article 43 of the GDPR.

(7) The national accreditation ~~authority~~ body must provide the Secretary of State with such information relating to its functions under this section, Schedule 5 and Article 43 of the GDPR as the Secretary of State may reasonably require.

(8) In this section—

"certification provider" means a person who issues certification for the purposes of Article 42 of the GDPR;

"the national accreditation body" means the national accreditation body for the purposes of Article 4(1) of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

Transfers of personal data to third countries etc

18 Transfers of personal data to third countries etc

(1) The Secretary of State may by regulations specify, for the purposes of Article 49(1)(d) of the GDPR—

(a) circumstances in which a transfer of personal data to a third country or international organisation is to be taken to be necessary for important reasons of public interest, and

(b) circumstances in which a transfer of personal data to a third country or international organisation which is not required by an enactment is not to be taken to be necessary for important reasons of public interest.

(2) The Secretary of State may by regulations restrict the transfer of a category of personal data to a third country or international organisation where—

(a) the transfer is not authorised by an adequacy decision under Article 45(3) of the GDPR, and

(b) the Secretary of State considers the restriction to be necessary for important reasons of public interest.

(3) Regulations under this section—

(a) are subject to the made affirmative resolution procedure where the Secretary of State has made an urgency statement in respect of them;

(b) are otherwise subject to the affirmative resolution procedure.

(4) For the purposes of this section, an urgency statement is a reasoned statement that the Secretary of State considers it desirable for the regulations to come into force without delay.

Specific processing situations

19 Processing for archiving, research and statistical purposes: safeguards

(1) This section makes provision about—

(a) processing of personal data that is necessary for archiving purposes in the public interest,

(b) processing of personal data that is necessary for scientific or historical research purposes, and

(c) processing of personal data that is necessary for statistical purposes.

(2) Such processing does not satisfy the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if it is likely to cause substantial damage or substantial distress to a data subject.

(3) Such processing does not satisfy that requirement if the processing is carried out for the purposes of measures or decisions with respect to a particular data subject, unless the purposes for which the processing is necessary include the purposes of approved medical research.

(4) In this section—

"approved medical research" means medical research carried out by a person who has approval to carry out that research from—

(a) a research ethics committee recognised or established by the Health Research Authority under Chapter 2 of Part 3 of the Care Act 2014, or

(b) a body appointed by any of the following for the purpose of assessing the ethics of research involving individuals—

(i) the Secretary of State, the Scottish Ministers, the Welsh Ministers, or a Northern Ireland department;

(ii) a relevant NHS body;

(iii) United Kingdom Research and Innovation or a body that is a Research Council for the purposes of the Science and Technology Act 1965;

(iv) an institution that is a research institution for the purposes of Chapter 4A of Part 7 of the Income Tax (Earnings and Pensions) Act 2003 (see section 457 of that Act);

"relevant NHS body" means—

(a) an NHS trust or NHS foundation trust in England,

(b) an NHS trust or Local Health Board in Wales,

(c) a Health Board or Special Health Board constituted under section 2 of the National Health Service (Scotland) Act 1978,

(d) the Common Services Agency for the Scottish Health Service, or

(e) any of the health and social care bodies in Northern Ireland falling within paragraphs (a) to (~~d~~e) of section 1(5) of the Health and Social Care (Reform) Act (Northern Ireland) 2009 (c. 1 (N.I.)).

(5) The Secretary of State may by regulations change the meaning of "approved medical research" for the purposes of this section, including by amending subsection (4).

(6) Regulations under subsection (5) are subject to the affirmative resolution procedure.

Minor definition

20 Meaning of "court"

Section 5(1) (terms used in this Chapter to have the same meaning as in the GDPR) does not apply to references in this Chapter to a court and, accordingly, such references do not include a tribunal.

CHAPTER 3

OTHER GENERAL PROCESSING

Scope

21 Processing to which this Chapter applies

(1) This Chapter applies to the automated or structured processing of personal data in the course of—

(a) an activity which is outside the scope of European Union law, or

(b) an activity which falls within the scope of Article 2(2)(b) of the GDPR (common foreign and security policy activities),

provided that the processing is not processing to which Part 3 (law enforcement processing) or Part 4 (intelligence services processing) applies.

(2) This Chapter also applies to the manual unstructured processing of personal data held by an FOI public authority.

(3) This Chapter does not apply to the processing of personal data by an individual in the course of a purely personal or household activity.

(4) In this section—

"the automated or structured processing of personal data" means—

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

(b) the processing 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;

"the manual unstructured processing of personal data" means the processing of personal data which is not the automated or structured processing of personal data.

(5) In this Chapter, "FOI public authority" means—

(a) a public authority as defined in the Freedom of Information Act 2000, or

(b) a Scottish public authority as defined in the Freedom of Information (Scotland) Act 2002 (asp 13).

(6) References in this Chapter to personal data "held" by an FOI public authority are to be interpreted—

(a) in relation to England and Wales and Northern Ireland, in accordance with section 3(2) of the Freedom of Information Act 2000, and

(b) in relation to Scotland, in accordance with section 3(2), (4) and (5) of the Freedom of Information (Scotland) Act 2002 (asp 13),

but such references do not include information held by an intelligence service (as defined in section 82) on behalf of an FOI public authority.

(7) But personal data is not to be treated as "held" by an FOI public authority for the purposes of this Chapter, where—

(a) section 7 of the Freedom of Information Act 2000 prevents Parts 1 to 5 of that Act from applying to the personal data, or

(b) section 7(1) of the Freedom of Information (Scotland) Act 2002 (asp 13) prevents that Act from applying to the personal data.

Application of the GDPR

22 Application of the GDPR to processing to which this Chapter applies

(1) The GDPR applies to the processing of personal data to which this Chapter applies but as if its Articles were part of an Act extending to England and Wales, Scotland and Northern Ireland.

(2) Chapter 2 of this Part applies for the purposes of the applied GDPR as it applies for the purposes of the GDPR.

(3) In this Chapter, "the applied Chapter 2" means Chapter 2 of this Part as applied by this Chapter.

(4) Schedule 6 contains provision modifying—

(a) the GDPR as it applies by virtue of subsection (1) (see Part ~~1~~1);

(b) Chapter 2 of this Part as it applies by virtue of subsection (2) (see Part ~~2~~2).

(5) A question as to the meaning or effect of a provision of the applied GDPR, or the applied Chapter 2, is to be determined consistently with the interpretation of the equivalent provision of the GDPR, or Chapter 2 of this Part, as it applies otherwise than by virtue of this Chapter, except so far as Schedule 6 requires a different interpretation.

23 Power to make provision in consequence of regulations related to the GDPR

(1) The Secretary of State may by regulations make provision in connection with the processing of personal data to which this Chapter applies which is equivalent to that made by GDPR regulations, subject to such modifications as the Secretary of State considers appropriate.

(2) In this section, "GDPR regulations" means regulations made under section 2(2) of the European Communities Act 1972 which make provision relating to the GDPR.

(3) Regulations under subsection (1) may apply a provision of GDPR regulations, with or without modification.

(4) Regulations under subsection (1) may amend or repeal a provision of—

(a) the applied GDPR;

(b) this Chapter;

(c) Parts 5 to 7, in so far as they apply in relation to the applied GDPR.

(5) Regulations under this section are subject to the affirmative resolution procedure.

Exemptions etc

24 Manual unstructured data held by FOI public authorities

(1) The provisions of the applied GDPR and this Act listed in subsection (2) do not apply to personal data to which this Chapter applies by virtue of section 21(2) (manual unstructured personal data held by FOI public authorities).

(2) Those provisions are—

(a) in Chapter II of the applied GDPR (principles)—
  (i) Article 5(1)(a) to (c), (e) and (f) (principles relating to processing, other than the accuracy principle),
  (ii) Article 6 (lawfulness),
  (iii) Article 7 (conditions for consent),
  (iv) Article 8(1) and (2) (child's consent),
  (v) Article 9 (processing of special categories of personal data),
  (vi) Article 10 (data relating to criminal convictions etc), and
  (vii) Article 11(2) (processing not requiring identification);
(b) in Chapter III of the applied GDPR (rights of the data subject)—
  (i) Article 13(1) to (3) (personal data collected from data subject: information to be provided),
  (ii) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),
  (iii) Article 20 (right to data portability), and
  (iv) Article 21(1) (objections to processing);
(c) in Chapter V of the applied GDPR, Articles 44 to 49 (transfers of personal data to third countries or international organisations);
(d) sections ~~170~~ 166 and ~~171~~ 167 of this Act;

(see also paragraph ~~1(2)~~1(2) of Schedule 17).

(3) In addition, the provisions of the applied GDPR listed in subsection (4) do not apply to personal data to which this Chapter applies by virtue of section 21(2) where the personal data relates to appointments, removals, pay, discipline, superannuation or other personnel matters in relation to—
(a) service in any of the armed forces of the Crown;
(b) service in any office or employment under the Crown or under any public authority;
(c) service in any office or employment, or under any contract for services, in respect of which power to take action, or to determine or approve the action taken, in such matters is vested in—
  (i) Her Majesty,
  (ii) a Minister of the Crown,
  (iii) the National Assembly for Wales,
  (iv) the Welsh Ministers,
  (v) a Northern Ireland Minister (within the meaning of the Freedom of Information Act 2000), or
  (vi) an FOI public authority.

(4) Those provisions are—
(a) the remaining provisions of Chapters II and III (principles and rights of the data subject);
(b) Chapter IV (controller and processor);
(c) Chapter IX (specific processing situations).

(5) A controller is not obliged to comply with Article 15(1) to (3) of the applied GDPR (right of access by the data subject) in relation to personal data to which this Chapter applies by virtue of section 21(2) if—
(a) the request under that Article does not contain a description of the personal data, or

(b) the controller estimates that the cost of complying with the request so far as relating to the personal data would exceed the appropriate maximum.

(6) Subsection (5)(b) does not remove the controller's obligation to confirm whether or not personal data concerning the data subject is being processed unless the estimated cost of complying with that obligation alone in relation to the personal data would exceed the appropriate maximum.

(7) An estimate for the purposes of this section must be made in accordance with regulations under section 12(5) of the Freedom of Information Act 2000.

(8) In subsections (5) and (6), "the appropriate maximum" means the maximum amount specified by the Secretary of State by regulations.

(9) Regulations under subsection (8) are subject to the negative resolution procedure.

25 Manual unstructured data used in longstanding historical research

(1) The provisions of the applied GDPR listed in subsection (2) do not apply to personal data to which this Chapter applies by virtue of section 21(2) (manual unstructured personal data held by FOI public authorities) at any time when—

(a) the personal data—

(i) is subject to processing which was already underway immediately before 24 October 1998, and

(ii) is processed only for the purposes of historical research, and

(b) the processing is not carried out—

(i) for the purposes of measures or decisions with respect to a particular ~~individual~~data subject, or

(ii) in a way that causes, or is likely to cause, substantial damage or substantial distress to a data subject.

(2) Those provisions are—

(a) in Chapter II of the applied GDPR (principles), Article 5(1)(d) (the accuracy principle), and

(b) in Chapter III of the applied GDPR (rights of the data subject)—

(i) Article 16 (right to rectification), and

(ii) Article 17(1) and (2) (right to erasure).

(3) The exemptions in this section apply in addition to the exemptions in section 24.

26 National security and defence exemption

(1) A provision of the applied GDPR or this Act mentioned in subsection (2) does not apply to personal data to which this Chapter applies if exemption from the provision is required for—

(a) the purpose of safeguarding national security, or

(b) defence purposes.

(2) The provisions are—

(a) Chapter II of the applied GDPR (principles) except for—

(i) Article 5(1)(a) (lawful, fair and transparent processing), so far as it requires processing of personal data to be lawful;

(ii) Article 6 (lawfulness of processing);
(iii) Article 9 (processing of special categories of personal data);
(b) Chapter III of the applied GDPR (rights of data subjects);
(c) in Chapter IV of the applied GDPR—
(i) Article 33 (notification of personal data breach to the Commissioner);
(ii) Article 34 (communication of personal data breach to the data subject);
(d) Chapter V of the applied GDPR (transfers of personal data to third countries or international organisations);
(e) in Chapter VI of the applied GDPR—
(i) Article 57(1)(a) and (h) (Commissioner's duties to monitor and enforce the applied GDPR and to conduct investigations);
(ii) Article 58 (investigative, corrective, authorisation and advisory powers of Commissioner);
(f) Chapter VIII of the applied GDPR (remedies, liabilities and penalties) except for—
(i) Article 83 (general conditions for imposing administrative fines);
(ii) Article 84 (penalties);
(g) in Part 5 of this Act—
(i) in section 115 (general functions of the Commissioner), subsections (3) and (8);
(ii) in section 115, subsection (9), so far as it relates to Article 58(2)(i) of the applied GDPR;
(iii) section 119 (inspection in accordance with international obligations);
(h) in Part 6 of this Act—
(i) sections ~~143~~ 141 to ~~153~~ 151 and Schedule 15 (Commissioner's notices and powers of entry and inspection);
(ii) sections ~~170~~ 166 to ~~173~~ 169 (offences relating to personal data);
(i) in Part 7 of this Act, section ~~183~~ 180 (representation of data subjects).

27 National security: certificate

(1) Subject to subsection (3), a certificate signed by a Minister of the Crown certifying that exemption from all or any of the provisions listed in section 26(2) is, or at any time was, required in relation to any personal data for the purpose of safeguarding national security is conclusive evidence of that fact.

(2) A certificate under subsection (1)—
(a) may identify the personal data to which it applies by means of a general description, and
(b) may be expressed to have prospective effect.

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

(4) If, on an appeal under subsection (3), 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 a certificate, the Tribunal may—
(a) allow the appeal, and

(b) quash the certificate.

(5) Where, in any proceedings under or by virtue of the applied GDPR or this Act, it is claimed by a controller that a certificate under subsection (1) which identifies the personal data to which it applies by means of a general description applies to any personal data, another party to the proceedings may appeal to the Tribunal on the ground that the certificate does not apply to the personal data in question.

(6) But, subject to any determination under subsection (7), the certificate is to be conclusively presumed so to apply.

(7) On an appeal under subsection (5), the Tribunal may determine that the certificate does not so apply.

(8) 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.

(9) 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;
(b) in any legal proceedings in Scotland, sufficient evidence of that certificate.

(10) 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.

28 National security and defence: modifications to Articles 9 and 32 of the applied GDPR

(1) Article 9(1) of the applied GDPR (prohibition on processing of special categories of personal data) does not prohibit the processing of personal data to which this Chapter applies to the extent that the processing is carried out—
(a) for the purpose of safeguarding national security or for defence purposes, and
(b) with appropriate safeguards for the rights and freedoms of data subjects.

(2) Article 32 of the applied GDPR (security of processing) does not apply to a controller or processor to the extent that the controller or the processor (as the case may be) is processing personal data to which this Chapter applies for—
(a) the purpose of safeguarding national security, or
(b) defence purposes.

(3) Where Article 32 of the applied GDPR does not apply, the controller or the processor must implement security measures appropriate to the risks arising from the processing of the personal data.

(4) For the purposes of subsection (3), where the processing of personal data is carried out wholly or partly by automated means, the controller or the 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 the processing,

(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.

PART 3

LAW ENFORCEMENT PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

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.

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 ~~a person to,~~ or remove a person ~~from, the Schedule~~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.

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.

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).

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 ~~198~~ 196 include definitions of other expressions used in this Part.

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 ~~an individual~~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 ~~with the day~~ when the controller ceases to carry out the processing.

CHAPTER 3

RIGHTS OF THE DATA SUBJECT

Overview and scope

43 Overview and scope

(1) This Chapter—

(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.

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;
(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 ~~165~~163.

(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.

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

(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 ~~165~~163.

(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—

(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.

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 ~~data~~ 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,

(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 ~~165~~163.

(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 ~~165~~163.

(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).

(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

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 ~~21 days~~ 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 ~~21 days~~ 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)—

(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).

Supplementary

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 ~~data~~ 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 ~~processing of personal data relating to~~ restriction imposed by the ~~data subject complies with this Part~~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 ~~143~~ 141 and ~~146~~144).

(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 ~~processing~~ restriction imposed by the controller ~~of personal data relating to the data subject complies with this Part~~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 ~~165~~163.

(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.

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 or~~ 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 or~~ 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.

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 ~~one~~ 1 month, or such longer period as may be specified in regulations, beginning with the relevant ~~day~~time.

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

(a) ~~the day on which~~ when the controller receives the request in question;

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

(c) ~~the day on which~~ 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 ~~three~~ 3 months.

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

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.

(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.

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

(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;

(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.

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 ~~one~~ 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 ~~one~~ 1 month beginning with receipt of the request for consultation, and

(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.

67 Notification of a personal data breach to the Commissioner

(1) If a controller becomes aware of a personal data breach in relation to personal data for which the controller is responsible, the controller must notify the breach to the Commissioner—
(a) without undue delay, and
(b) where feasible, not later than 72 hours after becoming aware of it.

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

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

(4) Subject to subsection (5), the notification must include—
(a) a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) the name and contact details of the data protection officer or other contact point from whom more information can be obtained;
(c) a description of the likely consequences of the personal data breach;
(d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

(6) The controller must record the following information in relation to a personal data breach—
(a) the facts relating to the breach,
(b) its effects, and
(c) the remedial action taken.

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

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

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

Obligations relating to personal data breaches

68 Communication of a personal data breach to the data subject

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

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

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

(b) the name and contact details of the data protection officer or other contact point from whom more information can be obtained;

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

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

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

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

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

(c) it would involve a disproportionate effort.

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

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

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

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

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

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

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

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

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

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

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

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.

(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.

(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.

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

(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).

(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.

(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 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.

CHAPTER 6

SUPPLEMENTARY

79 National security: certificates by the Minister

(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.

(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.

(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.

PART 4

INTELLIGENCE SERVICES PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

Scope

82 Processing to which this Part applies

(1) This Part applies to—

(a) the processing by an intelligence service of personal data wholly or partly by automated means, and

(b) the processing by an intelligence service 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) In this Part, "intelligence service" means—

(a) the Security Service;

(b) the Secret Intelligence Service;

(c) the Government Communications Headquarters.

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

Definitions

83 Meaning of "controller" and "processor"

(1) In this Part, "controller" means the intelligence service 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 intelligence service 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).

84 Other definitions

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

(2) "Consent", in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data.

(3) "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.

(4) "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.

(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 person 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) Sections 3 and ~~198~~ 196 include definitions of other expressions used in this Part.

CHAPTER 2

PRINCIPLES

Overview

85 Overview

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

(a) section 86 sets out the first data protection principle (requirement that processing be lawful, fair and transparent);

(b) section 87 sets out the second data protection principle (requirement that the purposes of processing be specified, explicit and legitimate);

(c) section 88 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);
(d) section 89 sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);
(e) section 90 sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);
(f) section 91 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) Each of sections 86, 87 and 91 makes provision to supplement the principle to which it relates.

The data protection principles

86 The first data protection principle

(1) The first data protection principle is that the processing of personal data must be—
(a) lawful, and
(b) fair and transparent.

(2) The processing of personal data is lawful only if and to the extent that—
(a) at least one of the conditions in Schedule 9 is met, and
(b) in the case of sensitive processing, at least one of the conditions in Schedule 10 is also met.

(3) The Secretary of State may by regulations amend Schedule 10—
(a) by adding conditions;
(b) by omitting conditions added by regulations under paragraph (a).

(4) Regulations under subsection (3) are subject to the affirmative resolution procedure.

(5) In determining whether the processing of personal data is fair and transparent, regard is to be had to the method by which it is obtained.

(6) For the purposes of subsection (5), data is to be treated as obtained fairly and transparently if it consists of information obtained from a person who—
(a) is authorised by an enactment to supply it, or
(b) is required to supply it by an enactment or by an international obligation of the United Kingdom.

(7) 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 for the purpose of uniquely identifying an individual;
(c) the processing of biometric data for the purpose of uniquely identifying an individual;
(d) the processing of data concerning health;
(e) the processing of data concerning an individual's sex life or sexual orientation;
(f) the processing of personal data as to—

(i) the commission or alleged commission of an offence by an individual, or

(ii) proceedings for an offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings.

87 The second data protection principle

(1) The second data protection principle is that—

(a) the 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 is collected.

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

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

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

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

(4) Processing of personal data is to be regarded as compatible with the purpose for which it is collected if the processing—

(a) consists of—

(i) processing for archiving purposes in the public interest,

(ii) processing for the purposes of scientific or historical research, or

(iii) processing for statistical purposes, and

(b) is subject to appropriate safeguards for the rights and freedoms of the data subject.

88 The third data protection principle

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

89 The fourth data protection principle

The fourth data protection principle is that personal data undergoing processing must be accurate and, where necessary, kept up to date.

90 The fifth data protection principle

The fifth data protection principle is that personal data must be kept for no longer than is necessary for the purpose for which it is processed.

91 The sixth data protection principle

(1) The sixth data protection principle is that personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

(2) The risks referred to in subsection (1) include (but are not limited to) accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of, personal data.

CHAPTER 3

RIGHTS OF THE DATA SUBJECT

Overview

92 Overview

(1) This Chapter sets out the rights of the data subject as follows—

(a) section 93 deals with the information to be made available to the data subject;

(b) sections 94 and 95 deal with the right of access by the data subject;

(c) sections 96 and 97 deal with rights in relation to automated processing;

(d) section 98 deals with the right to information about decision-making;

(e) section 99 deals with the right to object to processing;

(f) section 100 deals with rights to rectification and erasure of personal data.

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

Rights

93 Right to information

(1) The controller must give a data subject the following information—

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

(b) the legal basis on which, and the purposes for which, the controller processes personal data;

(c) the categories of personal data relating to the data subject that are being processed;

(d) the recipients or the categories of recipients of the personal data (if applicable);

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

(f) how to exercise rights under this Chapter;

(g) any other information needed to secure that the personal data is processed fairly and transparently.

(2) The controller may comply with subsection (1) by making information generally available, where the controller considers it appropriate to do so.

(3) The controller is not required under subsection (1) to give a data subject information that the data subject already has.

(4) Where personal data relating to a data subject is collected by or on behalf of the controller from a person other than the data subject, the requirement in

subsection (1) has effect, in relation to the personal data so collected, with the following exceptions—

(a) the requirement does not apply in relation to processing that is authorised by an enactment;

(b) the requirement does not apply in relation to the data subject if giving the information to the data subject would be impossible or involve disproportionate effort.

94 Right of access

(1) An individual is entitled to obtain from a controller—

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

(b) where that is the case—

(i) communication, in intelligible form, of the personal data of which that individual is the data subject, and

(ii) 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;

(d) the period for which the personal data is to be preserved;

(e) the existence of a data subject's rights to rectification and erasure of personal data (see section 100);

(f) the right to lodge a complaint with the Commissioner and the contact details of the Commissioner;

(g) any information about the origin of the personal data concerned.

(3) A controller is not obliged to provide information under this section unless the controller has received such reasonable fee as the controller may require, subject to subsection (4).

(4) The Secretary of State may by regulations—

(a) specify cases in which a controller may not charge a fee;

(b) specify the maximum amount of a fee.

(5) Where a controller—

(a) reasonably requires further information—

(i) in order that the controller be satisfied as to the identity of the individual making a request under subsection (1), or

(ii) to locate the information which that individual seeks, and

(b) has informed that individual of that requirement,

the controller is not obliged to comply with the request unless the controller is supplied with that further information.

(6) Where a controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, the controller is not obliged to comply with the request unless—

(a) the other individual has consented to the disclosure of the information to the individual making the request, or

(b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

(7) In subsection (6), the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request.

(8) Subsection (6) is not to be construed as excusing a controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.

(9) In determining for the purposes of subsection (6)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard must be had, in particular, to—

(a) any duty of confidentiality owed to the other individual,

(b) any steps taken by the controller with a view to seeking the consent of the other individual,

(c) whether the other individual is capable of giving consent, and

(d) any express refusal of consent by the other individual.

(10) Subject to subsection (6), a controller must comply with a request under subsection (1)—

(a) promptly, and

(b) in any event before the end of the applicable time period.

(11) If a court is satisfied on the application of an individual who has made a request under subsection (1) that the controller in question has failed to comply with the request in contravention of this section, the court may order the controller to comply with the request.

(12) A court may make an order under subsection (11) in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for compliance with the obligation to which the order relates.

(13) The jurisdiction conferred on a court by this section is exercisable by the High Court or, in Scotland, by the Court of Session.

(14) In this section—

"the applicable time period" ~~means the period of~~means—

(a) ~~one month, or~~

(b) the period of 1 month, or

(c) such longer period, not exceeding ~~three~~ 3 months, as may be specified in regulations made by the Secretary of State,

beginning with the relevant ~~day~~time;

"the relevant ~~day~~time", in relation to a request under subsection (1), means the latest of the ~~following days~~following—

(a) ~~the day on which~~ when the controller receives the request,

(b) ~~the day on which~~ when the fee (if any) is paid, and

(c) ~~the day on which~~ when the controller receives the information (if any) required under subsection (5) in connection with the request.

(15) Regulations under this section are subject to the negative resolution procedure.

95 Right of access: supplementary

(1) The controller must comply with the obligation imposed by section 94(1)(b)(i) by supplying the data subject with a copy of the information in writing unless—

(a) the supply of such a copy is not possible or would involve disproportionate effort, or

(b) the data subject agrees otherwise;

and where any of the information referred to in section 94(1)(b)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

(2) Where a controller has previously complied with a request made under section 94 by an individual, the controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(3) In determining for the purposes of subsection (2) whether requests under section 94 are made at reasonable intervals, regard must be had to—

(a) the nature of the data,

(b) the purpose for which the data is processed, and

(c) the frequency with which the data is altered.

(4) The information to be supplied pursuant to a request under section 94 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

(5) For the purposes of section 94(6) to (8), an individual can be identified from information to be disclosed to a data subject by a controller if the individual can be identified from—

(a) that information, or

(b) that and any other information that the controller reasonably believes the data subject making the request is likely to possess or obtain.

96 Right not to be subject to automated decision-making

(1) The controller may not take a decision significantly affecting a data subject that is based solely on automated processing of personal data relating to the data subject.

(2) Subsection (1) does not prevent such a decision being made on that basis if—

(a) the decision is required or authorised by law,

(b) the data subject has given consent to the decision being made on that basis, or

(c) the decision is a decision taken in the course of steps taken—

(i) for the purpose of considering whether to enter into a contract with the data subject,

(ii) with a view to entering into such a contract, or

(iii) in the course of performing such a contract.

(3) For the purposes of this section, a decision that has legal effects as regards an individual is to be regarded as significantly affecting the individual.

97 Right to intervene in automated decision-making

(1) This section applies where—

(a) the controller takes a decision significantly affecting a data subject that is based solely on automated processing of personal data relating to the data subject, and

(b) the decision is required or authorised by law.

(2) This section does not apply to such a decision if—

(a) the data subject has given consent to the decision being made on that basis, or

(b) the decision is a decision taken in the course of steps taken—

(i) for the purpose of considering whether to enter into a contract with the data subject,

(ii) with a view to entering into such a contract, or

(iii) in the course of performing such a contract.

(3) The controller must as soon as reasonably practicable notify the data subject that such a decision has been made.

(4) The data subject may, before the end of the period of ~~21 days~~ 1 month beginning with receipt of the notification, request the controller—

(a) to reconsider the decision, or

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

(5) If a request is made to the controller under subsection (4), the controller must, before the end of the period of ~~21 days~~ 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, and

(b) by notice in writing inform the data subject of the outcome of that consideration.

(6) For the purposes of this section, a decision that has legal effects as regards an individual is to be regarded as significantly affecting the individual.

98 Right to information about decision-making

(1) Where—

(a) the controller processes personal data relating to a data subject, and

(b) results produced by the processing are applied to the data subject,

the data subject is entitled to obtain from the controller, on request, knowledge of the reasoning underlying the processing.

(2) Where the data subject makes a request under subsection (1), the controller must comply with the request without undue delay.

99 Right to object to processing

(1) A data subject is entitled at any time, by notice given to the controller, to require the controller—

(a) not to process personal data relating to the data subject, or

(b) not to process such data for a specified purpose or in a specified manner,

on the ground that, for specified reasons relating to the situation of the data subject, the processing in question is an unwarranted interference with the interests or rights of the data subject.

(2) Where the controller—

(a) reasonably requires further information—

(i) in order that the controller be satisfied as to the identity of the individual giving notice under subsection (1), or

(ii) to locate the data to which the notice relates, and

(b) has informed that individual of that requirement,

the controller is not obliged to comply with the notice unless the controller is supplied with that further information.

(3) The controller must, before the end of 21 days beginning with the relevant ~~day~~time, give a notice to the data subject—

(a) stating that the controller has complied or intends to comply with the notice under subsection (1), or

(b) stating the controller's reasons for not complying with the notice to any extent and the extent (if any) to which the controller has complied or intends to comply with the notice under subsection (1).

(4) If the controller does not comply with a notice under subsection (1) to any extent, the data subject may apply to a court for an order that the controller take steps for complying with the notice.

(5) If the court is satisfied that the controller should comply with the notice (or should comply to any extent), the court may order the controller to take such steps for complying with the notice (or for complying with it to that extent) as the court thinks fit.

(6) A court may make an order under subsection (5) in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for compliance with the obligation to which the order relates.

(7) The jurisdiction conferred on a court by this section is exercisable by the High Court or, in Scotland, by the Court of Session.

(8) In this section, "the relevant ~~day~~time", in relation to a notice under subsection (1), means—

(a) ~~the day on which~~ when the controller receives the notice, or

(b) if later, ~~the day on which~~ when the controller receives the information (if any) required under subsection (2) in connection with the notice.

100 Rights to rectification and erasure

(1) If a court is satisfied on the application of a data subject that personal data relating to the data subject is inaccurate, the court may order the controller to rectify that data without undue delay.

(2) If a court is satisfied on the application of a data subject that the processing of personal data relating to the data subject would infringe any of sections 86 to 91, the court may order the controller to erase that data without undue delay.

(3) If personal data relating to the data subject must be maintained for the purposes of evidence, the court may (instead of ordering the controller to rectify or erase the personal data) order the controller to restrict its processing without undue delay.

(4) If—

(a) the data subject contests the accuracy of personal data, and

(b) the court is satisfied that the controller is not able to ascertain whether the data is accurate or not,

the court may (instead of ordering the controller to rectify or erase the personal data) order the controller to restrict its processing without undue delay.

(5) A court may make an order under this section in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for carrying out the rectification, erasure or restriction of processing that the court proposes to order.

(6) The jurisdiction conferred on a court by this section is exercisable by the High Court or, in Scotland, by the Court of Session.

CHAPTER 4

CONTROLLER AND PROCESSOR

Overview

101 Overview

This Chapter sets out—

(a) the general obligations of controllers and processors (see sections 102 to 106);

(b) specific obligations of controllers and processors with respect to security (see section 107);

(c) specific obligations of controllers and processors with respect to personal data breaches (see section 108).

General obligations

102 General obligations of the controller

Each controller must implement appropriate measures—

(a) to ensure, and

(b) to be able to demonstrate, in particular to the Commissioner,

that the processing of personal data complies with the requirements of this Part.

103 Data protection by design

(1) Where a controller proposes that a particular type of processing of personal data be carried out by or on behalf of the controller, the controller must, prior to the processing, consider the impact of the proposed processing on the rights and freedoms of data subjects.

(2) A controller must implement appropriate technical and organisational measures which are designed to ensure that—

(a) the data protection principles are implemented, and

(b) risks to the rights and freedoms of data subjects are minimised.

104 Joint controllers

(1) Where two or more intelligence services 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.

105 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 undertakes—

(a) to implement appropriate measures that are sufficient to secure that the processing complies with this Part;

(b) to provide to the controller such information as is necessary for demonstrating that the processing complies with this Part.

(3) 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.

106 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.

Obligations relating to security

107 Security of processing

(1) Each controller and each processor must implement security measures 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

108 Communication of a personal data breach

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

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

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

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

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

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

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

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

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

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

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

CHAPTER 5

TRANSFERS OF PERSONAL DATA OUTSIDE THE UNITED KINGDOM

109 Transfers of personal data outside the United Kingdom

(1) A controller may not transfer personal data to—

(a) a country or territory outside the United Kingdom, or

(b) an international organisation,

unless the transfer falls within subsection (2).

(2) A transfer of personal data falls within this subsection if the transfer is a necessary and proportionate measure carried out—

(a) for the purposes of the controller's statutory functions, or

(b) for other purposes provided for, in relation to the controller, in section 2(2)(a) of the Security Service Act 1989 or section 2(2)(a) or 4(2)(a) of the Intelligence Services Act 1994.

CHAPTER 6

EXEMPTIONS

110 National security

(1) A provision mentioned in subsection (2) does not apply to personal data to which this Part applies if exemption from the provision is required for the purpose of safeguarding national security.

(2) The provisions are—

(a) Chapter 2 (the data protection principles), except section 86(1)(a) and (2) and Schedules 9 and 10;

(b) Chapter 3 (rights of data subjects);

(c) in Chapter 4, section 108 (communication of a personal data breach to the Commissioner);

(d) in Part 5—

(i) section 119 (inspection in accordance with international obligations);

(ii) in Schedule 13 (other general functions of the Commissioner), paragraphs ~~1(a)~~1(a) and ~~(g)~~(g) and ~~2~~2;

(e) in Part 6—

(i) sections ~~143~~ 141 to ~~153~~ 151 and Schedule 15 (Commissioner's notices and powers of entry and inspection);

(ii) sections ~~170~~ 166 to ~~173~~ 169 (offences relating to personal data);

(iii) sections ~~174~~ 170 to ~~176~~ 172 (provision relating to the special purposes).

111 National security: certificate

(1) Subject to subsection (3), a certificate signed by a Minister of the Crown certifying that exemption from all or any of the provisions mentioned in section 110(2) is, or at any time was, required for the purpose of safeguarding national security in respect of any personal data is conclusive evidence of that fact.

(2) A certificate under subsection (1)—

(a) may identify the personal data to which it applies by means of a general description, and

(b) may be expressed to have prospective effect.

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

(4) If on an appeal under subsection (3), 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.

(5) Where, in any proceedings under or by virtue of this Act, it is claimed by a controller that a certificate under subsection (1) which identifies the personal data to which it applies by means of a general description applies to any personal data, another party to the proceedings may appeal to the Tribunal on the ground that the certificate does not apply to the personal data in question.

(6) But, subject to any determination under subsection (7), the certificate is to be conclusively presumed so to apply.

(7) On an appeal under subsection (5), the Tribunal may determine that the certificate does not so apply.

(8) 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.

(9) 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.

(10) 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.

112 Other exemptions

Schedule 11 provides for further exemptions.

113 Power to make further exemptions

(1) The Secretary of State may by regulations amend Schedule 11—

(a) by adding exemptions from any provision of this Part;

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

(2) Regulations under this section are subject to the affirmative resolution procedure.

PART 5

THE INFORMATION COMMISSIONER

The Commissioner

114 The Information Commissioner

(1) There is to continue to be an Information Commissioner.

(2) Schedule 12 makes provision about the Commissioner.

General functions

115 General functions under the GDPR and safeguards

(1) The Commissioner is to be the supervisory authority in the United Kingdom for the purposes of Article 51 of the GDPR.

(2) General functions are conferred on the Commissioner by—

(a) Article 57 of the GDPR (tasks), and

(b) Article 58 of the GDPR (powers),

(and see also the Commissioner's duty under section 2).

(3) The Commissioner's functions in relation to the processing of personal data to which the GDPR applies include—

(a) a duty to advise Parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, and

(b) a power to issue, on the Commissioner's own initiative or on request, opinions to Parliament, the government or other institutions and bodies as well as to the public on any issue related to the protection of personal data.

(4) The Commissioner's functions under Article 58 of the GDPR are subject to the safeguards in subsections (5) to (9).

(5) The Commissioner's power under Article 58(1)(a) of the GDPR (power to require a controller or processor to provide information that the Commissioner requires for the performance of the Commissioner's tasks under the GDPR) is exercisable only by giving an information notice under section ~~143~~141.

(6) The Commissioner's power under Article 58(1)(b) of the GDPR (power to carry out data protection audits) is exercisable only in accordance with section ~~146~~144.

(7) The Commissioner's powers under Article 58(1)(e) and (f) of the GDPR (power to obtain information from controllers and processors and access to their premises) are exercisable only—

(a) in accordance with Schedule 15 (see section ~~153~~151), or

(b) to the extent that they are exercised in conjunction with the power under Article 58(1)(b) of the GDPR, in accordance with section ~~146~~144.

(8) The following powers are exercisable only by giving an enforcement notice under section ~~148~~146—

(a) the Commissioner's powers under Article 58(2)(c) to (g) and (j) of the GDPR (certain corrective powers);

(b) the Commissioner's powers under Article 58(2)(h) to order a certification body to withdraw, or not to issue, a certification under Articles 42 and 43 of the GDPR.

(9) The Commissioner's powers under Articles 58(2)(i) and 83 of the GDPR (administrative fines) are exercisable only by giving a penalty notice under section ~~154~~152.

(10) This section is without prejudice to other functions conferred on the Commissioner, whether by the GDPR, this Act or otherwise.

116 Other general functions

(1) The Commissioner—

(a) is to be the supervisory authority in the United Kingdom for the purposes of Article 41 of the Law Enforcement Directive, and

(b) is to continue to be the designated authority in the United Kingdom for the purposes of Article 13 of the Data Protection Convention.

(2) Schedule 13 confers general functions on the Commissioner in connection with processing to which the GDPR does not apply (and see also the Commissioner's duty under section 2).

(3) This section and Schedule 13 are without prejudice to other functions conferred on the Commissioner, whether by this Act or otherwise.

117 Competence in relation to courts etc

Nothing in this Act permits or requires the Commissioner to exercise functions in relation to the processing of personal data by—

(a) an individual acting in a judicial capacity, or

(b) a court or tribunal acting in its judicial capacity,

(and see also Article 55(3) of the GDPR).

International role

118 Co-operation and mutual assistance

(1) Articles 60 to 62 of the GDPR confer functions on the Commissioner in relation to co-operation and mutual assistance between, and joint operations of, supervisory authorities under the GDPR.

(2) References to the GDPR in subsection (1) do not include the applied GDPR.

(3) Article 61 of the applied GDPR confers functions on the Commissioner in relation to co-operation with other supervisory authorities (as defined in Article 4(21) of the applied GDPR).

(4) Part ~~1~~1 of Schedule 14 makes provision as to the functions to be carried out by the Commissioner for the purposes of Article 50 of the Law Enforcement Directive (mutual assistance).

(5) Part ~~2~~2 of Schedule 14 makes provision as to the functions to be carried out by the Commissioner for the purposes of Article 13 of the Data Protection Convention (co-operation between parties).

119 Inspection of personal data in accordance with international obligations

(1) The Commissioner may inspect personal data where the inspection is necessary in order to discharge an international obligation of the United Kingdom, subject to the restriction in subsection (2).

(2) The power under subsection (1) is exercisable only if the personal data—
(a) is processed wholly or partly by automated means, or
(b) is processed otherwise than by automated means and forms part of a filing system or is intended to form part of a filing system.

(3) The power under subsection (1) includes power to inspect, operate and test equipment which is used for the processing of personal data.

(4) Before exercising the power under subsection (1), the Commissioner must by written notice inform the controller and any processor that the Commissioner intends to do so.

(5) Subsection (4) does not apply if the Commissioner considers that the case is urgent.

(6) It is an offence—
(a) intentionally to obstruct a person exercising the power under subsection (1), or
(b) to fail without reasonable excuse to give a person exercising that power any assistance the person may reasonably require.

120 Further international role

(1) The Commissioner must, in relation to third countries and international organisations, take appropriate steps to—
(a) develop international co-operation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;
(d) promote the exchange and documentation of legislation and practice for the protection of personal data, including legislation and practice relating to jurisdictional conflicts with third countries.

(2) Subsection (1) applies only in connection with the processing of personal data to which the GDPR does not apply; for the equivalent duty in connection with the processing of personal data to which the GDPR applies, see Article 50 of the GDPR (international co-operation for the protection of personal data).

(3) The Commissioner must carry out data protection functions which the Secretary of State directs the Commissioner to carry out for the purpose of

enabling Her Majesty's Government in the United Kingdom to give effect to an international obligation of the United Kingdom.

(4) The Commissioner may provide an authority carrying out data protection functions under the law of a British overseas territory with assistance in carrying out those functions.

(5) The Secretary of State may direct that assistance under subsection (4) is to be provided on terms, including terms as to payment, specified or approved by the Secretary of State.

(6) In this section—

"data protection functions" means functions relating to the protection of individuals with respect to the processing of personal data;

"mutual assistance in the enforcement of legislation for the protection of personal data" includes assistance in the form of notification, complaint referral, investigative assistance and information exchange;

"third country" means a country or territory that is not a member State.

Codes of practice

121 ~~Code on personal data of national significance~~

~~The Commissioner must prepare a code of practice which contains—~~

~~(a) best practice guidance in relation to information sharing agreements between publicly funded data controllers and third parties;~~

~~(b) guidance in relation to the calculation of value for money where publicly funded data controllers enter into information sharing agreements with third parties;~~

~~(c) guidance about securing financial benefits from the sharing of such personal data with third parties for the purposes of processing or developing associated software; and~~

~~(d) such other guidance as the Commissioner considers appropriate to promote best practice in the sharing and processing of personal data of national significance.~~

122 Data-sharing code

(1) The Commissioner must prepare a code of practice which contains—

(a) practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation, and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data.

(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.

(3) Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and such of the following as the Commissioner considers appropriate—

(a) trade associations;

(b) data subjects;

(c) persons who appear to the Commissioner to represent the interests of data subjects.

(4) A code under this section may include transitional provision or savings.

(5) In this section—

"good practice in the sharing of personal data" means such practice in the sharing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements of the data protection legislation;

"the sharing of personal data" means the disclosure of personal data by transmission, dissemination or otherwise making it available;

"trade association" includes a body representing controllers or processors.

123 Direct marketing code

(1) The Commissioner must prepare a code of practice which contains—

(a) practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426), and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in direct marketing.

(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.

(3) Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and such of the following as the Commissioner considers appropriate—

(a) trade associations;

(b) data subjects;

(c) persons who appear to the Commissioner to represent the interests of data subjects.

(4) A code under this section may include transitional provision or savings.

(5) In this section—

"direct marketing" means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals;

"good practice in direct marketing" means such practice in direct marketing as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements mentioned in subsection (1)(a);

"trade association" includes a body representing controllers or processors.

124 Age-appropriate design code

(1) The Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children.

(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.

(3) Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and such other persons as the Commissioner considers appropriate, including—

(a) children,

(b) parents,

(c) persons who appear to the Commissioner to represent the interests of children,

(d) child development experts, and

(e) trade associations.

(4) In preparing a code or amendments under this section, the Commissioner must have regard—

(a) to the fact that children have different needs at different ages, and

(b) to the United Kingdom's obligations under the United Nations Convention on the Rights of the Child.

(5) A code under this section may include transitional provision or savings.

(6) Any transitional provision included in the first code under this section must cease to have effect before the end of the period of 12 months beginning ~~with the day on which~~ when the code comes into force.

(7) In this section—

"age-appropriate design" means the design of services so that they are appropriate for use by, and meet the development needs of, children;

"information society services" has the same meaning as in the GDPR, but does not include preventive or counselling services;

"relevant information society services" means information society services which involve the processing of personal data to which the GDPR applies;

"standards of age-appropriate design of relevant information society services" means such standards of age-appropriate design of such services as appear to the Commissioner to be desirable having regard to the best interests of children;

"trade association" includes a body representing controllers or processors;

"the United Nations Convention on the Rights of the Child" means the Convention on the Rights of the Child adopted by the General Assembly of the United Nations on 20 November 1989 (including any Protocols to that Convention which are in force in relation to the United Kingdom), subject to any reservations, objections or interpretative declarations by the United Kingdom for the time being in force.

125 Approval of data-sharing, direct marketing and age-appropriate design codes

(1) When a code is prepared under section ~~122~~121, ~~123~~ 122 or ~~124~~123—

(a) the Commissioner must submit the final version to the Secretary of State, and

(b) the Secretary of State must lay the code before Parliament.

(2) In relation to the first code under section ~~124~~123—

(a) the Commissioner must prepare the code as soon as reasonably practicable and must submit it to the Secretary of State before the end of the period of 18 months beginning ~~with the day on which~~ when this Act is passed, and

(b) the Secretary of State must lay it before Parliament as soon as reasonably practicable.

(3) If, within the 40-day period, either House of Parliament resolves not to approve a code prepared under section ~~122~~121, ~~123~~ 122 or ~~124~~123, the Commissioner must not issue the code.

(4) If no such resolution is made within that period—

(a) the Commissioner must issue the code, and

(b) the code comes into force at the end of the period of 21 days beginning with the day on which it is issued.

(5) If, as a result of subsection (3), there is no code in force under section ~~122~~121, ~~123~~ 122 or ~~124~~123, the Commissioner must prepare another version of the code.

(6) Nothing in subsection (3) prevents another version of the code being laid before Parliament.

(7) In this section, "the 40-day period" means—

(a) if the code is laid before both Houses of Parliament on the same day, the period of 40 days beginning with that day, or

(b) if the code is laid before the Houses of Parliament on different days, the period of 40 days beginning with the later of those days.

(8) In calculating the 40-day period, no account is to be taken of any period during which Parliament is dissolved or prorogued or during which both Houses of Parliament are adjourned for more than 4 days.

(9) This section, other than subsections (2) and (5), applies in relation to amendments prepared under sections ~~122~~121, ~~123~~ 122 and ~~124~~ 123 as it applies in relation to codes prepared under those sections.

126 Publication and review of data-sharing, direct marketing and age-appropriate design codes

(1) The Commissioner must publish a code issued under section ~~125~~124(4).

(2) Where an amendment of a code is issued under section ~~125~~124(4), the Commissioner must publish—

(a) the amendment, or

(b) the code as amended by it.

(3) The Commissioner must keep under review each code issued under section ~~125~~124(4) for the time being in force.

(4) Where the Commissioner becomes aware that the terms of such a code could result in a breach of an international obligation of the United Kingdom, the Commissioner must exercise the power under section ~~122~~121(2), ~~123~~122(2) or ~~124~~123(2) with a view to remedying the situation.

127 Effect of data-sharing, direct marketing and age-appropriate design codes

(1) A failure by a person to act in accordance with a provision of a code issued under section ~~125~~124(4) does not of itself make that person liable to legal proceedings in a court or tribunal.

(2) A code issued under section ~~125~~124(4), including an amendment or replacement code, is admissible in evidence in legal proceedings.

(3) In any proceedings before a court or tribunal, the court or tribunal must take into account a provision of a code issued under section ~~125~~124(4) in determining a question arising in the proceedings if—

(a) the question relates to a time when the provision was in force, and

(b) the provision appears to the court or tribunal to be relevant to the question.

(4) Where the Commissioner is carrying out a function described in subsection (5), the Commissioner must take into account a provision of a code issued under section ~~125~~124(4) in determining a question arising in connection with the carrying out of the function if—

(a) the question relates to a time when the provision was in force, and

(b) the provision appears to the Commissioner to be relevant to the question.

(5) Those functions are functions under—

(a) the data protection legislation, or

(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426).

128 Other codes of practice

(1) The Secretary of State may by regulations require the Commissioner—

(a) to prepare appropriate codes of practice giving guidance as to good practice in the processing of personal data, and

(b) to make them available to such persons as the Commissioner considers appropriate.

(2) Before preparing such codes, the Commissioner must consult such of the following as the Commissioner considers appropriate—

(a) trade associations;

(b) data subjects;

(c) persons who appear to the Commissioner to represent the interests of data subjects.

(3) Regulations under this section—

(a) must describe the personal data or processing to which the code of practice is to relate, and

(b) may describe the persons or classes of person to whom it is to relate.

(4) Regulations under this section are subject to the negative resolution procedure.

(5) In this section—

"good practice in the processing of personal data" means such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others,

including compliance with the requirements of the data protection legislation;

"trade association" includes a body representing controllers or processors.

Consensual audits

129 Consensual audits

(1) The Commissioner's functions under Article 58(1) of the GDPR and paragraph ~~1~~1 of Schedule 13 include power, with the consent of a controller or processor, to carry out an assessment of whether the controller or processor is complying with good practice in the processing of personal data.

(2) The Commissioner must inform the controller or processor of the results of such an assessment.

(3) In this section, "good practice in the processing of personal data" has the same meaning as in section ~~128~~127.

Records of national security certificates

130 Records of national security certificates

(1) A Minister of the Crown who issues a certificate under section 27, 79 or 111 must send a copy of the certificate to the Commissioner.

(2) If the Commissioner receives a copy of a certificate under subsection (1), the Commissioner must publish a record of the certificate.

(3) The record must contain—
(a) the name of the Minister who issued the certificate,
(b) the date on which the certificate was issued, and
(c) subject to subsection (4), the text of the certificate.

(4) The Commissioner must not publish the text, or a part of the text, of the certificate if—
(a) the Minister determines that publishing the text or that part of the text—
(i) would be against the interests of national security,
(ii) would be contrary to the public interest, or
(iii) might jeopardise the safety of any person, and
(b) the Minister has notified the Commissioner of that determination.

(5) The Commissioner must keep the record of the certificate available to the public while the certificate is in force.

(6) If a Minister of the Crown revokes a certificate issued under section 27, 79 or 111, the Minister must notify the Commissioner.

Information provided to the Commissioner

131 Disclosure of information to the Commissioner

(1) No enactment or rule of law prohibiting or restricting the disclosure of information precludes a person from providing the Commissioner with information necessary for the discharge of the Commissioner's functions.

(2) But this section does not authorise the making of a disclosure which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

(3) 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 (2) has effect as if it included a reference to that Part.

132 Confidentiality of information

(1) A person who is or has been the Commissioner, or a member of the Commissioner's staff or an agent of the Commissioner, must not disclose information which—

(a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the Commissioner's functions,

(b) relates to an identified or identifiable individual or business, and

(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources,

unless the disclosure is made with lawful authority.

(2) For the purposes of subsection (1), a disclosure is made with lawful authority only if and to the extent that—

(a) the disclosure was made with the consent of the individual or of the person for the time being carrying on the business,

(b) the information was obtained or provided as described in subsection (1)(a) for the purpose of its being made available to the public (in whatever manner),

(c) the disclosure was made for the purposes of, and is necessary for, the discharge of one or more of the Commissioner's functions,

(d) the disclosure was made for the purposes of, and is necessary for, the discharge of an EU obligation,

(e) the disclosure was made for the purposes of criminal or civil proceedings, however arising, or

(f) having regard to the rights, freedoms and legitimate interests of any person, the disclosure was necessary in the public interest.

(3) It is an offence for a person knowingly or recklessly to disclose information in contravention of subsection (1).

133 Guidance about privileged communications

(1) The Commissioner must produce and publish guidance about—

(a) how the Commissioner proposes to secure that privileged communications which the Commissioner obtains or has access to in

the course of carrying out the Commissioner's functions are used or disclosed only so far as necessary for carrying out those functions, and

(b) how the Commissioner proposes to comply with restrictions and prohibitions on obtaining or having access to privileged communications which are imposed by an enactment.

(2) The Commissioner—

(a) may alter or replace the guidance, and

(b) must publish any altered or replacement guidance.

(3) The Commissioner must consult the Secretary of State before publishing guidance under this section (including altered or replacement guidance).

(4) The Commissioner must arrange for guidance under this section (including altered or replacement guidance) to be laid before Parliament.

(5) In this section, "privileged communications" means—

(a) communications made—

(i) between a professional legal adviser and the adviser's client, and

(ii) in connection with the giving of legal advice to the client with respect to legal obligations, liabilities or rights, and

(b) communications made—

(i) between a professional legal adviser and the adviser's client or between such an adviser or client and another person,

(ii) in connection with or in contemplation of legal proceedings, and

(iii) for the purposes of such proceedings.

(6) In subsection (5)—

(a) references to the client of a professional legal adviser include references to a person acting on behalf of the client, and

(b) references to a communication include—

(i) a copy or other record of the communication, and

(ii) anything enclosed with or referred to in the communication if made as described in subsection (5)(a)(ii) or in subsection (5)(b)(ii) and (iii).

Fees

134 Fees for services

The Commissioner may require a person other than a data subject or a data protection officer to pay a reasonable fee for a service provided to the person, or at the person's request, which the Commissioner is required or authorised to provide under the data protection legislation.

135 Manifestly unfounded or excessive requests by data subjects etc

(1) Where a request to the Commissioner from a data subject or a data protection officer is manifestly unfounded or excessive, the Commissioner 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 described in subsection (1) is manifestly unfounded or excessive, it is for the Commissioner to show that it is.

(4) Subsections (1) and (3) apply only in cases in which the Commissioner does not already have such powers and obligations under Article 57(4) of the GDPR.

136 Guidance about fees

(1) The Commissioner must produce and publish guidance about the fees the Commissioner proposes to charge in accordance with—

(a) section ~~134~~ 133 or ~~135~~134, or

(b) Article 57(4) of the GDPR.

(2) Before publishing the guidance, the Commissioner must consult the Secretary of State.

Charges

137 Charges payable to the Commissioner by controllers

(1) The Secretary of State may by regulations require controllers to pay charges of an amount specified in the regulations to the Commissioner.

(2) Regulations under subsection (1) may require a controller to pay a charge regardless of whether the Commissioner has provided, or proposes to provide, a service to the controller.

(3) Regulations under subsection (1) may—

(a) make provision about the time or times at which, or period or periods within which, a charge must be paid;

(b) make provision for cases in which a discounted charge is payable;

(c) make provision for cases in which no charge is payable;

(d) make provision for cases in which a charge which has been paid is to be refunded.

(4) In making regulations under subsection (1), the Secretary of State must have regard to the desirability of securing that the charges payable to the Commissioner under such regulations are sufficient to offset—

(a) expenses incurred by the Commissioner in discharging the Commissioner's functions—

(i) under the data protection legislation,

(ii) under the Data Protection Act 1998,

(iii) under or by virtue of sections 108 and 109 of the Digital Economy Act 2017, and

(iv) under or by virtue of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426),

(b) any expenses of the Secretary of State in respect of the Commissioner so far as attributable to those functions,

(c) to the extent that the Secretary of State considers appropriate, any deficit previously incurred (whether before or after the passing of this Act) in respect of the expenses mentioned in paragraph (a), and

(d) to the extent that the Secretary of State considers appropriate, expenses incurred by the Secretary of State in respect of the inclusion of any officers or staff of the Commissioner in any scheme under section 1 of the Superannuation Act 1972 or section 1 of the Public Service Pensions Act 2013.

(5) The Secretary of State may from time to time require the Commissioner to provide information about the expenses referred to in subsection (4)(a).

(6) The Secretary of State may by regulations make provision—

(a) requiring a controller to provide information to the Commissioner, or

(b) enabling the Commissioner to require a controller to provide information to the Commissioner,

for either or both of the purposes mentioned in subsection (7).

(7) Those purposes are—

(a) determining whether a charge is payable by the controller under regulations under subsection (1);

(b) determining the amount of a charge payable by the controller.

(8) The provision that may be made under subsection (6)(a) includes provision requiring a controller to notify the Commissioner of a change in the controller's circumstances of a kind specified in the regulations.

138 Regulations under section ~~137~~136: supplementary

(1) Before making regulations under section ~~137~~136(1) or (6), the Secretary of State must consult such representatives of persons likely to be affected by the regulations as the Secretary of State thinks appropriate (and see also section ~~179~~175).

(2) The Commissioner—

(a) must keep under review the working of regulations under section ~~137~~136(1) or (6), and

(b) may from time to time submit proposals to the Secretary of State for amendments to be made to the regulations.

(3) The Secretary of State must review the working of regulations under section ~~137~~136(1) or (6)—

(a) at the end of the period of 5 years beginning with the making of the first set of regulations under section 108 of the Digital Economy Act 2017, and

(b) at the end of each subsequent 5 year period.

(4) Regulations under section ~~137~~136(1) are subject to the negative resolution procedure if—

(a) they only make provision increasing a charge for which provision is made by previous regulations under section ~~137~~136(1) or section 108(1) of the Digital Economy Act 2017, and

(b) they do so to take account of an increase in the retail prices index since the previous regulations were made.

(5) Subject to subsection (4), regulations under section ~~137~~136(1) or (6) are subject to the affirmative resolution procedure.

(6) In subsection (4), "the retail prices index" means—

(a) the general index of retail prices (for all items) published by the Statistics Board, or

(b) where that index is not published for a month, any substitute index or figures published by the Board.

(7) Regulations under section ~~137~~136(1) or (6) may not apply to—

(a) Her Majesty in her private capacity,

(b) Her Majesty in right of the Duchy of Lancaster, or

(c) the Duke of Cornwall.

Reports etc

139 Reporting to Parliament

(1) The Commissioner must—

(a) produce a general report on the carrying out of the Commissioner's functions annually,

(b) arrange for it to be laid before Parliament, and

(c) publish it.

(2) The report must include the annual report required under Article 59 of the GDPR.

(3) The Commissioner may produce other reports relating to the carrying out of the Commissioner's functions and arrange for them to be laid before Parliament.

140 Publication by the Commissioner

A duty under this Act for the Commissioner to publish a document is a duty for the Commissioner to publish it, or to arrange for it to be published, in such form and manner as the Commissioner considers appropriate.

141 Notices from the Commissioner

(1) This section applies in relation to a notice authorised or required by this Act to be given to a person by the Commissioner.

(2) The notice may be given to an individual—

(a) by delivering it to the individual,

(b) by sending it to the individual by post addressed to the individual at his or her usual or last-known place of residence or business, or

(c) by leaving it for the individual at that place.

(3) The notice may be given to a body corporate or unincorporate—

(a) by sending it by post to the proper officer of the body at its principal office, or

(b) by addressing it to the proper officer of the body and leaving it at that office.

(4) The notice may be given to a partnership in Scotland—
(a) by sending it by post to the principal office of the partnership, or
(b) by addressing it to that partnership and leaving it at that office.

(5) The notice may be given to the person by other means, including by electronic means, with the person's consent.

(6) In this section—
"principal office", in relation to a registered company, means its registered office;
"proper officer", in relation to any body, means the secretary or other executive officer charged with the conduct of its general affairs;
"registered company" means a company registered under the enactments relating to companies for the time being in force in the United Kingdom.

(7) This section is without prejudice to any other lawful method of giving a notice.

PART 6

ENFORCEMENT

~~*Inquiry into issues arising from data protection breaches by news publishers*~~

142 ~~Inquiry into issues arising from data protection breaches committed by or on behalf of news publishers~~

(1) ~~The Secretary of State must, within the period of three months beginning on the day on which this Act is passed, establish an inquiry under the Inquiries Act 2005 into allegations of data protection breaches committed by, or on behalf of, news publishers.~~

(2) ~~The inquiry's terms of reference must include, but are not limited to—~~
(a) ~~to inquire, in respect of personal data processing, into the extent of unlawful or improper conduct within news publishers and, as appropriate, other organisations within the media, and by those responsible for holding personal data;~~
(b) ~~to inquire, in respect of personal data processing, into the extent of corporate governance and management failures at news publishers;~~
(c) ~~in the light of these inquiries, to consider the implications for personal data protection in relation to freedom of speech; and~~
(d) ~~to make recommendations on what action, if any, should be taken in the public interest.~~

Information notices

143 Information notices

(1) The Commissioner may, by written notice (an "information notice")—
(a) require a controller or processor to provide the Commissioner with information that the Commissioner reasonably requires for the purposes of carrying out the Commissioner's functions under the data protection legislation, or

(b) ~~The Commissioner may, by written notice (an "information notice"),~~ require ~~a controller or processor~~ any person to provide the Commissioner with information that the Commissioner reasonably requires for the purposes of determining whether the processing of ~~carrying~~ personal data is carried out by an individual in the ~~Commissioner's functions under the data protection legislation~~course of a purely personal or household activity.

(2) An information notice must state why the Commissioner requires the information.

(3) An information notice—

(a) may specify or describe particular information or a category of information;

(b) may specify the form in which the information must be provided;

(c) may specify the time at which, or the period within which, the information must be provided;

(d) may specify the place where the information must be provided;

(but see the restrictions in subsections (5) to (7)).

(4) An information notice must provide information about the rights of appeal under section ~~161~~159.

(5) An information notice may not require a person to provide information before the end of the period within which an appeal can be brought against the notice.

(6) If an appeal is brought against an information notice, the information need not be provided pending the determination or withdrawal of the appeal.

(7) If an information notice—

(a) states that, in the Commissioner's opinion, the information is required urgently, and

(b) gives the Commissioner's reasons for reaching that opinion,

subsections (5) and (6) do not apply but the notice must not require the information to be provided before the end of the period of 7 days beginning ~~with the day on which~~ when the notice is given.

(8) The Commissioner may cancel an information notice by written notice to the person to whom it was given.

(9) In subsection (1), in relation to a person who is a controller or processor for the purposes of the GDPR, the reference to a controller or processor includes a representative of a controller or processor designated under Article 27 of the GDPR (representatives of controllers or processors not established in the European Union).

(10) Section 3(14)(c) does not apply to the reference to the processing of personal data in subsection (1)(b).

144 Information notices: restrictions

(1) The Commissioner may not give an information notice with respect to the processing of personal data for the special purposes unless—

(a) a determination under section ~~174~~ 170 with respect to the data or the processing has taken effect, or

(b) the Commissioner—

(i) has reasonable grounds for suspecting that such a determination could be made, and

(ii) the information is required for the purposes of making such a determination.

(2) An information notice does not require a person to give the Commissioner information to the extent that requiring the person to do so would involve an infringement of the privileges of either House of Parliament.

(3) An information notice does not require a person to give the Commissioner information in respect of a communication which is made—

(a) between a professional legal adviser and the adviser's client, and

(b) in connection with the giving of legal advice to the client with respect to obligations, liabilities or rights under the data protection legislation.

(4) An information notice does not require a person to give the Commissioner information in respect of a communication which is made—

(a) between a professional legal adviser and the adviser's client or between such an adviser or client and another person,

(b) in connection with or in contemplation of proceedings under or arising out of the data protection legislation, and

(c) for the purposes of such proceedings.

(5) In subsections (3) and (4), references to the client of a professional legal adviser include references to a person acting on behalf of the client.

(6) An information notice does not require a person to provide the Commissioner with information if doing so would, by revealing evidence of the commission of an offence expose the person to proceedings for that offence.

(7) The reference to an offence in subsection (6) does not include an offence under—

(a) this Act;

(b) section 5 of the Perjury Act 1911 (false statements made otherwise than on oath);

(c) section 44(2) of the Criminal Law (Consolidation) (Scotland) Act 1995 (false statements made otherwise than on oath);

(d) Article 10 of the Perjury (Northern Ireland) Order 1979 (S.I. 1979/1714 (N.I. 19)) (false statutory declarations and other false unsworn statements).

(8) An oral or written statement provided by a person in response to an information notice may not be used in evidence against that person on a prosecution for an offence under this Act (other than an offence under section ~~145~~143) unless in the proceedings—

(a) in giving evidence the person provides information inconsistent with the statement, and

(b) evidence relating to the statement is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(9) In subsection (6), in relation to an information notice given to a representative of a controller or processor designated under Article 27 of the GDPR, the reference to the person providing the information being exposed to proceedings for an offence includes a reference to the controller or processor being exposed to such proceedings.

145 False statements made in response to an information notice

It is an offence for a person, in response to an information notice—

(a) to make a statement which the person knows to be false in a material respect, or

(b) recklessly to make a statement which is false in a material respect.

Assessment notices

146 Assessment notices

(1) The Commissioner may by written notice (an "assessment notice") require a controller or processor to permit the Commissioner to carry out an assessment of whether the controller or processor has complied or is complying with the data protection legislation.

(2) An assessment notice may require the controller or processor to do any of the following—

(a) permit the Commissioner to enter specified premises;

(b) direct the Commissioner to documents on the premises that are of a specified description;

(c) assist the Commissioner to view information of a specified description that is capable of being viewed using equipment on the premises;

(d) comply with a request from the Commissioner for—

(i) a copy of the documents to which the Commissioner is directed;

(ii) a copy (in such form as may be requested) of the information which the Commissioner is assisted to view;

(e) direct the Commissioner to equipment or other material on the premises which is of a specified description;

(f) permit the Commissioner to inspect or examine the documents, information, equipment or material to which the Commissioner is directed or which the Commissioner is assisted to view;

(g) permit the Commissioner to observe the processing of personal data that takes place on the premises;

(h) make available for interview by the Commissioner a specified number of people of a specified description who process personal data on behalf of the controller, not exceeding the number who are willing to be interviewed.

(3) In subsection (2), references to the Commissioner include references to the Commissioner's officers and staff.

(4) An assessment notice must, in relation to each requirement imposed by the notice, specify the time or times at which, or period or periods within which, the requirement must be complied with (but see the restrictions in subsections (6) to (8)).

(5) An assessment notice must provide information about the rights of appeal under section ~~161~~159.

(6) An assessment notice may not require a person to do anything before the end of the period within which an appeal can be brought against the notice.

(7) If an appeal is brought against an assessment notice, the controller or processor need not comply with a requirement in the notice pending the determination or withdrawal of the appeal.

(8) If an assessment notice—

(a) states that, in the Commissioner's opinion, it is necessary for the controller or processor to comply with a requirement in the notice urgently, and

(b) gives the Commissioner's reasons for reaching that opinion,

subsections (6) and (7) do not apply but the notice must not require the controller or processor to comply with the requirement before the end of the period of 7 days beginning ~~with the day on which~~ when the notice is given.

(9) The Commissioner may cancel an assessment notice by written notice to the controller or processor to whom it was given.

(10) Where the Commissioner gives an assessment notice to a processor, the Commissioner must, so far as reasonably practicable, give a copy of the notice to each controller for whom the processor processes personal data.

(11) In this section, "specified" means specified in an assessment notice.

147 Assessment notices: restrictions

(1) An assessment notice does not require a person to do something to the extent that requiring the person to do it would involve an infringement of the privileges of either House of Parliament.

(2) An assessment notice does not have effect so far as compliance would result in the disclosure of a communication which is made—

(a) between a professional legal adviser and the adviser's client, and

(b) in connection with the giving of legal advice to the client with respect to obligations, liabilities or rights under the data protection legislation.

(3) An assessment notice does not have effect so far as compliance would result in the disclosure of a communication which is made—

(a) between a professional legal adviser and the adviser's client or between such an adviser or client and another person,

(b) in connection with or in contemplation of proceedings under or arising out of the data protection legislation, and

(c) for the purposes of such proceedings.

(4) In subsections (2) and (3)—

(a) references to the client of a professional legal adviser include references to a person acting on behalf of such a client, and

(b) references to a communication include—

(i) a copy or other record of the communication, and

(ii) anything enclosed with or referred to in the communication if made as described in subsection (2)(b) or in subsection (3)(b) and (c).

(5) The Commissioner may not give a controller or processor an assessment notice with respect to the processing of personal data for the special purposes.

(6) The Commissioner may not give an assessment notice to—

(a) a body specified in section 23(3) of the Freedom of Information Act 2000 (bodies dealing with security matters), or

(b) the Office for Standards in Education, Children's Services and Skills in so far as it is a controller or processor in respect of information processed for the purposes of functions exercisable by Her Majesty's Chief Inspector of Education, Children's Services and Skills by virtue of section 5(1)(a) of the Care Standards Act 2000.

Enforcement notices

148 Enforcement notices

(1) Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person—

(a) to take steps specified in the notice, or

(b) to refrain from taking steps specified in the notice,

or both (and see also sections ~~149~~ 147 and ~~150~~148).

(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—

(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);

(b) a provision of Articles 12 to 22 of the GDPR or Part 3 or 4 of this Act conferring rights on a data subject;

(c) a provision of Articles 25 to 39 of the GDPR (obligations of controllers and processors);

(d) a requirement to communicate a personal data breach to the Commissioner or a data subject under section 67, 68 or 108 of this Act;

(e) the principles for transfers of personal data to third countries, non-Convention countries and international organisations in Articles 44 to 49 of the GDPR or in sections 73 to 78 or 109 of this Act.

(3) The second type of failure is where a monitoring body has failed, or is failing, to comply with an obligation under Article 41 of the GDPR (monitoring of approved codes of conduct).

(4) The third type of failure is where a person who is a certification provider—

(a) does not meet the requirements for accreditation,

(b) has failed, or is failing, to comply with an obligation under Article 42 or 43 of the GDPR (certification of controllers and processors), or

(c) has failed, or is failing, to comply with any other provision of the GDPR (whether in the person's capacity as a certification provider or otherwise).

(5) The fourth type of failure is where a controller has failed, or is failing, to comply with regulations under section ~~137~~136.

(6) An enforcement notice given in reliance on subsection (2), (3) or (5) may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure.

(7) An enforcement notice given in reliance on subsection (4) may only impose requirements which the Commissioner considers appropriate having regard to the failure (whether or not for the purpose of remedying the failure).

(8) The Secretary of State may by regulations confer power on the Commissioner to give an enforcement notice in respect of other failures to comply with the data protection legislation.

(9) Regulations under this section—

(a) may make provision about the giving of enforcement notices in respect of the failure,

(b) may amend this section and sections ~~149~~ 147 to ~~152~~150, and

(c) are subject to the affirmative resolution procedure.

149 Enforcement notices: supplementary

(1) An enforcement notice must—

(a) state what the person has failed or is failing to do, and

(b) give the Commissioner's reasons for reaching that opinion.

(2) In deciding whether to give an enforcement notice in reliance on section ~~148~~146(2), the Commissioner must consider whether the failure has caused or is likely to cause any person damage or distress.

(3) In relation to an enforcement notice given in reliance on section ~~148~~146(2), the Commissioner's power under section ~~148~~146(1)(b) to require a person to refrain from taking specified steps includes power—

(a) to impose a ban relating to all processing of personal data, or

(b) to impose a ban relating only to a specified description of processing of personal data, including by specifying one or more of the following—

(i) a description of personal data;

(ii) the purpose or manner of the processing;

(iii) the time when the processing takes place.

(4) An enforcement notice may specify the time or times at which, or period or periods within which, a requirement imposed by the notice must be complied with (but see the restrictions in subsections (6) to (8)).

(5) An enforcement notice must provide information about the rights of appeal under section ~~161~~159.

(6) An enforcement notice must not specify a time for compliance with a requirement in the notice which falls before the end of the period within which an appeal can be brought against the notice.

(7) If an appeal is brought against an enforcement notice, a requirement in the notice need not be complied with pending the determination or withdrawal of the appeal.

(8) If an enforcement notice—

(a) states that, in the Commissioner's opinion, it is necessary for a requirement to be complied with urgently, and

(b) gives the Commissioner's reasons for reaching that opinion,

subsections (6) and (7) do not apply but the notice must not require the requirement to be complied with before the end of the period of 7 days beginning ~~with the day on which~~ when the notice is given.

(9) In this section, "specified" means specified in an enforcement notice.

150 Enforcement notices: rectification and erasure of personal data etc

(1) Subsections (2) and (3) apply where an enforcement notice is given in respect of a failure by a controller or processor—

(a) to comply with a data protection principle relating to accuracy, or

(b) to comply with a data subject's request to exercise rights under Article 16, 17 or 18 of the GDPR (right to rectification, erasure or restriction on processing) or section 46, 47 or 100 of this Act.

(2) If the enforcement notice requires the controller or processor to rectify or erase inaccurate personal data, it may also require the controller or processor to rectify or erase any other data which—

(a) is held by the controller or processor, and

(b) contains an expression of opinion which appears to the Commissioner to be based on the inaccurate personal data.

(3) Where a controller or processor has accurately recorded personal data provided by the data subject or a third party but the data is inaccurate, the enforcement notice may require the controller or processor—

(a) to take steps specified in the notice to ensure the accuracy of the data,

(b) if relevant, to secure that the data indicates the data subject's view that the data is inaccurate, and

(c) to supplement the data with a statement of the true facts relating to the matters dealt with by the data that is approved by the Commissioner,

(as well as imposing requirements under subsection (2)).

(4) When deciding what steps it is reasonable to specify under subsection (3)(a), the Commissioner must have regard to the purpose for which the data was obtained and further processed.

(5) Subsections (6) and (7) apply where—

(a) an enforcement notice requires a controller or processor to rectify or erase personal data, or

(b) the Commissioner is satisfied that the processing of personal data which has been rectified or erased by the controller or processor involved a failure described in subsection (1).

(6) An enforcement notice may, if reasonably practicable, require the controller or processor to notify third parties to whom the data has been disclosed of the rectification or erasure.

(7) In determining whether it is reasonably practicable to require such notification, the Commissioner must have regard, in particular, to the number of people who would have to be notified.

(8) In this section, "data protection principle relating to accuracy" means the principle in—

(a) Article 5(1)(d) of the GDPR,

(b) section 38(1) of this Act, or

(c) section 89 of this Act.

151 Enforcement notices: restrictions

(1) The Commissioner may not give a controller or processor an enforcement notice in reliance on section ~~148~~146(2) with respect to the processing of personal data for the special purposes unless—

(a) a determination under section ~~174~~ 170 with respect to the data or the processing has taken effect, and

(b) a court has granted leave for the notice to be given.

(2) A court must not grant leave for the purposes of subsection (1)(b) unless it is satisfied that—

(a) the Commissioner has reason to suspect a failure described in section ~~148~~146(2) which is of substantial public importance, and

(b) the controller or processor has been given notice of the application for leave in accordance with rules of court or the case is urgent.

(3) An enforcement notice does not require a person to do something to the extent that requiring the person to do it would involve an infringement of the privileges of either House of Parliament.

(4) In the case of a joint controller in respect of the processing of personal data to which Part 3 or 4 applies whose responsibilities for compliance with that Part are determined in an arrangement under section 58 or 104, the Commissioner may only give the controller an enforcement notice in reliance on section ~~148~~146(2) if the controller is responsible for compliance with the provision, requirement or principle in question.

152 Enforcement notices: cancellation and variation

(1) The Commissioner may cancel or vary an enforcement notice by giving written notice to the person to whom it was given.

(2) A person to whom an enforcement notice is given may apply in writing to the Commissioner for the cancellation or variation of the notice.

(3) An application under subsection (2) may be made only—

(a) after the end of the period within which an appeal can be brought against the notice, and

(b) on the ground that, by reason of a change of circumstances, one or more of the provisions of that notice need not be complied with in order to remedy the failure identified in the notice.

Powers of entry and inspection

153 Powers of entry and inspection

Schedule 15 makes provision about powers of entry and inspection.

Penalties

154 Penalty notices

(1) If the Commissioner is satisfied that a person—

(a) has failed or is failing as described in section ~~148~~146(2), (3), (4) or (5), or

(b) has failed to comply with an information notice, an assessment notice or an enforcement notice,

the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.

(2) ~~In the case of a failure described in section 148(2), (3) or (4)~~Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant—

(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR;

(b) to the extent that the notice concerns another matter, the matters listed in subsection (3).

(3) Those matters are—

(a) the nature, gravity and duration of the failure;

(b) the intentional or negligent character of the failure;

(c) any action taken by the controller or processor to mitigate the damage or distress suffered by data subjects;

(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor in accordance with section 57, 66, 103 or 107;

(e) any relevant previous failures by the controller or processor;

(f) the degree of co-operation with the Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;

(g) the categories of personal data affected by the failure;

(h) the manner in which the infringement became known to the Commissioner, including whether, and if so to what extent, the controller or processor notified the Commissioner of the failure;

(i) the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;

(j) adherence to approved codes of conduct or certification mechanisms;

(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);

(l) whether the penalty would be effective, proportionate and dissuasive.

(4) Subsections (2) and (3) do not apply in the case of a decision or determination relating to a failure described in section 146(5).

(5) Schedule 16 makes further provision about penalty notices, including provision requiring the Commissioner to give a notice of intent to impose a penalty and provision about payment, variation, cancellation and enforcement.

(6) The Secretary of State may by regulations—

(a) confer power on the Commissioner to give a penalty notice in respect of other failures to comply with the data protection legislation, and

(b) provide for the maximum penalty that may be imposed in relation to such failures to be either the standard maximum amount or the higher maximum amount.

(7) Regulations under this section—

(a) may make provision about the giving of penalty notices in respect of the failure,

(b) may amend this section and sections ~~155~~ 153 to ~~157~~155, and

(c) are subject to the affirmative resolution procedure.

(8) In this section, "higher maximum amount" and "standard maximum amount" have the same meaning as in section ~~156~~154.

155 Penalty notices: restrictions

(1) The Commissioner may not give a controller or processor a penalty notice in reliance on section ~~148~~146(2) with respect to the processing of personal data for the special purposes unless—

(a) a determination under section ~~174~~ 170 with respect to the data or the processing has taken effect, and

(b) a court has granted leave for the notice to be given.

(2) A court must not grant leave for the purposes of subsection (1)(b) unless it is satisfied that—

(a) the Commissioner has reason to suspect a failure described in section ~~148~~146(2) which is of substantial public importance, and

(b) the controller or processor has been given notice of the application for leave in accordance with rules of court or the case is urgent.

(3) The Commissioner may not give a controller or processor a penalty notice with respect to the processing of personal data where the purposes and manner of the processing are determined by or on behalf of either House of Parliament.

(4) The Commissioner may not give a penalty notice to—

(a) the Crown Estate Commissioners, or

(b) a person who is a controller by virtue of section ~~202~~200(4) (controller for the Royal Household etc).

(5) In the case of a joint controller in respect of the processing of personal data to which Part 3 or 4 applies whose responsibilities for compliance with that Part are determined in an arrangement under section 58 or 104, the Commissioner may only give the controller a penalty notice in reliance on section ~~148~~146(2) if the controller is responsible for compliance with the provision, requirement or principle in question.

156 Maximum amount of penalty

(1) In relation to an infringement of a provision of the GDPR, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) the amount specified in Article 83 of the GDPR, or

(b) if an amount is not specified there, the standard maximum amount.

(2) In relation to an infringement of a provision of Part 3 of this Act, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) in relation to a failure to comply with section 35, 36, 37, 38(1), 39(1), 40, 44, 45, 46, 47, 48, 49, 52, 53, 73, 74, 75, 76, 77 or 78, the higher maximum amount, and

(b) otherwise, the standard maximum amount.

(3) In relation to an infringement of a provision of Part 4 of this Act, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) in relation to a failure to comply with section 86, 87, 88, 89, 90, 91, 93, 94, 100 or 109, the higher maximum amount, and

(b) otherwise, the standard maximum amount.

(4) In relation to a failure to comply with an information notice, an assessment notice or an enforcement notice, the maximum amount of the penalty that may be imposed by a penalty notice is the higher maximum amount.

(5) The "higher maximum amount" is—

(a) in the case of an undertaking, 20 million Euros or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or

(b) in any other case, 20 million Euros.

(6) The "standard maximum amount" is—

(a) in the case of an undertaking, 10 million Euros or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or

(b) in any other case, 10 million Euros.

(7) The maximum amount of a penalty in sterling must be determined by applying the spot rate of exchange set by the Bank of England on the day on which the penalty notice is given.

157 Fixed penalties for non-compliance with charges regulations

(1) The Commissioner must produce and publish a document specifying the amount of the penalty for a failure to comply with regulations made under section ~~137~~136.

(2) The Commissioner may specify different amounts for different types of failure.

(3) The maximum amount that may be specified is 150% of the highest charge payable by a controller in respect of a financial year in accordance with the regulations, disregarding any discount available under the regulations.

(4) The Commissioner—

(a) may alter or replace the document, and

(b) must publish any altered or replacement document.

(5) Before publishing a document under this section (including any altered or replacement document), the Commissioner must consult—

(a) the Secretary of State, and

(b) such other persons as the Secretary of State considers appropriate.

(6) The Commissioner must arrange for a document published under this section (including any altered or replacement document) to be laid before Parliament.

158 Amount of penalties: supplementary

(1) For the purposes of Article 83 of the GDPR and section ~~156~~154, the Secretary of State may by regulations—

(a) provide that a person of a description specified in the regulations is or is not an undertaking, and

(b) make provision about how an undertaking's turnover is to be determined.

(2) For the purposes of Article 83 of the GDPR, section ~~156~~ 154 and section ~~157~~155, the Secretary of State may by regulations provide that a period is or is not a financial year.

(3) Regulations under this section are subject to the affirmative resolution procedure.

Guidance

159 Guidance about regulatory action

(1) The Commissioner must produce and publish guidance about how the Commissioner proposes to exercise the Commissioner's functions in connection with—

(a) assessment notices,

(b) enforcement notices, and

(c) penalty notices.

(2) The Commissioner may produce and publish guidance about how the Commissioner proposes to exercise the Commissioner's other functions under this Part.

(3) In relation to assessment notices, the guidance must include—

(a) provision specifying factors to be considered in determining whether to give an assessment notice to a person;

(b) provision specifying descriptions of documents or information that—

(i) are not to be examined or inspected in accordance with an assessment notice, or

(ii) are to be so examined or inspected only by a person of a description specified in the guidance;

(c) provision about the nature of inspections and examinations carried out in accordance with an assessment notice;

(d) provision about the nature of interviews carried out in accordance with an assessment notice;

(e) provision about the preparation, issuing and publication by the Commissioner of assessment reports in respect of controllers and processors that have been given assessment notices.

(4) The guidance produced in accordance with subsection (3)(b) must include provisions that relate to—

(a) documents and information concerning an individual's physical or mental health;

(b) documents and information concerning the provision of social care for an individual.

(5) In relation to penalty notices, the guidance must include—

(a) provision about the circumstances in which the Commissioner would consider it appropriate to issue a penalty notice;

(b) provision about the circumstances in which the Commissioner would consider it appropriate to allow a ~~controller or processor~~ person to

make oral representations about the Commissioner's intention to give the person a ~~notice of intent~~penalty notice;

(c) provision explaining how the Commissioner will determine the amount of penalties.

(6) The Commissioner—

(a) may alter or replace guidance produced under this section, and

(b) must publish any altered or replacement guidance.

(7) Before producing guidance under this section (including any altered or replacement guidance), the Commissioner must consult—

(a) the Secretary of State, and

(b) such other persons as the Secretary of State considers appropriate.

(8) Section ~~160~~ 158 applies in relation to the first guidance under subsection (1).

(9) The Commissioner must arrange for other guidance under this section (including any altered or replacement guidance) to be laid before Parliament.

(10) In this section, "social care" has the same meaning as in Part 1 of the Health and Social Care Act 2008 (see section 9(3) of that Act).

160 Approval of first guidance about regulatory action

(1) When the first guidance is produced under section ~~159~~157(1)—

(a) the Commissioner must submit the final version to the Secretary of State, and

(b) the Secretary of State must lay the guidance before Parliament.

(2) If, within the 40-day period, either House of Parliament resolves not to approve the guidance—

(a) the Commissioner must not issue the guidance, and

(b) the Commissioner must produce another version of the guidance (and this section applies to that version).

(3) If, within the 40-day period, no such resolution is made—

(a) the Commissioner must issue the guidance, and

(b) the guidance comes into force at the end of the period of 21 days beginning with the day on which it is issued.

(4) Nothing in subsection (2)(a) prevents another version of the guidance being laid before Parliament.

(5) In this section, "the 40-day period" means—

(a) if the guidance is laid before both Houses of Parliament on the same day, the period of 40 days beginning with that day, or

(b) if the guidance is laid before the Houses of Parliament on different days, the period of 40 days beginning with the later of those days.

(6) In calculating the 40-day period, no account is to be taken of any period during which Parliament is dissolved or prorogued or during which both Houses of Parliament are adjourned for more than 4 days.

Appeals

161 Rights of appeal

(1) A person who is given any of the following notices may appeal to the Tribunal—

(a) an information notice;

(b) an assessment notice;

(c) an enforcement notice;

(d) a penalty notice;

(e) a penalty variation notice.

(2) Where a notice listed in subsection (1) contains a statement under section ~~143~~141(7)(a), ~~146~~144(8)(a) or ~~149~~147(8)(a) (urgency), the person given the notice may appeal against—

(a) the Commissioner's decision to include the statement in the notice, or

(b) the effect of its inclusion as respects any part of the notice,

whether or not the person appeals against the notice.

(3) A person who is given an enforcement notice may appeal to the Tribunal against the refusal of an application under section ~~152~~ 150 for the cancellation or variation of the notice.

(4) A person who is given a penalty notice or a penalty variation notice may appeal against the amount of the penalty specified in the notice, whether or not the person appeals against the notice.

(5) Where a determination is made under section ~~174~~ 170 in respect of the processing of personal data, the controller or processor may appeal to the Tribunal against the determination.

162 Determination of appeals

(1) Subsections (2) to (4) apply where a person appeals to the Tribunal under section ~~161~~159(1) or (4).

(2) The Tribunal may review any determination of fact on which the notice or decision against which the appeal is brought was based.

(3) If the Tribunal considers—

(a) that the notice or decision against which the appeal is brought is not in accordance with the law, or

(b) to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently,

the Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.

(4) Otherwise, the Tribunal must dismiss the appeal.

(5) On an appeal under section ~~161~~159(2), the Tribunal may direct—

(a) that the notice against which the appeal is brought is to have effect as if it did not contain the statement under section ~~143~~141(7)(a), ~~146~~144(8)(a) or ~~149~~147(8)(a) (urgency), or

(b) that the inclusion of that statement is not to have effect in relation to any part of the notice,

and may make such modifications to the notice as are required to give effect to the direction.

(6) On an appeal under section ~~161~~159(3), if the Tribunal considers that the enforcement notice ought to be cancelled or varied by reason of a change in circumstances, the Tribunal must cancel or vary the notice.

(7) On an appeal under section ~~161~~159(5), the Tribunal may cancel the Commissioner's determination.

Complaints

163 Complaints by data subjects

(1) Articles 57(1)(f) and (2) and 77 of the GDPR (data subject's right to lodge a complaint) confer rights on data subjects to complain to the Commissioner if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of the GDPR.

(2) A data subject may make a complaint to the Commissioner if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of Part 3 or 4 of this Act.

(3) The Commissioner must facilitate the making of complaints under subsection (2) by taking steps such as providing a complaint form which can be completed electronically and by other means.

(4) If the Commissioner receives a complaint under subsection (2), the Commissioner must—

(a) take appropriate steps to respond to the complaint,

(b) inform the complainant of the outcome of the complaint,

(c) inform the complainant of the rights under section ~~164~~162, and

(d) if asked to do so by the complainant, provide the complainant with further information about how to pursue the complaint.

(5) The reference in subsection (4)(a) to taking appropriate steps in response to a complaint includes—

(a) investigating the subject matter of the complaint, to the extent appropriate, and

(b) informing the complainant about progress on the complaint, including about whether further investigation or co-ordination with another supervisory authority or foreign designated authority is necessary.

(6) If the Commissioner receives a complaint relating to the infringement of a data subject's rights under provisions adopted by a member State other than the United Kingdom pursuant to the Law Enforcement Directive, the Commissioner must—

(a) send the complaint to the relevant supervisory authority for the purposes of that Directive,

(b) inform the complainant that the Commissioner has done so, and

(c) if asked to do so by the complainant, provide the complainant with further information about how to pursue the complaint.

(7) In this section—

"foreign designated authority" means an authority designated for the purposes of Article 13 of the Data Protection Convention by a party, other than the United Kingdom, which is bound by that Convention;

"supervisory authority" means a supervisory authority for the purposes of Article 51 of the GDPR or Article 41 of the Law Enforcement Directive in a member State other than the United Kingdom.

164 Orders to progress complaints

(1) This section applies where, after a data subject makes a complaint under section ~~163~~ 161 or Article 77 of the GDPR, the Commissioner—

(a) fails to take appropriate steps to respond to the complaint,

(b) fails to provide the complainant with information about progress on the complaint, or of the outcome of the complaint, before the end of the period of 3 months beginning ~~with the day on which~~ when the Commissioner received the complaint, or

(c) if the Commissioner's consideration of the complaint is not concluded during that period, fails to provide the complainant with such information during a subsequent period of 3 months.

(2) The Tribunal may, on an application by the data subject, make an order requiring the Commissioner—

(a) to take appropriate steps to respond to the complaint, or

(b) to inform the complainant of progress on the complaint, or of the outcome of the complaint, within a period specified in the order.

(3) An order under subsection (2)(a) may require the Commissioner—

(a) to take steps specified in the order;

(b) to conclude an investigation, or take a specified step, within a period specified in the order.

(4) Section ~~163~~161(5) applies for the purposes of subsections (1)(a) and (2)(a) as it applies for the purposes of section ~~163~~161(4)(a).

Remedies in the court

165 Compliance orders

(1) This section applies if, on an application by a data subject, a court is satisfied that there has been an infringement of the data subject's rights under the data protection legislation in contravention of that legislation.

(2) A court may make an order for the purposes of securing compliance with the data protection legislation which requires the controller in respect of the processing, or a processor acting on behalf of that controller—

(a) to take steps specified in the order, or

(b) to refrain from taking steps specified in the order.

(3) The order may, in relation to each step, specify the time at which, or the period within which, it must be taken.

(4) In subsection (1)—

(a) the reference to an application by a data subject includes an application made in exercise of the right under Article 79(1) of the GDPR (right to an effective remedy against a controller or processor);

(b) the reference to the data protection legislation does not include Part 4 of this Act or regulations made under that Part.

(5) In relation to a joint controller in respect of the processing of personal data to which Part 3 applies whose responsibilities are determined in an arrangement under section 58, a court may only make an order under this section if the controller is responsible for compliance with the provision of the data protection legislation that is contravened.

166 Compensation for contravention of the GDPR

(1) In Article 82 of the GDPR (right to compensation for material or non-material damage), "non-material damage" includes distress.

(2) Subsection (3) applies where—

(a) in accordance with rules of court, proceedings under Article 82 of the GDPR are brought by a representative body on behalf of a person, and

(b) a court orders the payment of compensation.

(3) The court may make an order providing for the compensation to be paid on behalf of the person to—

(a) the representative body, or

(b) such other person as the court thinks fit.

167 Compensation for contravention of other data protection legislation

(1) A person who suffers damage by reason of a contravention of a requirement of the data protection legislation, other than the GDPR, is entitled to compensation for that damage from the controller or the processor, subject to subsections (2) and (3).

(2) Under subsection (1)—

(a) a controller involved in processing of personal data is liable for any damage caused by the processing, and

(b) a processor involved in processing of personal data is liable for damage caused by the processing only if the processor—

(i) has not complied with an obligation under the data protection legislation specifically directed at processors, or

(ii) has acted outside, or contrary to, the controller's lawful instructions.

(3) A controller or processor is not liable as described in subsection (2) if the controller or processor proves that the controller or processor is not in any way responsible for the event giving rise to the damage.

(4) A joint controller in respect of the processing of personal data to which Part 3 or 4 applies whose responsibilities are determined in an arrangement under section 58 or 104 is only liable as described in subsection (2) if the controller is responsible for compliance with the provision of the data protection legislation that is contravened.

(5) In this section, "damage" includes financial loss and damage not involving financial loss, such as distress.

168 ~~Publishers of news-related material: damages and costs~~

(1) ~~This section applies where—~~

(a) ~~a relevant claim for breach of the data protection legislation is made against a person ("the defendant"),~~

(b) ~~the defendant was a relevant publisher at the material time, and~~

(c) ~~the claim is related to the publication of news-related material.~~

(2) ~~If the defendant was a member of an approved regulator at the time when the claim was commenced (or was unable to be a member at that time for reasons beyond the defendant's control or it would have been unreasonable in the circumstances for the defendant to have been a member at that time), the court must not award costs against the defendant unless satisfied that—~~

(a) ~~the issues raised by the claim could not have been resolved by using an arbitration scheme of the approved regulator, or~~

(b) ~~it is just and equitable in all the circumstances of the case to award costs against the defendant.~~

(3) ~~If the defendant was not a member of an approved regulator at the time when the claim was commenced (but would have been able to be a member at that time and it would have been reasonable in the circumstances for the defendant to have been a member at that time), the court must award costs against the defendant unless satisfied that—~~

(a) ~~the issues raised by the claim could not have been resolved by using an arbitration scheme of the approved regulator (had the defendant been a member), or~~

(b) ~~it is just and equitable in all the circumstances of the case to make a different award of costs or make no award of costs.~~

(4) ~~This section is not to be read as limiting any power to make rules of court.~~

(5) ~~This section does not apply until such time as a body is first recognised as an approved regulator.~~

169 ~~Publishers of news-related material: interpretive provisions~~

(1) ~~This section applies for the purposes of section 168.~~

(2) ~~"Approved regulator" means a body recognised as a regulator of relevant publishers.~~

(3) ~~For the purposes of subsection (2), a body is "recognised" as a regulator of relevant publishers if it is so recognised by any body established by Royal Charter (whether established before or after the coming into force of this section) with the purpose of carrying on activities relating to the recognition of independent regulators of relevant publishers.~~

(4) ~~"Relevant claim" means a civil claim made in respect of data protection under the data protection legislation.~~

(5) ~~The "material time", in relation to a relevant claim, is the time of the events giving rise to the claim.~~

(6) ~~"News-related material" means—~~

(a) ~~news or information about current affairs,~~

(b) ~~opinion about matters relating to the news or current affairs, or~~

(c) ~~gossip about celebrities, other public figures or other persons in the news.~~

(7) ~~A relevant claim is related to the publication of news-related material if the claim results from –~~

(a) ~~the publication of news-related material, or~~

(b) ~~activities carried on in connection with the publication of such material (whether or not the material is in fact published).~~

(8) ~~A reference to the "publication" of material is a reference to publication –~~

(a) ~~on a website,~~

(b) ~~in hard copy, or~~

(c) ~~by any other means;~~

~~and references to a person who "publishes" material are to be read accordingly.~~

(9) ~~A reference to "conduct" includes a reference to omissions; and a reference to a person's conduct includes a reference to a person's conduct after the events giving rise to the claim concerned.~~

(10) ~~"Relevant publisher" has the same meaning as in section 41 of the Crime and Courts Act 2013.~~

Offences relating to personal data

170 Unlawful obtaining etc of personal data

(1) It is an offence for a person knowingly or recklessly –

(a) to obtain or disclose personal data without the consent of the controller,

(b) to procure the disclosure of personal data to another person without the consent of the controller, or

(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

(2) It is a defence for a person charged with an offence under subsection (1) to prove that the obtaining, disclosing, procuring or retaining –

(a) was necessary for the purposes of preventing or detecting crime,

(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or

(c) in the particular circumstances, was justified as being in the public interest.

(3) It is also a defence for a person charged with an offence under subsection (1) to prove that –

(a) the person acted in the reasonable belief that the person had a legal right to do the obtaining, disclosing, procuring or retaining,

(b) the person acted in the reasonable belief that the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it, or

(c) the person acted –

(i) for the special purposes,

(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

(iii) in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or retaining was justified as being in the public interest.

(4) It is an offence for a person to sell personal data if the person obtained the data in circumstances in which an offence under subsection (1) was committed.

(5) It is an offence for a person to offer to sell personal data if the person—

(a) has obtained the data in circumstances in which an offence under subsection (1) was committed, or

(b) subsequently obtains the data in such circumstances.

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale is an offer to sell the data.

(7) In this section—

(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 59(8) or 105(3) of this Act (processor to be treated as controller in certain circumstances);

(b) where there is more than one controller, such references are references to the consent of one or more of them.

171 Re-identification of de-identified personal data

(1) It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.

(2) For the purposes of this section and section ~~172~~168—

(a) personal data is "de-identified" if it has been processed in such a manner that it can no longer be attributed, without more, to a specific data subject;

(b) a person "re-identifies" information if the person takes steps which result in the information no longer being de-identified within the meaning of paragraph (a).

(3) It is a defence for a person charged with an offence under subsection (1) to prove that the re-identification—

(a) was necessary for the purposes of preventing or detecting crime,

(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or

(c) in the particular circumstances, was justified as being in the public interest.

(4) It is also a defence for a person charged with an offence under subsection (1) to prove that—

(a) the person acted in the reasonable belief that the person—

(i) is the data subject to whom the information relates,

(ii) had the consent of that data subject, or

(iii) would have had such consent if the data subject had known about the re-identification and the circumstances of it,

(b) the person acted in the reasonable belief that the person—

(i) is the controller responsible for de-identifying the personal data,
(ii) had the consent of that controller, or
(iii) would have had such consent if that controller had known about the re-identification and the circumstances of it,

(c) the person acted—
(i) for the special purposes,
(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and
(iii) in the reasonable belief that in the particular circumstances the re-identification was justified as being in the public interest, or

(d) the effectiveness testing conditions were met (see section ~~172~~168).

(5) It is an offence for a person knowingly or recklessly to process personal data that is information that has been re-identified where the person does so—
(a) without the consent of the controller responsible for de-identifying the personal data, and
(b) in circumstances in which the re-identification was an offence under subsection (1).

(6) It is a defence for a person charged with an offence under subsection (5) to prove that the processing—
(a) was necessary for the purposes of preventing or detecting crime,
(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or
(c) in the particular circumstances, was justified as being in the public interest.

(7) It is also a defence for a person charged with an offence under subsection (5) to prove that—
(a) the person acted in the reasonable belief that the processing was lawful,
(b) the person acted in the reasonable belief that the person—
(i) had the consent of the controller responsible for de-identifying the personal data, or
(ii) would have had such consent if that controller had known about the processing and the circumstances of it, or
(c) the person acted—
(i) for the special purposes,
(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and
(iii) in the reasonable belief that in the particular circumstances the processing was justified as being in the public interest.

(8) In this section—
(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 59(8) or 105(3) of this Act (processor to be treated as controller in certain circumstances);
(b) where there is more than one controller, such references are references to the consent of one or more of them.

172 Re-identification: effectiveness testing conditions

(1) For the purposes of section ~~171~~167, in relation to a person who re-identifies information that is de-identified personal data, "the effectiveness testing conditions" means the conditions in subsections (2) and (3).

(2) The first condition is that the person acted—

(a) with a view to testing the effectiveness of the de-identification of personal data,

(b) without intending to cause, or threaten to cause, damage or distress to a person, and

(c) in the reasonable belief that, in the particular circumstances, re-identifying the information was justified as being in the public interest.

(3) The second condition is that the person notified the Commissioner or the controller responsible for de-identifying the personal data about the re-identification—

(a) without undue delay, and

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

(4) Where there is more than one controller responsible for de-identifying personal data, the requirement in subsection (3) is satisfied if one or more of them is notified.

173 Alteration etc of personal data to prevent disclosure

(1) Subsection (3) applies where—

(a) a request has been made in exercise of a data subject access right, and

(b) the person making the request would have been entitled to receive information in response to that request.

(2) In this section, "data subject access right" means a right under—

(a) Article 15 of the GDPR (right of access by the data subject);

(b) Article 20 of the GDPR (right to data portability);

(c) section 45 of this Act (law enforcement processing: right of access by the data subject);

(d) section 94 of this Act (intelligence services processing: right of access by the data subject).

(3) It is an offence for a person listed in subsection (4) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

(4) Those persons are—

(a) the controller, and

(b) a person who is employed by the controller, an officer of the controller or subject to the direction of the controller.

(5) It is a defence for a person charged with an offence under subsection (3) to prove that—

(a) the alteration, defacing, blocking, erasure, destruction or concealment of the information would have occurred in the absence of a request made in exercise of a data subject access right, or

(b) the person acted in the reasonable belief that the person making the request was not entitled to receive the information in response to the request.

The special purposes

174 The special purposes

(1) In this Part, "the special purposes" means one or more of the following—
(a) the purposes of journalism;
(b) academic purposes;
(c) artistic purposes;
(d) literary purposes.

(2) In this Part, "special purposes proceedings" means legal proceedings against a controller or processor which relate, wholly or partly, to personal data processed for the special purposes and which are—
(a) proceedings under section ~~165~~ 163 (including proceedings on an application under Article 79 of the GDPR), or
(b) proceedings under Article 82 of the GDPR or section ~~167~~165.

(3) The Commissioner may make a written determination, in relation to the processing of personal data, that—
(a) the personal data is not being processed only for the special purposes;
(b) the personal data is not being processed with a view to the publication by a person of journalistic, academic, artistic or literary material which has not previously been published by the controller.

(4) The Commissioner must give written notice of the determination to the controller and the processor.

(5) The notice must provide information about the rights of appeal under section ~~161~~159.

(6) The determination does not take effect until one of the following conditions is satisfied—
(a) the period for the controller or the processor to appeal against the determination has ended without an appeal having been brought, or
(b) an appeal has been brought against the determination and—
(i) the appeal and any further appeal in relation to the determination has been decided or has otherwise ended, and
(ii) the time for appealing against the result of the appeal or further appeal has ended without another appeal having been brought.

175 Provision of assistance in special purposes proceedings

(1) An individual who is a party, or prospective party, to special purposes proceedings may apply to the Commissioner for assistance in those proceedings.

(2) As soon as reasonably practicable after receiving an application under subsection (1), the Commissioner must decide whether, and to what extent, to grant it.

(3) The Commissioner must not grant the application unless, in the Commissioner's opinion, the case involves a matter of substantial public importance.

(4) If the Commissioner decides not to provide assistance, the Commissioner must, as soon as reasonably practicable, notify the applicant of the decision, giving reasons for the decision.

(5) If the Commissioner decides to provide assistance, the Commissioner must—

(a) as soon as reasonably practicable, notify the applicant of the decision, stating the extent of the assistance to be provided, and

(b) secure that the person against whom the proceedings are, or are to be, brought is informed that the Commissioner is providing assistance.

(6) The assistance that may be provided by the Commissioner includes—

(a) paying costs in connection with the proceedings, and

(b) indemnifying the applicant in respect of liability to pay costs, expenses or damages in connection with the proceedings.

(7) In England and Wales or Northern Ireland, the recovery of expenses incurred by the Commissioner in providing an applicant with assistance under this section (as taxed or assessed in accordance with rules of court) is to constitute a first charge for the benefit of the Commissioner—

(a) on any costs which, by virtue of any judgment or order of the court, are payable to the applicant by any other person in respect of the matter in connection with which the assistance is provided, and

(b) on any sum payable to the applicant under a compromise or settlement arrived at in connection with that matter to avoid, or bring to an end, any proceedings.

(8) In Scotland, the recovery of such expenses (as taxed or assessed in accordance with rules of court) is to be paid to the Commissioner, in priority to other debts—

(a) out of any expenses which, by virtue of any judgment or order of the court, are payable to the applicant by any other person in respect of the matter in connection with which the assistance is provided, and

(b) out of any sum payable to the applicant under a compromise or settlement arrived at in connection with that matter to avoid, or bring to an end, any proceedings.

176 Staying special purposes proceedings

(1) In any special purposes proceedings before a court, if the controller or processor claims, or it appears to the court, that any personal data to which the proceedings relate—

(a) is being processed only for the special purposes,

(b) is being processed with a view to the publication by any person of journalistic, academic, artistic or literary material, and

(c) has not previously been published by the controller,

the court must stay or, in Scotland, sist the proceedings.

(2) In considering, for the purposes of subsection (1)(c), whether material has previously been published, publication in the immediately preceding 24 hours is to be ignored.

(3) Under subsection (1), the court must stay or sist the proceedings until either of the following conditions is met—

(a) a determination of the Commissioner under section ~~174~~ 170 with respect to the personal data or the processing takes effect;

(b) where the proceedings were stayed or sisted on the making of a claim, the claim is withdrawn.

Jurisdiction of courts

177 Jurisdiction

(1) The jurisdiction conferred on a court by the provisions listed in subsection (2) is exercisable—

(a) in England and Wales, by the High Court or the county court,

(b) in Northern Ireland, by the High Court or a county court, and

(c) in Scotland, by the Court of Session or the sheriff,

subject to subsection (3).

(2) Those provisions are—

(a) section ~~151~~ 149 (enforcement notices and processing for the special purposes);

(b) section ~~155~~ 153 (penalty notices and processing for the special purposes);

(c) section ~~165~~ 163 and Article 79 of the GDPR (compliance orders);

(d) sections ~~166~~ 164 and ~~167~~ 165 and Article 82 of the GDPR (compensation).

(3) In relation to the processing of personal data to which Part 4 applies, the jurisdiction is exercisable only by the High Court or, in Scotland, the Court of Session.

Definitions

178 Interpretation of Part 6

In this Part—

"assessment notice" has the meaning given in section ~~146~~144;

"certification provider" has the meaning given in section 17;

"enforcement notice" has the meaning given in section ~~148~~146;

"information notice" has the meaning given in section ~~143~~141;

"penalty notice" has the meaning given in section ~~154~~152;

"penalty variation notice" has the meaning given in Schedule 16;

"representative", in relation to a controller or processor, means a person designated by the controller or processor under Article 27 of the GDPR to represent the controller or processor with regard to the controller's or processor's obligations under the GDPR.

PART 7

SUPPLEMENTARY AND FINAL PROVISION

Regulations under this Act

179 Regulations and consultation

(1) Regulations under this Act are to be made by statutory instrument.

(2) Before making regulations under this Act, the Secretary of State must consult—
(a) the Commissioner, and
(b) such other persons as the Secretary of State considers appropriate.

(3) Subsection (2) does not apply to regulations made under—
(a) section 23;
(b) section 30;
(c) section ~~204~~202;
(d) section ~~205~~203;
(e) section ~~206~~204;
(f) paragraph ~~13~~15 of Schedule 2.

(4) Subsection (2) does not apply to regulations made under section 18 where the Secretary of State has made an urgency statement in respect of them.

(5) Regulations under this Act may—
(a) make different provision for different purposes;
(b) include consequential, supplementary, incidental, transitional, transitory or saving provision.

(6) Where regulations under this Act are subject to "the negative resolution procedure" the statutory instrument containing the regulations is subject to annulment in pursuance of a resolution of either House of Parliament.

(7) Where regulations under this Act are subject to "the affirmative resolution procedure" the regulations may not be made unless a draft of the statutory instrument containing them has been laid before Parliament and approved by a resolution of each House of Parliament.

(8) Where regulations under this Act are subject to "the made affirmative resolution procedure"—
(a) the statutory instrument containing the regulations must be laid before Parliament after being made, together with the urgency statement in respect of them, and
(b) the regulations cease to have effect at the end of the period of 120 days beginning with the day on which the instrument is made, unless within that period the instrument is approved by a resolution of each House of Parliament.

(9) In calculating the period of 120 days, no account is to be taken of any time during which—
(a) Parliament is dissolved or prorogued, or
(b) both Houses of Parliament are adjourned for more than 4 days.

(10) Where regulations cease to have effect as a result of subsection (8), that does not—

(a) affect anything previously done under the regulations, or

(b) prevent the making of new regulations.

(11) Any provision that may be included in regulations under this Act subject to the negative resolution procedure may be made by regulations subject to the affirmative resolution procedure or the made affirmative resolution procedure.

(12) If a draft of a statutory instrument containing regulations under section 7 would, apart from this subsection, be treated for the purposes of the standing orders of either House of Parliament as a hybrid instrument, it is to proceed in that House as if it were not such an instrument.

(13) A requirement under a provision of this Act to consult may be satisfied by consultation before, as well as by consultation after, the provision comes into force.

(14) In this section, "urgency statement" has the meaning given in section 18(4).

Changes to the Data Protection Convention

180 Power to reflect changes to the Data Protection Convention

(1) The Secretary of State may by regulations make such provision as the Secretary of State considers necessary or appropriate in connection with an amendment of, or an instrument replacing, the Data Protection Convention which has effect, or is expected to have effect, in the United Kingdom.

(2) The power under subsection (1) includes power—

(a) to amend or replace the definition of "the Data Protection Convention" in section 3;

(b) to amend Chapter 3 of Part 2 of this Act;

(c) to amend Part 4 of this Act;

(d) to make provision about the functions of the Commissioner, courts or tribunals in connection with processing of personal data to which Chapter 3 of Part 2 or Part 4 of this Act applies, including provision amending Parts 5 to 7 of this Act;

(e) to make provision about the functions of the Commissioner in connection with the Data Protection Convention or an instrument replacing that Convention, including provision amending Parts 5 to 7 of this Act;

(f) to consequentially amend this Act.

(3) Regulations under this section are subject to the affirmative resolution procedure.

(4) Regulations under this section may not be made after the end of the period of 3 years beginning with the day on which this Act is passed.

Rights of the data subject

181 Prohibition of requirement to produce relevant records

(1) It is an offence for a person ("P1") to require another person to provide P1 with, or give P1 access to, a relevant record in connection with—
  (a) the recruitment of an employee by P1,
  (b) the continued employment of a person by P1, or
  (c) a contract for the provision of services to P1.

(2) It is an offence for a person ("P2") to require another person to provide P2 with, or give P2 access to, a relevant record if—
  (a) P2 is involved in the provision of goods, facilities or services to the public or a section of the public, and
  (b) the requirement is a condition of providing or offering to provide goods, facilities or services to the other person or to a third party.

(3) It is a defence for a person charged with an offence under subsection (1) or (2) to prove that imposing the requirement—
  (a) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or
  (b) in the particular circumstances, was justified as being in the public interest.

(4) The imposition of the requirement referred to in subsection (1) or (2) is not to be regarded as justified as being in the public interest on the ground that it would assist in the prevention or detection of crime, given Part 5 of the Police Act 1997 (certificates of criminal records etc).

(5) In subsections (1) and (2), the references to a person who requires another person to provide or give access to a relevant record include a person who asks another person to do so—
  (a) knowing that, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request, or
  (b) being reckless as to whether, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request,

and the references to a "requirement" in subsections (3) and (4) are to be interpreted accordingly.

(6) In this section—

"employment" means any employment, including—
  (a) work under a contract for services or as an office-holder,
  (b) work under an apprenticeship,
  (c) work experience as part of a training course or in the course of training for employment, and
  (d) voluntary work,

and "employee" is to be interpreted accordingly;

"relevant record" has the meaning given in Schedule 17 and references to a relevant record include—
  (a) a part of such a record, and
  (b) a copy of, or of part of, such a record.

182 Avoidance of certain contractual terms relating to health records

(1) A term or condition of a contract is void in so far as it purports to require an individual to supply another person with a record which—

(a) consists of the information contained in a health record, and

(b) has been or is to be obtained by a data subject in the exercise of a data subject access right.

(2) A term or condition of a contract is also void in so far as it purports to require an individual to produce such a record to another person.

(3) The references in subsections (1) and (2) to a record include a part of a record and a copy of all or part of a record.

(4) In this section, "data subject access right" means a right under—

(a) Article 15 of the GDPR (right of access by the data subject);

(b) Article 20 of the GDPR (right to data portability);

(c) section 45 of this Act (law enforcement processing: right of access by the data subject);

(d) section 94 of this Act (intelligence services processing: right of access by the data subject).

183 Data subject's rights and other prohibitions and restrictions

(1) An enactment or rule of law prohibiting or restricting the disclosure of information, or authorising the withholding of information, does not remove or restrict the obligations and rights provided for in the provisions listed in subsection (2), except as provided by or under the provisions listed in subsection (3).

(2) The provisions providing obligations and rights are—

(a) Chapter III of the GDPR (rights of the data subject),

(b) Chapter 3 of Part 3 of this Act (law enforcement processing: rights of the data subject), and

(c) Chapter 3 of Part 4 of this Act (intelligence services processing: rights of the data subject).

(3) The provisions providing exceptions are—

(a) in Chapter 2 of Part 2 of this Act, sections 15 and 16 and Schedules 2, 3 and 4,

(b) in Chapter 3 of Part 2 of this Act, sections 23, 24, 25 and 26,

(c) in Part 3 of this Act, sections 44(4), 45(4) and 48(3), and

(d) in Part 4 of this Act, Chapter 6.

Representation of data subjects

184 Representation of data subjects with their authority

(1) In relation to the processing of personal data to which the GDPR applies—

(a) Article ~~80~~ 80(1) of the GDPR (representation of data subjects) enables a data subject to authorise a body or other organisation which meets the conditions set out in that Article to exercise ~~certain~~ the data subject's rights under Articles 77, 78 and 79 of the GDPR (rights to lodge

complaints and to an effective judicial remedy) on the data subject's behalf, and

(b) a data subject may also authorise such a body or organisation to exercise the data subject's rights under Article 82 of the GDPR (right to compensation).

(2) In relation to the processing of personal data to which the GDPR does not apply, a body or other organisation which meets the conditions in subsections (3) and (4), if authorised to do so by a data subject, may exercise some or all of the following rights ~~under the following provisions~~ of a data subject on the data subject's behalf—

(a) rights under section ~~163~~161(2), (4)(d) and (6)(c) (complaints to the Commissioner);

(b) rights under section ~~164~~162(2) (orders for the Commissioner to progress complaints);

(c) rights under section ~~165~~163(1) (compliance orders);

(d) the right to bring judicial review proceedings against the Commissioner.

(3) The first condition is that the body or organisation, by virtue of its constitution or an enactment—

(a) is required (after payment of outgoings) to apply the whole of its income and any capital it expends for charitable or public purposes,

(b) is prohibited from directly or indirectly distributing amongst its members any part of its assets (otherwise than for charitable or public purposes), and

(c) has objectives which are in the public interest.

(4) The second condition is that the body or organisation is active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data.

(5) In this Act, references to a "representative body", in relation to a right of a data subject, are to a body or other organisation authorised to exercise the right on the data subject's behalf under Article 80 of the GDPR or this section.

185 ~~Data subject's rights and other prohibitions and restrictions~~

(1) ~~An enactment or rule of law prohibiting or restricting the disclosure of information, or authorising the withholding of information, does not remove or restrict the obligations and rights provided for in the provisions listed in subsection (2), except as provided by or under the provisions listed in subsection (3).~~

(2) ~~The provisions providing obligations and rights are—~~

186 Representation of data subjects with their authority: collective proceedings

(1) The Secretary of State may by regulations make provision for representative bodies to bring proceedings before a court or tribunal in England and Wales or Northern Ireland combining two or more relevant claims.

(2) In this section, "relevant claim", in relation to a representative body, means a claim in respect of a right of a data subject which the representative body is

authorised to exercise on the data subject's behalf under Article 80(1) of the GDPR or section 180.

(3) The power under subsection (1) includes power—

(a) to make provision about the proceedings;

(b) to confer functions on a person, including functions involving the exercise of a discretion;

(c) to make different provision in relation to England and Wales and in relation to Northern Ireland.

(4) The provision mentioned in subsection (3)(a) includes provision about—

(a) the effect of judgments and orders;

(b) agreements to settle claims;

(c) the assessment of the amount of compensation;

(d) the persons to whom compensation may or must be paid, including compensation not claimed by the data subject;

(e) costs.

(5) Regulations under this section are subject to the negative resolution procedure.

187 Duty to review provision for representation of data subjects

(1) Before the end of the review period, the Secretary of State must—

(a) review the matters listed in subsection (2) in relation to England and Wales and Northern Ireland,

(b) prepare a report of the review, and

(c) lay a copy of the report before Parliament.

(2) Those matters are—

(a) ~~Chapter III~~ the operation of ~~the GDPR~~ Article 80(~~rights~~ 1) of the ~~data subject)~~GDPR,

(b) ~~Chapter 3 of Part 3 of this Act (law enforcement processing: rights of the data subject), and~~

(c) ~~Chapter 3 of Part 4 of this Act (intelligence services processing: rights of the data subject).~~

(3) ~~The provisions providing exceptions are—~~

(a) ~~in Chapter 2 of Part 2 of this Act (including as applied by Chapter 3 of that Part), sections 15 and 16 and Schedules 2, 3 and 4,~~

(b) ~~in Chapter 3 of Part 2 of this Act, sections 23, 24, 25 and 26,~~

(c) ~~in Part 3 of this Act, sections 44(4), 45(4) and 48(3), and~~

(d) ~~in Part 4 of this Act, Chapter 6.~~

(e) the operation of section 180,

(f) the merits of exercising the power under Article 80(2) of the GDPR (power to enable a body or other organisation which meets the conditions in Article 80(1) of the GDPR to exercise some or all of a data subject's rights under Articles 77, 78 and 79 of the GDPR without being authorised to do so by the data subject), and

(g) the merits of making equivalent provision in relation to data subjects' rights under Article 82 of the GDPR (right to compensation).

(4) "The review period" is the period of 30 months beginning when section 180 comes into force.

(5) After the report under subsection (1) is laid before Parliament, the Secretary of State may by regulations—

(a) exercise the powers under Article 80(2) of the GDPR in relation to England and Wales and Northern Ireland, and

(b) make provision enabling a body or other organisation which meets the conditions in Article 80(1) of the GDPR to exercise a data subject's rights under Article 82 of the GDPR in England and Wales and Northern Ireland without being authorised to do so by the data subject.

(6) The powers under subsection (4) include power—

(a) to make provision enabling a data subject to prevent a body or other organisation from exercising, or continuing to exercise, the data subject's rights;

(b) to make provision about proceedings before a court or tribunal where a body or organisation exercises a data subject's rights,

(c) to make provision for bodies or other organisations to bring proceedings before a court or tribunal combining two or more claims in respect of a right of a data subject;

(d) to confer functions on a person, including functions involving the exercise of a discretion;

(e) to amend sections 162 to 164, 173, 180, 194, 196 and 197;

(f) to insert new sections and Schedules into Part 6 or 7;

(g) to make different provision in relation to England and Wales and in relation to Northern Ireland.

(7) The provision mentioned in subsection (5)(b) and (c) includes provision about—

(a) the effect of judgments and orders;

(b) agreements to settle claims;

(c) the assessment of the amount of compensation;

(d) the persons to whom compensation may or must be paid, including compensation not claimed by the data subject;

(e) costs.

(8) Regulations under this section are subject to the affirmative resolution procedure.

Framework for Data Processing by Government

188 Framework for Data Processing by Government

(1) The Secretary of State may prepare a document, called the Framework for Data Processing by Government, which contains guidance about the processing of personal data in connection with the exercise of functions of—

(a) the Crown, a Minister of the Crown or a United Kingdom government department, and

(b) a person with functions of a public nature who is specified or described in regulations made by the Secretary of State.

(2) The document may make provision relating to all of those functions or only to particular functions or persons.

(3) The document may not make provision relating to, or to the functions of, a part of the Scottish Administration, the Welsh Government, a Northern Ireland Minister or a Northern Ireland department.

(4) The Secretary of State may from time to time prepare amendments of the document or a replacement document.

(5) Before preparing a document or amendments under this section, the Secretary of State must consult—

(a) the Commissioner, and

(b) any other person the Secretary of State considers it appropriate to consult.

(6) Regulations under subsection (1)(b) are subject to the negative resolution procedure.

(7) In this section, "Northern Ireland Minister" includes the First Minister and deputy First Minister in Northern Ireland.

189 Approval of the Framework

(1) Before issuing a document prepared under section ~~185~~183, the Secretary of State must lay it before Parliament.

(2) If, within the 40-day period, either House of Parliament resolves not to approve the document, the Secretary of State must not issue it.

(3) If no such resolution is made within that period—

(a) the Secretary of State must issue the document, and

(b) the document comes into force at the end of the period of 21 days beginning with the day on which it is issued.

(4) Nothing in subsection (2) prevents another version of the document being laid before Parliament.

(5) In this section, "the 40-day period" means—

(a) if the document is laid before both Houses of Parliament on the same day, the period of 40 days beginning with that day, or

(b) if the document is laid before the Houses of Parliament on different days, the period of 40 days beginning with the later of those days.

(6) In calculating the 40-day period, no account is to be taken of any period during which Parliament is dissolved or prorogued or during which both Houses of Parliament are adjourned for more than 4 days.

(7) This section applies in relation to amendments prepared under section ~~185~~183 as it applies in relation to a document prepared under that section.

190 Publication and review of the Framework

(1) The Secretary of State must publish a document issued under section ~~186~~184(3).

(2) Where an amendment of a document is issued under section ~~186~~184(3), the Secretary of State must publish—

(a) the amendment, or

(b) the document as amended by it.

(3) The Secretary of State must keep under review the document issued under section ~~186~~184(3) for the time being in force.

(4) Where the Secretary of State becomes aware that the terms of such a document could result in a breach of an international obligation of the United Kingdom, the Secretary of State must exercise the power under section ~~185~~183(4) with a view to remedying the situation.

191 Effect of the Framework

(1) When carrying out processing of personal data which is the subject of a document issued under section ~~186~~184(3) which is for the time being in force, a person must have regard to the document.

(2) A failure to act in accordance with a provision of such a document does not of itself make a person liable to legal proceedings in a court or tribunal.

(3) A document issued under section ~~186~~184(3), including an amendment or replacement document, is admissible in evidence in legal proceedings.

(4) In any legal proceedings before a court or tribunal, the court or tribunal must take into account a provision of any document issued under section ~~186~~184(3) in determining a question arising in the proceedings if—

(a) the question relates to a time when the provision was in force, and

(b) the provision appears to the court or tribunal to be relevant to the question.

(5) In determining a question arising in connection with the carrying out of any of the Commissioner's functions, the Commissioner must take into account a provision of a document issued under section ~~186~~184(3) if—

(a) the question relates to a time when the provision was in force, and

(b) the provision appears to the Commissioner to be relevant to the question.

Offences

192 Penalties for offences

(1) A person who commits an offence under section 119 or ~~173~~ 169 or paragraph ~~15~~15 of Schedule 15 is liable—

(a) on summary conviction in England and Wales, to a fine;

(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding level 5 on the standard scale.

(2) A person who commits an offence under section ~~132~~131, ~~145~~143, ~~170~~166, ~~171~~ 167 or ~~181~~ 177 is liable—

(a) on summary conviction in England and Wales, to a fine;

(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding the statutory maximum;

(c) on conviction on indictment, to a fine.

(3) Subsections (4) and (5) apply where a person is convicted of an offence under section ~~170~~ 166 or ~~181~~177.

(4) The court by or before which the person is convicted may order a document or other material to be forfeited, destroyed or erased if—

(a) it has been used in connection with the processing of personal data, and

(b) it appears to the court to be connected with the commission of the offence,

subject to subsection (5).

(5) If a person, other than the offender, who claims to be the owner of the material, or to be otherwise interested in the material, applies to be heard by the court, the court must not make an order under subsection (4) without giving the person an opportunity to show why the order should not be made.

193 Prosecution

(1) In England and Wales, proceedings for an offence under this Act may be instituted only—

(a) by the Commissioner, or

(b) by or with the consent of the Director of Public Prosecutions.

(2) In Northern Ireland, proceedings for an offence under this Act may be instituted only—

(a) by the Commissioner, or

(b) by or with the consent of the Director of Public Prosecutions for Northern Ireland.

(3) Subject to subsection (4), summary proceedings for an offence under section ~~173~~ 169 (alteration etc of personal data to prevent disclosure) may be brought within the period of 6 months beginning with the day on which the prosecutor first knew of evidence that, in the prosecutor's opinion, was sufficient to bring the proceedings.

(4) Such proceedings may not be brought after the end of the period of 3 years beginning with the day on which the offence was committed.

(5) A certificate signed by or on behalf of the prosecutor and stating the day on which the 6 month period described in subsection (3) began is conclusive evidence of that fact.

(6) A certificate purporting to be signed as described in subsection (5) is to be treated as so signed unless the contrary is proved.

(7) In relation to proceedings in Scotland, section 136(3) of the Criminal Procedure (Scotland) Act 1995 (deemed date of commencement of proceedings) applies for the purposes of this section as it applies for the purposes of that section.

194 Liability of directors etc

(1) Subsection (2) applies where—

(a) an offence under this Act has been committed by a body corporate, and

(b) it is proved to have been committed with the consent or connivance of or to be attributable to neglect on the part of—

(i) a director, manager, secretary or similar officer of the body corporate, or

(ii) a person who was purporting to act in such a capacity.

(2) The director, manager, secretary, officer or person, as well as the body corporate, is guilty of the offence and liable to be proceeded against and punished accordingly.

(3) Where the affairs of a body corporate are managed by its members, subsections (1) and (2) apply in relation to the acts and omissions of a member in connection with the member's management functions in relation to the body as if the member were a director of the body corporate.

(4) Subsection (5) applies where—

(a) an offence under this Act has been committed by a Scottish partnership, and

(b) the contravention in question is proved to have occurred with the consent or connivance of, or to be attributable to any neglect on the part of, a partner.

(5) The partner, as well as the partnership, is guilty of the offence and liable to be proceeded against and punished accordingly.

195 Recordable offences

(1) The National Police Records (Recordable Offences) Regulations 2000 (S.I. 2000/1139) have effect as if the offences under the following provisions were listed in the Schedule to the Regulations—

(a) section 119;

(b) section ~~132~~131;

(c) section ~~145~~143;

(d) section ~~170~~166;

(e) section ~~171~~167;

(f) section ~~173~~169;

(g) section ~~181~~177;

(h) paragraph ~~15~~15 of Schedule 15.

(2) Regulations under section 27(4) of the Police and Criminal Evidence Act 1984 (recordable offences) may repeal subsection (1).

196 Guidance about PACE codes of practice

(1) The Commissioner must produce and publish guidance about how the Commissioner proposes to perform the duty under section 67(9) of the Police and Criminal Evidence Act 1984 (duty to have regard to codes of practice under that Act when investigating offences and charging offenders) in connection with offences under this Act.

(2) The Commissioner—

(a) may alter or replace the guidance, and

(b) must publish any altered or replacement guidance.

(3) The Commissioner must consult the Secretary of State before publishing guidance under this section (including any altered or replacement guidance).

(4) The Commissioner must arrange for guidance under this section (including any altered or replacement guidance) to be laid before Parliament.

The Tribunal

197 Disclosure of information to the Tribunal

(1) No enactment or rule of law prohibiting or restricting the disclosure of information precludes a person from providing the First-tier Tribunal or the Upper Tribunal with information necessary for the discharge of—

(a) its functions under the data protection legislation, or

(b) its other functions relating to the Commissioner's acts and omissions.

(2) But this section does not authorise the making of a disclosure which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

(3) 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 (2) has effect as if it included a reference to that Part.

198 Proceedings in the First-tier Tribunal: contempt

(1) This section applies where—

(a) a person does something, or fails to do something, in relation to proceedings before the First-tier Tribunal—

(i) on an appeal under section 27, 79, 111 or ~~161~~159, or

(ii) for an order under section ~~164~~162, and

(b) if those proceedings were proceedings before a court having power to commit for contempt, the act or omission would constitute contempt of court.

(2) The First-tier Tribunal may certify the offence to the Upper Tribunal.

(3) Where an offence is certified under subsection (2), the Upper Tribunal may—

(a) inquire into the matter, and

(b) deal with the person charged with the offence in any manner in which it could deal with the person if the offence had been committed in relation to the Upper Tribunal.

(4) Before exercising the power under subsection (3)(b), the Upper Tribunal must—

(a) hear any witness who may be produced against or on behalf of the person charged with the offence, and

(b) hear any statement that may be offered in defence.

199 Tribunal Procedure Rules

(1) Tribunal Procedure Rules may make provision for regulating—

(a) the exercise of the rights of appeal conferred by section 27, 79, 111 or ~~161~~159, and

(b) the exercise of the rights of data subjects under section ~~164~~162, including their exercise by a representative body.

(2) In relation to proceedings involving the exercise of those rights, Tribunal Procedure Rules may make provision about—

(a) securing the production of material used for the processing of personal data, and

(b) the inspection, examination, operation and testing of equipment or material used in connection with the processing of personal data.

Definitions

200 Meaning of "health professional" and "social work professional"

(1) In this Act, "health professional" means any of the following—

(a) a registered medical practitioner;

(b) a registered nurse or midwife;

(c) a registered dentist within the meaning of the Dentists Act 1984 (see section 53 of that Act);

(d) a registered dispensing optician or a registered optometrist within the meaning of the Opticians Act 1989 (see section 36 of that Act);

(e) a registered osteopath with the meaning of the Osteopaths Act 1993 (see section 41 of that Act);

(f) a registered chiropractor within the meaning of the Chiropractors Act 1994 (see section 43 of that Act);

(g) a person registered as a member of a profession to which the Health and Social Work Professions Order 2001 (S.I. 2002/254) for the time being extends, other than the social work profession in England;

(h) a registered pharmacist or a registered pharmacy technician within the meaning of the Pharmacy Order 2010 (S.I. 2010/231) (see ~~Article~~ article 3 of that Order);

(i) a registered person within the meaning of the Pharmacy (Northern Ireland) Order 1976 (S.I. 1976/1213 (N.I. 22)) (see Article 2 of that Order);

(j) a child psychotherapist;

(k) a scientist employed by a health service body as head of a department.

(2) In this Act, "social work professional" means any of the following—

(a) a person registered as a social worker in England in the register maintained under the Health and Social Work Professions Order 2001 (S.I. 2002/254);

(b) a person registered as a social worker in the register maintained by Social Care Wales under section 80 of the Regulation and Inspection of Social Care (Wales) Act 2016 (anaw 2);

(c) a person registered as a social worker in the register maintained by the Scottish Social Services Council under section 44 of the Regulation of Care (Scotland) Act 2001 (asp 8);

(d) a person registered as a social worker in the register maintained by the Northern Ireland Social Care Council under section 3 of the Health and Personal Social Services Act (Northern Ireland) 2001 (c. 3 (N.I.)).

(3) In subsection (1)(a) "registered medical practitioner" includes a person who is provisionally registered under section 15 or 21 of the Medical Act 1983 and is engaged in such employment as is mentioned in subsection (3) of that section.

(4) In subsection (1)(k) "health service body" means any of the following—

(a) the Secretary of State in relation to the exercise of functions under section 2A or 2B of, or paragraph 7C, 8 or 12 of Schedule 1 to, the National Health Service Act 2006;

(b) a local authority in relation to the exercise of functions under section 2B or 111 of, or any of paragraphs 1 to 7B or 13 of Schedule 1 to, the National Health Service Act 2006;

(c) a National Health Service trust first established under section 25 of the National Health Service Act 2006;

(d) a Special Health Authority established under section 28 of the National Health Service Act 2006;

(e) an NHS foundation trust;

(f) the National Institute for Health and Care Excellence;

(g) the Health and Social Care Information Centre;

(h) a National Health Service trust first established under section 5 of the National Health Service and Community Care Act 1990;

(i) a Local Health Board established under section 11 of the National Health Service (Wales) Act 2006;

(j) a National Health Service trust first established under section 18 of the National Health Service (Wales) Act 2006;

(k) a Special Health Authority established under section 22 of the National Health Service (Wales) Act 2006;

(l) a Health Board within the meaning of the National Health Service (Scotland) Act 1978;

(m) a Special Health Board within the meaning of the National Health Service (Scotland) Act 1978;

(n) a National Health Service trust first established under section 12A of the National Health Service (Scotland) Act 1978;

(o) the managers of a State Hospital provided under section 102 of the National Health Service (Scotland) Act 1978;

(p) the Regional Health and Social Care Board established under section 7 of the Health and Social Care (Reform) Act (Northern Ireland) 2009 (c. 1 (N.I));

(q) a special health and social care agency established under the Health and Personal Social Services (Special Agencies) (Northern Ireland) Order 1990 (S.I. 1990/247 (N.I. 3));

(r) a Health and Social Care trust established under Article 10 of the Health and Personal Social Services (Northern Ireland) Order 1991 (S.I. 1991/194 (N.I. 1)).

201 ~~Other definitions~~General interpretation

(1) In this Act—

"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data;

"data concerning health" means personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveals information about his or her health status;

"enactment" includes—

(a) an enactment passed or made after this Act,
(b) an enactment comprised in subordinate legislation,
(c) an enactment comprised in, or in an instrument made under, a Measure or Act of the National Assembly for Wales,
(d) an enactment comprised in, or in an instrument made under, an Act of the Scottish Parliament, and
(e) an enactment comprised in, or in an instrument made under, Northern Ireland legislation;

"genetic data" means personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about the physiology or the health of that individual and which results, in particular, from an analysis of a biological sample from the individual in question;

~~"government department" includes —~~

"government department" includes the following (except in the expression "United Kingdom government department") —

(a) a part of the Scottish Administration;
(b) a Northern Ireland department;
(c) the Welsh Government;
(d) a body or authority exercising statutory functions on behalf of the Crown;

"health record" means a record which —

(a) consists of data concerning health, and
(b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates;

"inaccurate", in relation to personal data, means incorrect or misleading as to any matter of fact;

"international obligation of the United Kingdom" includes —

(a) an EU obligation, and
(b) an obligation that arises under an international agreement or arrangement to which the United Kingdom is a party;

"international organisation" means an organisation and its subordinate bodies governed by international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

"Minister of the Crown" has the same meaning as in the Ministers of the Crown Act 1975;

"publish" means make available to the public or a section of the public (and related expressions are to be read accordingly);

"subordinate legislation" has the meaning given in the Interpretation Act 1978;

"tribunal" means any tribunal in which legal proceedings may be brought;

"the Tribunal", in relation to an application or appeal under this Act, means —

(a) the Upper Tribunal, in any case where it is determined by or under Tribunal Procedure Rules that the Upper Tribunal is to hear the application or appeal, or
(b) the First-tier Tribunal, in any other case.

(2) References in this Act to a period expressed in hours, days, weeks, months or years are to be interpreted in accordance with Article 3 of Regulation (EEC, Euratom) No. 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits, except in—

(a) section 124(4), (7) and (8);
(b) section 158(3), (5) and (6);
(c) section 172(2);
(d) section 175(8) and (9);
(e) section 176(4);
(f) section 184(3), (5) and (6);
(g) section 188(3) and (4);
(h) paragraph 23(4) and (5) of Schedule 1;
(i) paragraphs 5(4) and 6(4) of Schedule 3;
(j) Schedule 5;
(k) paragraph 11(5) of Schedule 12;
(l) Schedule 15;

(and the references in section 5 to terms used in Chapter 2 or 3 of Part 2 do not include references to a period expressed in hours, days, weeks, months or years).

(3) Section 3(14)(b) (interpretation of references to Chapter 2 of Part 2 in Parts 5 to 7) and the amendments in Schedule 18 which make equivalent provision are not to be treated as implying a contrary intention for the purposes of section 20(2) of the Interpretation Act 1978, or any similar provision in another enactment, as it applies to other references to, or to a provision of, Chapter 2 of Part 2 of this Act.

202 Index of defined expressions

The Table below lists provisions which define or otherwise explain terms defined for this Act, for a Part of this Act or for Chapter 2 or 3 of Part 2 of this Act.

the affirmative resolution procedure	section ~~179~~175
the applied Chapter 2 (in Chapter 3 of Part 2)	section 22
the applied GDPR	section 3
assessment notice (in Part 6)	section ~~178~~174
biometric data	section ~~198~~196
certification provider (in Part 6)	section ~~178~~174
the Commissioner	section 3
competent authority (in Part 3)	section 30
consent (in Part 4)	section 84
controller	section 3

data concerning health	section ~~198~~196
the Data Protection Convention	section 3
the data protection legislation	section 3
data subject	section 3
employee (in Parts 3 and 4)	sections 33 and 84
enactment	section ~~198~~196
enforcement notice (in Part 6)	section ~~178~~174
filing system	section 3
FOI public authority (in Chapter 3 of Part 2)	section 21
the GDPR	section 3
genetic data	section ~~198~~196
government department	section ~~198~~196
health professional	section ~~197~~195
health record	section ~~198~~196
identifiable living individual	section 3
inaccurate	section ~~198~~ 196
information notice (in Part 6)	section ~~178~~174
intelligence service (in Part 4)	section 82
international obligation of the United Kingdom	section ~~198~~196
international organisation	section ~~198~~196
the Law Enforcement Directive	section 3
the law enforcement purposes (in Part 3)	section 31
the made affirmative resolution procedure	section ~~179~~175
Minister of the Crown	section ~~198~~196
the negative resolution procedure	section ~~179~~175
penalty notice (in Part 6)	section ~~178~~174
penalty variation notice (in Part 6)	section ~~178~~174
personal data	section 3

personal data breach (in Parts 3 and 4)	sections 33 and 84
processing	section 3
processor	section 3
profiling (in Part 3)	section 33
public authority (in the GDPR and Part 2)	section 7
public body (in the GDPR and Part 2)	section 7
publish	section ~~198~~196
recipient (in Parts 3 and 4)	sections 33 and 84
representative (in Part 6)	section ~~178~~174
representative body (in relation to a right of a data subject)	section ~~183~~180
restriction of processing (in Parts 3 and 4)	sections 33 and 84
social work professional	section ~~197~~195
the special purposes (in Part 6)	section ~~174~~170
special purposes proceedings (in Part 6)	section ~~174~~170
subordinate legislation	section ~~198~~196
third country (in Part 3)	section 33
tribunal	section ~~198~~196
the Tribunal	section ~~198~~196

Territorial application

203 Territorial application of this Act

(1) ~~This Act applies to a controller in respect of the processing of personal data only if the controller is established in the United Kingdom and the personal data is processed in the context of the activities of that establishment, subject to subsection (3).~~

(2) ~~This Act applies to a processor in respect of the processing of personal data only if—~~

(a) ~~the controller on whose behalf the processor acts is established in the United Kingdom and the personal data is processed in the context of the activities of that establishment, or~~

(b) ~~the processor is established in the United Kingdom and the personal data is processed in the context of the activities of that establishment,~~

~~subject to subsection (4).~~

(1) This Act applies only to processing of personal data described in subsections (2) and (3).

(2) It applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the United Kingdom, whether or not the processing takes place in the United Kingdom.

(3) ~~This Act~~ It also applies to ~~a controller in respect of~~ the processing of personal data to which Chapter ~~2~~ 2 of Part ~~2~~ 2 (the GDPR) applies where—

(a) ~~the controller is established in a country or territory other than the United Kingdom and the personal data is processed in the context of the activities of that establishment,~~

(b) the processing is carried out in the context of the activities of an establishment of a controller or processor in a country or territory that is not a member State, whether or not the processing takes place in such a country or territory,

(c) the personal data relates to ~~an individual~~ a data subject who is in the United Kingdom when the processing takes place, and

(d) ~~the purpose of the processing is—~~

(e) the processing activities are related to—

(i) ~~to offer~~ the offering of goods or services to ~~individuals~~ data subjects in the United Kingdom, whether or not for payment, or

(ii) ~~to monitor individuals~~the monitoring of data subjects' behaviour in the United Kingdom.

(4) ~~This Act also applies to a processor in respect of the processing of personal data to which Chapter 2 of Part 2 (the GDPR) applies where—~~

(a) ~~the controller on whose behalf the processor acts is established in a country or territory other than the United Kingdom and the personal data is processed in the context of the activities of that establishment, or~~

(b) ~~the processor is established in a country or territory other than the United Kingdom and the personal data is processed in the context of the activities of that establishment,~~

~~and the conditions in subsection (3)(b) and (c) are satisfied.~~

(5) Subsections ~~(1)~~ (1) to ~~(4)~~ (3) have effect subject to any provision made under section 120 providing for the Commissioner to carry out functions in relation to other ~~controllers or processors~~processing of personal data.

(5) Section 3(14)(c) does not apply to the reference to the processing of personal data in subsection (2).

(6) The reference in subsection (3) to Chapter 2 of Part 2 (the GDPR) does not include that Chapter as applied by Chapter 3 of Part 2 (the applied GDPR).

(7) In this section, references to a person ~~established~~ who has an establishment in the United Kingdom include the following—

(a) an individual who is ordinarily resident in the United Kingdom,

(b) a body incorporated under the law of the United Kingdom or a part of the United Kingdom,

(c) a partnership or other unincorporated association formed under the law of the United Kingdom or a part of the United Kingdom, and

(d) a person not within paragraph ~~(a)~~(a), ~~(b)~~(b) or ~~(c)~~(c) who maintains, and carries on activities through, an office, branch or agency or other stable arrangements in the United Kingdom,

and references to a person who has an establishment in another country or territory have a corresponding meaning.

(8) ~~For the purposes of this section —~~

(a) ~~a person who is treated as a controller by virtue of Article 28(10) of the GDPR or section 59(8) or 105(3) of this Act (processor to be treated as controller in certain circumstances) is to be treated as a processor;~~

(b) ~~where there is more than one controller, the references in subsections (2)(a) and (4)(a) to the controller are to one or more of them.~~

General

204 Children in Scotland

(1) Subsections (2) and (3) apply where a question falls to be determined in Scotland as to the legal capacity of a person aged under 16 to—

(a) exercise a right conferred by the data protection legislation, or

(b) give consent for the purposes of the data protection legislation.

(2) The person is to be taken to have that capacity where the person has a general understanding of what it means to exercise the right or give such consent.

(3) A person aged 12 or over is to be presumed to be of sufficient age and maturity to have such understanding, unless the contrary is shown.

205 Application to the Crown

(1) This Act binds the Crown.

(2) For the purposes of the GDPR and this Act, each government department is to be treated as a person separate from the other government departments (to the extent that is not already the case).

(3) Where government departments are not able to enter into contracts with each other, a provision of the GDPR or this Act that would require relations between them to be governed by a contract (or other binding legal act) in writing is to be treated as satisfied if the relations are the subject of a memorandum of understanding between them.

(4) Where the purposes for which and the manner in which personal data is, or is to be, processed are determined by a person acting on behalf of the Royal Household, the Duchy of Lancaster or the Duchy of Cornwall, the controller in respect of that data for the purposes of the GDPR and this Act is—

(a) in relation to the Royal Household, the Keeper of the Privy Purse,

(b) in relation to the Duchy of Lancaster, such person as the Chancellor of the Duchy appoints, and

(c) in relation to the Duchy of Cornwall, such person as the Duke of Cornwall, or the possessor for the time being of the Duchy of Cornwall, appoints.

(5) Different persons may be appointed under subsection (4)(b) or (c) for different purposes.

(6) As regards criminal liability—

(a) a government department is not liable to prosecution under this Act;

(b) nothing in subsection (4) makes a person who is a controller by virtue of that subsection liable to prosecution under this Act;

(c) a person in the service of the Crown is liable to prosecution under the provisions of this Act listed in subsection (7).

(7) Those provisions are—

(a) section 119;

(b) section ~~170~~166;

(c) section ~~171~~167;

(d) section ~~173~~169;

(e) paragraph ~~15~~15 of Schedule 15.

206 Application to Parliament

(1) Parts 1, 2 and 5 to 7 of this Act apply to the processing of personal data by or on behalf of either House of Parliament.

(2) Where the purposes for which and the manner in which personal data is, or is to be, processed are determined by or on behalf of the House of Commons, the controller in respect of that data for the purposes of the GDPR and this Act is the Corporate Officer of that House.

(3) Where the purposes for which and the manner in which personal data is, or is to be, processed are determined by or on behalf of the House of Lords, the controller in respect of that data for the purposes of the GDPR and this Act is the Corporate Officer of that House.

(4) Subsections (2) and (3) do not apply where the purposes for which and the manner in which the personal data is, or is to be, processed are determined by or on behalf of the Intelligence and Security Committee of Parliament.

(5) As regards criminal liability—

(a) nothing in subsection (2) or (3) makes the Corporate Officer of the House of Commons or the Corporate Officer of the House of Lords liable to prosecution under this Act;

(b) a person acting on behalf of either House of Parliament is liable to prosecution under the provisions of this Act listed in subsection (6).

(6) Those provisions are—

(a) section ~~170~~166;

(b) section ~~171~~167;

(c) section ~~173~~169;

(d) paragraph ~~15~~15 of Schedule 15.

207 Minor and consequential ~~amendments~~provision

(1) ~~Schedule 18 contains minor and consequential amendments.~~

(1) In Schedule 18—

(a) Part 1 contains minor and consequential amendments of primary legislation;

(b) Part 2 contains minor and consequential amendments of other legislation;
(c) Part 3 contains consequential modifications of legislation;
(d) Part 4 contains supplementary provision.

(2) The Secretary of State may by regulations make provision that is consequential on any provision made by this Act.

(3) Regulations under subsection (2)—
(a) may include transitional, transitory or saving provision;
(b) may amend, repeal or revoke an enactment.

(4) The reference to an enactment in subsection (3)(b) does not include an enactment passed or made after the end of the Session in which this Act is passed.

(5) Regulations under this section that amend, repeal or revoke primary legislation are subject to the affirmative resolution procedure.

(6) Any other regulations under this section are subject to the negative resolution procedure.

(7) In this section, "primary legislation" means—
(a) an Act;
(b) an Act of the Scottish Parliament;
(c) a Measure or Act of the National Assembly for Wales;
(d) Northern Ireland legislation.

Final

208 Commencement

(1) Except as provided by subsection (2), this Act comes into force on such day as the Secretary of State may by regulations appoint.

(2) This section and the following provisions come into force on the day on which this Act is passed—
(a) sections 1 and 3;
(b) ~~sections 168 and 169;~~
(c) section ~~179~~175;
(d) sections ~~197~~195, ~~198~~ 196 and ~~199~~197;
(e) sections ~~202~~ 200 and ~~203~~201;
(f) this section and sections ~~206~~204, ~~207~~ 205 and ~~208~~206;
(g) any other provision of this Act so far as it confers power to make regulations or Tribunal Procedure Rules or is otherwise necessary for enabling the exercise of such a power on or after the day on which this Act is passed.

(3) Regulations under this section may make different provision for different areas.

209 Transitional provision

The Secretary of State may by regulations make transitional, transitory or saving provision in connection with the coming into force of any provision of this Act.

210 Extent

(1) This Act extends to England and Wales, Scotland and Northern Ireland, subject to—

(a) subsections (2) ~~and (3)~~to (5), and

(b) paragraph ~~12~~12 of Schedule 12.

(2) Section 190 extends to England and Wales only.

(3) ~~Section 192 extends~~ Sections 181 and 182 extend to England and Wales and Northern Ireland only.

(4) An amendment, repeal or revocation made by this Act has the same extent in the United Kingdom as the enactment amended, repealed or ~~revoked (ignoring extent by virtue of an Order in Council)~~revoked.

(5) This subsection and the following provisions also extend to the Isle of Man—

(a) paragraphs 313 and 409 of Schedule 18;

(b) sections 202(1), 203(1) and 204, so far as relating to those paragraphs.

(6) Where there is a power to extend a part of an Act by Order in Council to any of the Channel Islands, the Isle of Man or any of the British overseas territories, the power may be exercised in relation to an amendment or repeal of that part which is made by or under this Act.

211 Short title

This Act may be cited as the Data Protection Act 2018.

~~(1) Nothing in this Act shall impose any charge on the people or on public funds, or vary the amount or incidence of or otherwise alter any such charge in any manner, or affect the assessment, levying, administration or application of any money raised by any such charge.~~