Key	
Purple additions	Changes in No.1 Bill that remain
Green additions	New changes in No.2 Bill
Teal references	Reference to affected provision in No.2 Bill as first published

Note – some provisions of the Government Bill amend provisions that are later omitted. In these circumstances, we have not shown the amendments subsequently omitted.

Data Protection Act 2018

2018 CHAPTER 12

An Act 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.

23rd May 2018

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 1PRELIMINARY

1. Overview

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

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

(3) Part 2 supplements the UK GDPR.

(4) Part 3 makes provision about the processing of personal data by competent authorities for law enforcement purposes

(5) Part 4 makes provision about the processing of personal data by the intelligence services (and certain processing carried out by competent authorities jointly with the intelligence services).

[s. 26(2)]

(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 UK 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 UK 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~~. [s. 27(2)]

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.

(and see section 3A for provision about when information relates to an identifiable living individual). [s. 1(1)(a)]

(3A) An individual is identifiable from information "directly" if the individual can be identified without the use of additional information.

(3B) An individual is identifiable from information "indirectly" if the individual can be identified only with the use of additional information. [s. 1(1)(b)]

(4) "Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of 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 Part 2, Part 3 or Part 4 applies, have the same meaning as in that Part (see sections 5, 6, 32 and 83 and see also subsection (14)(d)).

(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).~~ [s. 101(3)]

(8A) The Commission" means the Information Commission (see section 114A). [s. 100(3)]

(9) "The data protection legislation" means—

(a) the UK GDPR,

(b) …..

(c) this Act, and [sch 9. para 13(a)]

(d) regulations made under this Act or the UK GDPR, ~~and~~ [s. 44(2)]

(e) ~~regulations made under section 2(2) of the European Communities Act 1972 which relate to the EU GDPR or the Law Enforcement Directive.~~

[sch 9. para.13(b)]

(10) "The UK 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 (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and see section 205(4)).

(10A) "The EU GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th 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) as it has effect in EU law.

(11) . . . . . .

(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 UK GDPR are to the UK GDPR read with Part 2;

(b) . . . . . .

(c) references to personal data, and the processing of personal data, are to personal data and processing to which Part 2, Part 3 or Part 4 applies;

(d) references to a controller or processor are to a controller or processor in relation to the processing of personal data to which Part 2, Part 3 or Part 4 applies.

(15) There is an index of defined expressions in section 206.

3A Information relating to an identifiable living individual

(1) For the purposes of this Act, information being processed is information relating to an identifiable living individual only in cases described in subsections (2) and (3).

(2) The first case is where the living individual is identifiable (as described in section 3(3)) by the controller or processor by reasonable means at the time of the processing.

(3) The second case is where the controller or processor knows, or ought reasonably to know, that—

(a) another person will, or is likely to, obtain the information as a result of the processing, and

(b) the living individual will be, or is likely to be, identifiable (as described in section 3(3)) by that person by reasonable means at the time of the processing.

(4) The reference in subsection (3)(a) to obtaining the information as a result of the processing includes obtaining the information as a result of the controller or processor carrying out the processing without implementing appropriate technical and organisational measures to mitigate the risk of the information being obtained by persons with whom the controller or processor does not intend to share the information.

(5) For the purposes of this section, an individual is identifiable by a person "by reasonable means" if the individual is identifiable by the person by any means that the person is reasonably likely to use.

(6) For the purposes of subsection (5), whether a person is reasonably likely to use a means of identifying an individual is to be determined taking into account, among other things—

(a) the time, effort and costs involved in identifying the individual by that means, and

(b) the technology and other resources available to the person. [s. 1(2)]

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) This Part—

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

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

(3) . . . . . .

5. Definitions

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

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

(3) Subsection (1) is subject to any provision in this Part which provides expressly for the term to have a different meaning and to section 204.

(4) . . . . . .

(5) . . . . . .

(6) . . . . . .

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

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

CHAPTER 2 THE UK GDPR

Meaning of certain terms used in the UK GDPR

6. Meaning of "controller"

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

(a) subsection (2),

(b) section 209, and

(c) section 210. [s. 1(4)]

(2) For the purposes of the UK 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 UK GDPR, the following (and only the following) are "public authorities" and "public bodies" —

(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 body specified or described by the Secretary of State in regulations,

subject to subsections (2), (3) and (4).

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

(3) The references in subsection (1)(a) and (b) to public authorities and Scottish public authorities as defined by the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 (asp 13) do not include any of the following that fall within those definitions—

(a) a parish council in England;

(b) a community council in Wales;

(c) a community council in Scotland;

(d) a parish meeting constituted under section 13 of the Local Government Act 1972;

(e) a community meeting constituted under section 27 of that Act;

(f) charter trustees constituted—

(i) under section 246 of that Act,

(ii) under Part 1 of the Local Government and Public Involvement in Health Act 2007, or

(iii) by the Charter Trustees Regulations 1996 (S.I. 1996/263).

(4) 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 UK GDPR.

(5) 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 UK 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~~. [s. 5(7)]

9. Child's consent in relation to information society 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 UK 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 UK 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 of Schedule 1.

(3) The processing meets the requirement in point (g) of Article 9(2) of the UK 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 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(1) of the UK 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, 2 or 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 UK 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 UK 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 UK 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)~~ 12A of the UK GDPR (reasonable fees when responding to ~~manifestly unfounded~~ vexatious or excessive requests), or [s. 7(5)]

(b) Article 15(3) of the UK 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 UK 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 UK 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 UK GDPR (exception from Article 22(1) of the UK GDPR for significant decisions based solely on automated processing that are required or authorised under the law of the United Kingdom or a part of the United Kingdom 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 UK 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 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, within the period described in Article 12(3) of the UK 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 UK 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 UK 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.~~ [sch. 3 para. 12]

Exemptions etc

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 UK GDPR.

(2) In Schedule 2—

(a) Part 1 makes provision adapting or restricting the application of rules contained in Articles 13 to 21 and 34 of the UK GDPR in specified circumstances (of a kind described in Article 6(3) and Article 23(1) of the UK GDPR;

(b) Part 2 makes provision restricting the application of rules contained in Articles 13 to 21 and 34 of the UK GDPR in specified circumstances (of a kind described in Article 23(1) of the UK GDPR;

(c) Part 3 makes provision restricting the application of Article 15 of the UK GDPR where this is necessary to protect the rights of others (of a kind described in Article 23(1) of the UK GDPR);

(d) Part 4 makes provision restricting the application of rules contained in Articles 13 to 15 of the UK GDPR in specified circumstances (of a kind described in Article 23(1) of the UK GDPR);

(e) Part 5 makes provision containing exemptions or derogations from Chapters II, III, IV and V of the UK GDPR for reasons relating to freedom of expression (of a kind described in Article 85(2) of the UK GDPR);

(f) Part 6 makes provision containing derogations from rights contained in Articles 15, 16, 18, 19, 20 and 21 of the UK GDPR for scientific or historical research purposes, statistical purposes and archiving purposes

(3) Schedule 3 makes provision restricting the application of rules contained in Articles 13 to 21 of the UK GDPR to health, social work, education and child abuse data (of a kind described in Article 23(1) of the UK GDPR).

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

(4A)In connection with the manual unstructured processing of personal data held by an FOI public authority, see Chapter 3 of this Part (sections 21, 24 and 25).

(5) In connection with the safeguarding of national security and with defence, see Chapter 3 of this Part (sections 26 to 28).

16. Power to make further exemptions etc by regulations

(1) The following powers to make provision altering the application of the UK GDPR may be exercised by way of regulations made by the Secretary of State under this section—

(a) the power in Article 6(3) to lay down a legal basis containing specific provisions to adapt the application of rules of the UK 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 provision 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 UK 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,

(b) consequentially amend section 15, and

(c) consequentially amend the UK GDPR by adding, varying or omitting a reference to section 15, Schedule 2, 3 or 4, this section or regulations under this section.

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

Certification

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 UK 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 UK 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 UK 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 UK GDPR.

(7) The UK national accreditation body must provide the Secretary of State with such information relating to its functions under this section, Schedule 5 and Article 43 of the UK 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 UK GDPR;

"the UK national accreditation body" means the UK 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*~~

~~**17ATransfers based on adequacy regulations**~~

(1) The Secretary of State may by regulations specify any of the following which the Secretary of State considers ensures an adequate level of protection of personal data—

(a) a third country,

(b) a territory or one or more sectors within a third country,

(c) an international organisation, or

(d) a description of such a country, territory, sector or organisation.

(2) For the purposes of the UK GDPR and this Part of this Act, a transfer of personal data to a third country or an international organisation is based on adequacy regulations if, at the time of the transfer, regulations made under this section are in force which specify, or specify a description which includes—

(a) in the case of a third country, the country or a relevant territory or sector within the country, or

(b) in the case of an international organisation, the organisation.

(3) Regulations under this section may specify that the Secretary of State considers that an adequate level of protection of personal data is ensured only for a transfer specified or described in the regulations and, if they do so, only such a transfer may rely on those regulations for the purposes of subsection (2).

(4) Article 45(2) of the UK GDPR makes provision about the assessment of the adequacy of the level of protection for the purposes of this section and section 17B.

(5) Regulations under this section—

(a) where they relate to a third country, must specify their territorial and sectoral application;

(b) where applicable, must specify the independent supervisory authority or authorities referred to in Article 45(2)(b) of the UK GDPR.

(6) Regulations under this section may, among other things—

(a) provide that in relation to a country, territory, sector, organisation or transfer specified, or falling within a description specified, in the regulations, section 17B(1) has effect as if it required the reviews described there to be carried out at such shorter intervals as are specified in the regulations;

(b) identify a transfer of personal data by any means, including by reference to the controller or processor, the recipient, the personal data transferred or the means by which the transfer is made or by reference to relevant legislation, lists or other documents, as they have effect from time to time;

(c) confer a discretion on a person.

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

[sch. 7 para 11]

17BTransfers based on adequacy regulations: review etc

(1) For so long as regulations under section 17A are in force which specify, or specify a description which includes, a third country, a territory or sector within a third country or an international organisation, the Secretary of State must carry out a review of whether the country, territory, sector or organisation ensures an adequate level of protection of personal data at intervals of not more than 4 years.

(2) Each review under subsection (1) must take into account all relevant developments in the third country or international organisation.

(3) The Secretary of State must, on an ongoing basis, monitor developments in third countries and international organisations that could affect decisions to make regulations under section 17A or to amend or revoke such regulations.

(4) Where the Secretary of State becomes aware that a country, territory, sector or organisation specified, or falling within a description specified, in regulations under section 17A no longer ensures an adequate level of protection of personal data, whether as a result of a review under this section or otherwise, the Secretary of State must, to the extent necessary, amend or revoke the regulations.

(5) Where regulations under section 17A are amended or revoked in accordance with subsection (4), the Secretary of State must enter into consultations with the third country or international organisation concerned with a view to remedying the lack of an adequate level of protection.

(6) The Secretary of State must publish—

(a) a list of the third countries, territories and specified sectors within a third country and international organisations, and the descriptions of such countries, territories, sectors and organisations, which are for the time being specified in regulations under section 17A, and

(b) a list of the third countries, territories and specified sectors within a third country and international organisations, and the descriptions of such countries, territories, sectors and organisations, which have been but are no longer specified in such regulations.

(7) In the case of regulations under section 17A which specify that an adequate level of protection of personal data is ensured only for a transfer specified or described in the regulations—

(a) the duty under subsection (1) is only to carry out a review of the level of protection ensured for such a transfer, and

(b) the lists published under subsection (6) must specify or describe the relevant transfers. [sch. 7 para 12]

17CStandard data protection clauses

(1) The Secretary of State may by regulations specify standard data protection clauses which the Secretary of State considers provide appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Article 46 of the UK GDPR (and see also section 119A).

~~(2) The Secretary of State must keep under review the standard data protection clauses specified in regulations under this section that are for the time being in force.~~

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

[sch. 7 para 13]

18. ~~Transfers of personal data to third countries etc: public interest~~

(1) ~~The Secretary of State may by regulations specify, for the purposes of Article 49(1)(d) of the UK 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 cannot take place based on adequacy regulations (see section 17A), 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.~~

[sch. 7 para 14]

~~*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 **F101**UK 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, (e) any of the health and social care bodies in Northern Ireland falling within paragraphs (to (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.~~

[s. 22(6)]

Minor definition

20. ~~Meaning of "court"~~

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

[sch 9. para 14]

CHAPTER 3 EXEMPTIONS FOR MANUAL UNSTRUCTURED PROCESSING AND FOR NATIONAL SECURITY AND DEFENCE PURPOSES

Definitions

21. Definitions

(1) . . . . . .

(2) . . . . . .

(3) . . . . . .

(4) . . . . . .

(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.

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

. . . . . .

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

. . . . . .

Exemptions etc

24. Manual unstructured data held by FOI public authorities

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

(2) Those provisions are—

(a) in Chapter II of the UK 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 UK 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 UK GDPR, Articles 44A to 49A (transfers of personal data to third countries or international organisations);

~~(ca)in Part 2 of this Act, sections 17A, 17B and 17C (transfers to third countries);~~

[sch. 7 para 15]

(cb)in Part 5 of this Act, section 119A (standard clauses for transfers to third countries);

(d) in Part 7 of this Act, sections 170 and 171 (offences relating to personal data).

(see also paragraph 1(2) of Schedule 18).

(3) In addition, the provisions of the UK GDPR listed in subsection (4) do not apply to personal data to which the UK GDPR applies by virtue of Article 2(1A) 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);

(ba) Chapter 8A (safeguards for processing for research, archiving or statistical purposes); [s. 23(2)(a)]

(c) Chapter IX (specific processing situations).

(5) A controller is not obliged to comply with Article 15(1) to (3) of the UK GDPR (right of access by the data subject) in relation to personal data to which the UK GDPR applies by virtue of Article 2(1A) if—

(a) the request under Article 15 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 UK GDPR listed in subsection (2) do not apply to personal data to which the UK GDPR applies by virtue of Article 2(1A) (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 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 (principles), Article 5(1)(d) (the accuracy principle), and

(b) in Chapter III (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 UK GDPR or this Act mentioned in subsection (2) does not apply to personal data to which the UK GDPR 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 UK 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 UK GDPR (rights of data subjects);

(c) In Chapter IV of the UK 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 UK GDPR (transfers of personal data to third countries or international organisations);

(e) in Chapter VI of the UK GDPR—

(i) Article 57(1)(a) and (h) (Commissioner's duties to monitor and enforce he UK GDPR and to conduct investigations);

(ii) Article 58 (investigative, corrective, authorisation and advisory powers of Commissioner);

(f) Chapter VIII of the UK GDPR (remedies, liabilities and penalties) except for—

(i) Article 83 (general conditions for imposing administrative fines);

(ii) Article 84 (penalties);

~~(fa)in Part 2 of this Act, sections 17A, 17B and 17C (transfers to third countries);~~

[sch. 7 para 16]

(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 UK GDPR;

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

(iv) section 119A (standard clauses for transfers to third countries);

(h) in Part 6 of this Act—

(i) sections 142 to 154 and Schedule 15 (Commissioner's notices and powers of entry and inspection);

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

(i) in Part 7 of this Act, section 187 (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 UK 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 UK GDPR

(1) Article 9(1) of the UK GDPR (prohibition on processing of special categories of personal data) does not prohibit the processing of personal data to which the UK GDPR 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 UK 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 the UK GDPR applies for—

(a) the purpose of safeguarding national security, or

(b) defence purposes.

(3) Where Article 32 of the UK 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.

(5) The functions conferred on the Commissioner in relation to the UK GDPR by Articles 57(1)(a), (d), (e), (h) and (u) and 58(1)(d) and (2)(a) to (d) of the UK GDPR (which are subject to safeguards set out in section 115) include functions in relation to subsection (3).

PART 3LAW ENFORCEMENT PROCESSING

CHAPTER 1SCOPE 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.

(1A) This Part does not apply to processing to which Part 4 applies by virtue of a designation notice (see section 82A). [s. 26(3)]

(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 or remove a person or description of person;

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

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

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

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

(7) In this section—

"intelligence service" means—

(a) the Security Service;
(b) the Secret Intelligence Service;
(c) the Government Communications Headquarters;

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

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.

(1A) "Consent" of the data subject to the processing of personal data means a freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data (and see section 40A). [s. 4(2)]

(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.

(6A) "Senior responsible individual" means an individual designated as the senior responsible individual of a controller or processor under section 58A. [sch. 4 para 12]

(7) "Third country" means a country or territory outside the United Kingdom.

(8) Sections 3 and 205 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,

(aa) section 40A makes provision about processing carried out in reliance on the consent of the data subject, and [s. 4(3)]

(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~~ (whether from the data subject or otherwise) must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed by or on behalf of a controller in a manner that is incompatible with the purpose for which the controller collected it ~~it was collected~~. [s. 6(8)]

(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).

40A Conditions for consent

(1) This section is about processing of personal data that is carried out in reliance on the consent of the data subject.

(2) The controller must be able to demonstrate that the data subject consented to the processing.

(3) If the data subject's consent is given in writing as part of a document which also concerns other matters, the request for consent must be made—

(a) in a manner which clearly distinguishes the request from the other matters,

(b) in an intelligible and easily accessible form, and

(c) in clear and plain language.

(4) Any part of a document described in subsection (3) which constitutes an infringement of this Part is not binding.

(5) The data subject may withdraw the consent at any time (but the withdrawal of consent does not affect the lawfulness of processing in reliance on the consent before its withdrawal).

(6) Processing may only be carried out in reliance on consent if—

(a) before the consent is given, the controller or processor informs the data subject of the right to withdraw it, and

(b) it is as easy for the data subject to withdraw the consent as to give it.

(7) When assessing whether consent is freely given, account must be taken of, among other things, whether the provision of a service is conditional on consent to the processing of personal data that is not necessary for the provision of that service. [s. 4(4)]

41. Safeguards: archiving

(1) This section applies in relation to the processing of personal data for a law enforcement purpose where the processing is carried out ~~necessary~~— [s. 22(7)]

(a) for archiving purposes in the public interest,

(b) for scientific or historical research purposes, or

(c) for statistical purposes.

(2) The processing is not permitted if—

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

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

42. Safeguards: sensitive processing

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

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

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

(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may

be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained.

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

(a) retain the appropriate policy document,

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

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

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

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

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

(c) ~~whether the personal data is retained and erased in accordance with the policies described in subsection (2)(b) and, if it is not, the reasons for not following those policies.~~ [s. 15(6)]

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

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

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

CHAPTER 3 RIGHTS OF THE DATA SUBJECT

Overview and scope

43. Overview and scope

(1) This Chapter—

(a) imposes general duties on the controller to make information available (see sections 44 and 45A);

(b) confers a right of access by the data subject (see sections 45 and 45A); [s. 10(2)]

(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~~ 50A to 50D) [sch. 3 para 13]

(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*~~ *Data subject's rights to information* [s. 10(3)]

44. ~~Information:~~ C~~c~~ontroller's general duties [s. 10(3)]

(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~~ senior responsible individual (see sections 69 to 71); [sch. 4 para 13]

(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);

(da) the existence of the right to make a complaint to the controller (see section 164A);

(e) the existence of the right to lodge a complaint with the Commissioner (see section 165) and the contact details of the Commissioner. [sch. 8 para 12(2)]

(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;~~ [s. 24(3)(a)]

(e) protect the rights and freedoms of others.

(5) Where the provision of information to a data subject under subsection (2) is restricted under subsection (4) wholly or partly, the controller must inform the data subject in writing without undue delay— [s. 24(3)(b)],

(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,

(ca) of the data subject's right to make a complaint to the controller under section 164A,

(d) of the data subject's right to lodge a complaint with the Commissioner under section 165, and [sch. 8 para 12(3)]

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

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

(7) The controller must—

(a) record the reasons for a decision to restrict (whether wholly or partly) the provision of information to a data subject under subsection (2) in reliance on subsection (4), and

[s. 24(3)(c)]

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

~~*Data subject's right of access*~~ [s. 10(5)]

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);

(ea) the existence of the data subject's right to make a complaint to the controller (see section 164A);

(f) the existence of the data subject's right to lodge a complaint with the Commissioner (see section 165) and the contact details of the Commissioner;

[sch. 8 para 13(2)]

(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;~~ [s. 24(4)(a)]

(e) protect the rights and freedoms of others.

(5) Where the rights of a data subject under subsection (1) are restricted under subsection (4) wholly or partly, the controller must inform the data subject in writing without undue delay and in any event before the end of the applicable time period (as to which see section 54).—

[[s. 24(4)(b) and s. 8(5)]

(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,

(ca) of the data subject's right to make a complaint to the controller under section 164A,

(d) of the data subject's right to lodge a complaint with the Commissioner under section 165, and [sch. 8 para 13(3)]

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

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

(7) The controller must—

(a) record the reasons for a decision to restrict (whether wholly or partly) the rights of a data subject under subsection (1) in reliance on subsection (4), and

(b) if requested to do so by the Commissioner, make the record available to the Commissioner. [s. 24(4)(c)]

45A Exemption from sections 44 and 45: legal professional privilege

(1) Sections 44(2) and 45(1) do not require the controller to give the data subject—

(a) information in respect of which a claim to legal professional privilege or, in Scotland, confidentiality of communications could be maintained in legal proceedings, or

(b) information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser.

(2) A controller relying on the exemption in subsection (1) must inform the data subject in writing without undue delay of—

(a) the decision to rely on the exemption,

(b) the reason for the decision,

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

(ca) the data subject's right to make a complaint to the controller under section 164A

[s.10(6) and sch. 8 para 14]

(d) the data subject's right to lodge a complaint with the Commissioner under section 165, and

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

(3) Subsection (2)(a) and (b) do not apply to the extent that complying with them would—

(a) undermine a claim described in subsection (1)(a), or

(b) conflict with a duty described in subsection (1)(b).

(4) The controller must—

(a) record the reason for a decision to rely on the exemption in subsection (1), and

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

(5) The reference in subsection (1) to sections 44(2) and 45(1) includes sections 35 to 40 so far as their provisions correspond to the rights and obligations provided for in sections 44(2) and 45(1).

[s. 10(6)]

Data subject's rights to rectification or erasure etc

46. Right to rectification

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

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

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

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

47. Right to erasure or restriction of processing

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

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

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

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

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

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

48. Rights under section 46 or 47: supplementary

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

(a) whether the request has been granted, and

(b) if it has been refused—

(i) of the reasons for the refusal,

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

(iia) of the data subject's right to make a complaint to the controller under section 164A,

(iii) of the data subject's right to lodge a complaint with the Commissioner under section 165, and [sch. 8 para 15(2)]

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

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

(a) without undue delay, and

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

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

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

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

(c) protect public security;

(d) ~~protect national security;~~ [s. 24(5)(a)]

(e) protect the rights and freedoms of others.

(4) Where the rights of a data subject under subsection (1)(b)(i) are restricted under subsection (3), wholly or partly, the controller must inform the data subject in writing without undue delay— [s. 24(5)(b)]

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

(b) of the reasons for the restriction,

(ba) of the data subject's right to make a complaint to the controller under section 164A,

(i) of the data subject's right to lodge a complaint with the Commissioner under section 165, and [sch. 8 para 15(3)]

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

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

(6) The controller must—

(a) record the reasons for a decision to restrict (whether wholly or partly) the provision of information to a data subject under subsection (1)(b)(i) in reliance on subsection (3), and

[s. 24(5)(c)]

(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) . . . . . .

(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.~~

[s.11(3)]

~~50. Automated decision-making authorised by law: safeguards~~

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

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

(b) ~~it is required or authorised by law.~~

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

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

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

~~(i) reconsider the decision, or~~

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

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

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

(b) ~~comply with the request, and~~

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

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

~~(ii) the outcome of complying with the request.~~

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

(5) ~~Regulations under subsection (4)—~~

(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).~~ [s.11(3)]

50A Automated processing and significant decisions

(1) For the purposes of sections 50B and 50C—

(a) a decision is based solely on automated processing if there is no meaningful human involvement in the taking of the decision, and

(b) a decision is a significant decision, in relation to a data subject, if—

(i) it produces an adverse legal effect for the data subject, or

(ii) it has a similarly significant adverse effect for the data subject.

(2) When considering whether there is meaningful human involvement in the taking of a decision, a person must consider, among other things, the extent to which the decision is reached by means of profiling. [s. 11(3)]

50B Restrictions on automated decision-making using sensitive personal data

(1) A significant decision based entirely or partly on sensitive personal data may not be taken based solely on automated processing, unless one of the following conditions is met.

(2) The first condition is that the decision is based entirely on processing of personal data to which the data subject has given explicit consent.

(3) The second condition is that the decision is required or authorised by law. [s. 11(3)]

50C Safeguards for automated decision-making

(1) Subject to subsection (3), where a significant decision taken by or on behalf of a controller in relation to a data subject is—

(a) based entirely or partly on personal data, and

(b) based solely on automated processing,

the controller must ensure that safeguards for the data subject's rights, freedoms and legitimate interests are in place which comply with subsection (2) and any regulations under section 50D(3).

(2) The safeguards must consist of or include measures which—

(a) provide the data subject with information about decisions described in subsection (1) taken in relation to the data subject;

(b) enable the data subject to make representations about such decisions;

(c) enable the data subject to obtain human intervention on the part of the controller in relation to such decisions;

(d) enable the data subject to contest such decisions.

(3) Subsections (1) and (2) do not apply in relation to a significant decision if—

(a) exemption from those provisions is required for a reason listed in subsection (4),

(b) the controller reconsiders the decision, as soon as reasonably practicable, and

(c) there is meaningful human involvement in the reconsideration of the decision.

(4) Those reasons are—

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

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

(c) to protect public security;

(d) to safeguard national security;

(e) to protect the rights and freedoms of others.

(5) When considering whether there is meaningful human involvement in the reconsideration of a decision, a person must consider, among other things, the extent to which the conclusion reached on reconsideration is reached by means of profiling. [s. 11(3)]

50D Further provision about automated decision-making

(1) The Secretary of State may by regulations provide that, for the purposes of sections 50A(1)(a) and 50C(3)(c), there is, or is not, to be taken to be meaningful human involvement in the taking or reconsideration of a decision in cases described in the regulations.

(2) The Secretary of State may by regulations provide that, for the purposes of section 50A(1)(b)(ii), a description of decision is, or is not, to be taken to have a similarly significant adverse effect for the data subject.

(3) Regulations under subsection (1) or (2) may amend section 50A.

(4) The Secretary of State may by regulations make further provision about the safeguards required under section 50C(1), including provision about what is, or is not, to be taken to satisfy a requirement under section 50C(1) or (2).

(5) Regulations under subsection (4) may amend section 50C—

(a) by adding or varying safeguards, and

(b) by omitting provision added by regulations under that subsection.

(6) Regulations under this section are subject to the affirmative resolution procedure. [s. 11(3)]

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 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),

(ba) relies on the exemption from sections 44(2) and 45(1) in section 45A (legal professional privilege), or [s. 10(7)(a)]

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

(2) The data subject may—

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

(aa) where subsection (1)(ba) applies, request the Commissioner to check that the controller was entitled to rely on the exemption; [s. 10(7)(b)]

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

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

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

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

(aa) where subsection (1)(ba) applies, whether the Commissioner is satisfied that the controller was entitled to rely on the exemption; [s. 10(7)(c)]

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

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

(6) Where the Commissioner is not satisfied as mentioned in subsection (4)(a), (aa) or (b), the Commissioner may also inform the data subject of any further steps that the Commissioner is considering taking under Part 6 . [s. 10(7)(d)]

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, or 47 ~~or 50~~, the controller must provide the information in the same form as the request where it is practicable to do so. [sch. 3 para 14(2)]

(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 50D. [sch. 3 para 14(3)]

53. ~~Manifestly unfounded~~ Vexatious or excessive requests by the data subject

(A1) Subsection (1) applies where a request made by a data subject under or by virtue of any of sections 45, 46, 47, 50C or 50D is vexatious or excessive (see section 204A).

[s. 7(6) and sch. 3 para 15(2)]

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

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

(b) refuse to act on the request.

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

(3) In any proceedings where there is an issue as to whether a request ~~under section 45, 46, 47 or 50~~ described in subsection (A1) is ~~manifestly unfounded~~ vexatious or excessive, it is for the controller to show that it is. [s. 7(6) and sch. 3 para 15(3)]

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

(4A) 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 accordance with subsection (1)(a), and

(b) specify what the guidance must include.

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

(6) If, in reliance on subsection (1)(b), the controller does not take action on the request, the controller must inform the data subject of—

(a) the reasons for not doing so, and

(b) the data subject's right to lodge a complaint with the Commissioner

(7) The controller must comply with subsection (6)—

(a) without undue delay, and

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

[s. 7(6)]

54. Meaning of "applicable time period"

(1) This section defines "the applicable time period" for the purposes of sections 45(3)(b) and 5, ~~and~~ 48(2)(b) and 53(7). [s. 8(6)(a)] and s. 7(7)]

(2) "The applicable time period" means the period of one month ~~1 month, or such longer period as may be specified in regulations~~, beginning with the relevant time, subject to subsection (3A)

[s. 8(6)(b)]

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

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

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

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

(3A) The controller may, by giving notice to the data subject, extend the applicable time period by two further months where that is necessary by reason of—

(a) the complexity of requests made by the data subject, or

(b) the number of such requests.

(3B) A notice under subsection (3A) must—

(a) be given before the end of the period of one month beginning with the relevant time, and

(b) state the reasons for the delay.

(3C) Where the controller reasonably requires further information in order to identify the information or processing activities to which a request under section 45(1) relates—

(a) the controller may ask the data subject to provide the further information, and

(b) the period beginning with the day on which the controller makes the request and ending with the day on which the controller receives the information does not count towards—

(i) the applicable time period, or

(ii) the period described in subsection (3B)(a).

(3D) An example of a case in which a controller may reasonably require further information is where the controller processes a large amount of information concerning the data subject.

[s. 8(6)(c)]

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

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

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

[s. 8(6)(d)]

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 58 ~~65~~); [sch. 4 para. 14(a)]

(aa) makes provision for the designation, tasks and position of senior responsible individuals (see sections 58A to 58C);

(ab) makes provision about processors (see section 59) and processing under the authority of the controller or processor (see section 60);

(ac) makes provision about records (see sections 61A and 62) and co-operation with the Commissioner (see section 63);

(ad) makes provision about risk assessment (see section 64) and prior consultation with the Commissioner (see section 65) [sch. 4 para 14(b)]

(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)~~. [sch. 4 para 14(c)]

(e) makes provision about codes of conduct (see section 68A). [s. 19(2)]

(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— [s. 12(6)]

(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 measures, including 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. [s. 12(7)(a)]

(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. [s. 12(7)(b)]

(4) Adherence to a code of conduct approved under section 68A may be used by a controller as a means of demonstrating compliance with the requirements of this Part. [s. 19(3)]

57. Data protection by design and default

(1) Each controller must implement appropriate measures, including technical and organisational measures, which are designed— [s. 12(8)(a)]

(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 measures, including technical and organisational measures, for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed. [s. 12(8)(b)]

(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.

Senior responsible individual [s. 14(5)]

58A Designation of senior responsible individual

(1) This section and sections 58B and 58C apply to all controllers and processors other than a court, or other judicial authority, acting in its judicial capacity.

(2) The controller or processor must designate one individual to be its senior responsible individual.

(3) Where the controller or processor is an organisation—

(a) a designated individual must be part of the organisation's senior management, and

(b) the controller or processor may designate two or more individuals to act jointly as its senior responsible individual where the individuals are employed part-time and share a single role within the organisation's senior management.

(4) The controller or processor must—

(a) ensure that the current contact details of the senior responsible individual are publicly available, and

(b) send those details to the Commissioner.

(5) In this section, "senior management", in relation to an organisation, means the individuals who play significant roles in the making of decisions about how the whole or a substantial part of its activities are to be managed or organised. [s. 14(5)]

58B Tasks of the senior responsible individual

(1) The senior responsible individual designated by a controller must be responsible at least for performing the tasks listed in subsection (2) or securing that they are performed by another person.

(2) Those tasks are—

(a) monitoring compliance by the controller with the data protection legislation;

(b) ensuring that the controller develops, implements, reviews and updates measures to ensure its compliance with the data protection legislation;

(c) informing and advising the controller, any processor engaged by the controller and employees of the controller who carry out processing of personal data of their obligations under the data protection legislation;

(d) organising training for employees of the controller who carry out processing of personal data;

(e) dealing with complaints made to the controller in connection with the processing of personal data;

(f) dealing with personal data breaches;

(g) co-operating with the Commissioner on behalf of the controller;

(h) acting as the contact point for the Commissioner on issues relating to processing of personal data.

(3) The senior responsible individual designated by a processor must be responsible at least for performing the tasks listed in subsection (4) or securing that they are performed by another person.

(4) Those tasks are—

(a) monitoring compliance by the processor with sections 59, 61A and 66;

(b) co-operating with the Commissioner on behalf of the processor;

(c) acting as the contact point for the Commissioner on issues relating to processing of personal data.

(5) Where the performance of one of its tasks would result in a conflict of interests, the senior responsible individual must secure that the task is performed by another person.

(6) In deciding whether one or more of their tasks should be performed by another person (whether alone or jointly with others), and, if so, by whom, the senior responsible individual must consider, among other things—

(a) the other person's professional qualifications and knowledge of the data protection legislation,

(b) the resources likely to be available to the other person to carry out the task, and

(c) whether the other person is involved in day-to-day processing of personal data for the controller or processor and, if so, whether that affects the person's ability to perform the task. [s. 14(5)]

58C Senior responsible individual's position

(1) A controller or processor must support its senior responsible individual in the performance of the individual's tasks, including by providing the individual with appropriate resources.

(2) A controller or processor must not dismiss or penalise its senior responsible individual for performing the individual's tasks.

(3) Where its senior responsible individual decides that one or more of its tasks should be performed by another person, the controller or processor must ensure that the person—

(a) has appropriate resources to perform the task,

(b) is not dismissed or penalised by the controller or processor for performing the task, and

(c) does not receive instructions about the performance of the task.

(4) Subsection (3)(c) does not require the controller or processor to prevent instructions being given by the senior responsible individual or another person performing a task for the senior responsible individual, except where such instructions would involve a conflict of interests.

Processor etc [s. 14(5)]

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 measures, including technical and organisational measures, that are sufficient to secure that the processing will— [s. 12(9)]

(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.

(7A) Adherence to a code of conduct approved under section 68A may be used by a processor as a means of demonstrating sufficient guarantees as described in subsection (2).

[s. 19(4)]

(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.

Records and co-operation with the Commissioner [s. 15(7)]

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 controllers 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.~~ [s. 15(8)]

61A Records of processing of personal data

(1) Each controller must maintain appropriate records of processing of personal data carried out by or on behalf of the controller.

(2) The controller's records must include at least the following information about the personal data in respect of which the controller is for the time being a controller—

(a) where the personal data is (including information about any personal data that is outside the United Kingdom),

(b) the purposes for which the controller is processing the personal data,

(c) the categories of person with whom the controller has shared, or intends to share, the personal data with (including persons who are in third countries or international organisations),

(d) how long the controller intends to retain the personal data, and

(e) whether the personal data includes personal data described in section 35(8) and, if so, which types of such data.

(3) Where possible, the controller's records must include information about how it ensures that personal data is secure.

(4) Each processor must maintain appropriate records of its processing of personal data.

(5) The processor's records must include at least the following information about the personal data in respect of which it is for the time being a processor—

(a) the name and contact details of each controller on behalf of which the processor is acting, and

(b) where the personal data is (including information about any personal data that is outside the United Kingdom).

(6) Where possible, the processor's records must include information about how it ensures that personal data is secure.

(7) A controller or processor must make the records maintained under this section available to the Commissioner on request.

(8) In deciding what is appropriate for the purposes of this section, a controller or processor must take into account, among other things—

(a) the nature, scope, context and purposes of processing carried out by or on behalf of the controller or by the processor,

(b) the risks for the rights and freedoms of individuals arising from that processing, including the likelihood of risks arising and their severity, and

(c) the resources available to the controller or processor. [s. 15(9)]

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 [s. 16(a)]

(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 [s. 16(b)]

(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.

Risk assessment and prior consultation [s. 17(6)]

64. Assessment of high risk processing ~~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 an assessment of the impact of the envisaged processing operations on the protection of personal data ~~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) The controller must produce a document recording compliance with this section which includes at least—

(a) a summary of the purposes of the processing,

(b) an assessment of whether the processing is necessary for those purposes,

(c) an assessment of the risks to the rights and freedoms of individuals referred to in subsection (1), and

(d) a description of how the controller proposes to mitigate those risks.

~~A data protection impact assessment must include the following—~~

~~a general description of the envisaged processing operations;~~

~~an assessment of the risks to the rights and freedoms of data subjects;~~

~~the measures envisaged to address those risks;~~

~~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.~~

[s. 17(7)]

(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 may ~~must~~ consult the Commissioner prior to the processing where an assessment ~~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 taken by the controller to mitigate the risk~~)~~. [s. 18(5)]

(3) Where the controller consults ~~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.

[s. 18(6)]

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

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

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

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

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

(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.

(3) Adherence to a code of conduct approved under section 68A may be used by a controller or processor as a means of demonstrating compliance with subsection (1). [s. 19(5)]

Obligations relating to personal data breaches

67. Notification of a personal data breach to the Commissioner

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

(a) without undue delay, and

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

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

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

(4) Subject to subsection (5), the notification must include—

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

(b) the name and contact details of the ~~data protection officer~~ senior responsible individual or other contact point from whom more information can be obtained; [sch. 4 para 15]

(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) . . . . . .

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

68. Communication of a personal data breach to the data subject

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

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

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

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

[sch. 4 para 16]

(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;~~ [s. 24(6)]

(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 .

Codes of conduct

68A Codes of conduct

(1) The Commissioner must encourage expert public bodies to produce codes of conduct intended to contribute to compliance with this Part.

(2) Under subsection (1), the Commissioner must, among other things, encourage the production of codes which take account of the specific features of the various processing sectors.

(3) For the purposes of this section—

(a) "public body" means a body or other person whose functions are, or include, functions of a public nature, and

(b) a public body is "expert" if, in the Commissioner's opinion, the body has the knowledge and experience needed to produce a code of conduct described in subsection (1).

(4) A code of conduct described in subsection (1) may, for example, make provision with regard to—

(a) lawful and fair processing;

(b) the collection of personal data;

(c) the information provided to the public and to data subjects;

(d) the exercise of the rights of data subjects;

(e) the measures and procedures referred to in sections 56, 57 and 62;

(f) the notification of personal data breaches to the Commissioner and the communication of personal data breaches to data subjects;

(g) the transfer of personal data to third countries or international organisations;

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing.

(5) Where an expert public body prepares a code of conduct described in subsection (1), it must submit the code to the Commissioner in draft.

(6) Where an expert public body submits a draft code to the Commissioner under this section, the Commissioner must—

(a) provide the body with an opinion on whether the draft code correctly reflects the requirements of this Part,

(b) decide whether to approve the code, and

(c) if the code is approved, register and publish the code.

(7) Subsections (5) and (6) apply in relation to amendments of a code of conduct described in subsection (1) as they apply in relation to such a code." [s. 19(6)]

~~*Data protection officers*~~ [s. 14(6)]

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.~~ [s. 14(6)]

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.~~ [s. 14(6)]

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.~~ [s. 14(6)]

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.~~

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;

"relevant international organisation" means an international organisation that carries out functions for any of the law enforcement purposes;

"relevant restricted transfer case" means (subject to subsection (3)) a case in which the personal data was originally made available to a competent authority (whether the current controller or a previous controller)—

(a) by a relevant authority in a third country or by a relevant international organisation, and

(b) subject to a condition (however imposed) that the data is not to be transferred to a third country or international organisation without authorisation from that authority or organisation or another such authority or organisation;

"overseas authoriser", in connection with a relevant restricted transfer case, means the person whose authorisation is required.

(3) In a case in which the personal data was originally made available to a competent authority subject to a condition that only requires authorisation for further transfers in certain circumstances, the case is a relevant restricted transfer case only in those circumstances. [sch. 6 para 2]

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 for a law enforcement purpose only if ~~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, 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.~~

(c) the transfer is carried out in accordance with the other provisions of this Part, and

(d) in a relevant restricted transfer case, the overseas authoriser has authorised the transfer or subsection (5) applies." [sch. 6 para 3(2)]

(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 adequacy regulations (see section 74A,~~

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

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

(3) Condition 2 is that the transfer—

(a) is approved by regulations under section 74AA that are in force at the time of the transfer,

(b) is made subject to appropriate safeguards (see section 75), or

(c) is based on special circumstances (see section 76). [sch. 6 para 3(3)]

(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)~~ This subsection applies if—

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

(b) ~~the authorisation~~ authorisation from the overseas authoriser cannot be obtained in good time. [sch. 6 para 3(4)]

(6) Where a transfer is made in a relevant restricted transfer case without the authorisation from the overseas authoriser ~~without the authorisation~~ mentioned in subsection (1)(d), the overseas authoriser ~~(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. [sch. 6 para 3(5)]

(7) ~~In this section, "relevant international organisation" means an international organisation that carries out functions for any of the law enforcement purposes.~~ [sch. 6 para 3(6)]

74. Transfers on the basis of an adequacy decision

. . . . . .

~~74ATransfers based on adequacy regulations~~

(1) ~~The Secretary of State may by regulations specify any of the following which the Secretary of State considers ensures an adequate level of protection of personal data—~~

(a) ~~a third country,~~

(b) ~~a territory or one or more sectors within a third country,~~

(c) ~~an international organisation, or~~

(d) ~~a description of such a country, territory, sector or organisation.~~

(2) ~~For the purposes of this Part of this Act, a transfer of personal data to a third country or an international organisation is based on adequacy regulations if, at the time of the transfer, regulations made under this section are in force which specify, or specify a description which includes—~~

(a) ~~in the case of a third country, the country or a relevant territory or sector within the country, and~~

(b) ~~in the case of an international organisation, the organisation,~~

~~and such a transfer does not require specific authorisation.~~

(3) ~~Regulations under this section may specify that the Secretary of State considers that an adequate level of protection of personal data is ensured only for a transfer specified or described in the regulations and, if they do so, only such a transfer may rely on those regulations for the purposes of subsection (2).~~

(4) ~~When assessing the adequacy of the level of protection for the purposes of this section or section 74B, the Secretary of State must, in particular, take account of—~~

(a) ~~the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, case-law, as~~

~~well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data is transferred,~~

(b) ~~the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, for assisting and advising data subjects in exercising their rights and for cooperation with the Commissioner, and~~

(c) ~~the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.~~

(5) ~~Regulations under this section—~~

(a) ~~where they relate to a third country, must specify their territorial and sectoral application;~~

(b) ~~where applicable, must specify the independent supervisory authority or authorities referred to in subsection (4)(b).~~

(6) ~~Regulations under this section may, among other things—~~

(a) ~~provide that, in relation to a country, territory, sector, organisation or territory specified, or falling within a description specified, in the regulations, section 74B(1) has effect as if it required the reviews described there to be carried out at such shorter intervals as are specified in the regulations;~~

(b) ~~identify a transfer of personal data by any means, including by reference to the controller or processor, the recipient, the personal data transferred or the means by which the transfer is made or by reference to relevant legislation, lists or other documents, as they have effect from time to time;~~

(c) ~~confer a discretion on a person.~~

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

[sch. 6 para 4]

74AA Transfers approved by regulations

(1) For the purposes of section 73, the Secretary of State may by regulations approve transfers of personal data to—

(a) a third country, or

(b) an international organisation.

(2) The Secretary of State may only make regulations under this section approving transfers to a third country or international organisation if the Secretary of State considers that the data protection test is met in relation to the transfers (see section 74AB).

(3) In making regulations under this section, the Secretary of State may have regard to any matter which the Secretary of State considers relevant, including the desirability of facilitating transfers of personal data to and from the United Kingdom.

(4) Regulations under this section may, among other things—

(a) make provision by reference to a third country or international organisation specified in the regulations or a description of country or organisation;

(b) approve all transfers of personal data to a third country or international organisation or only transfers specified or described in the regulations;

(c) identify a transfer of personal data by any means, including by reference to—

(i) a sector or geographic area within a third country,

(ii) the controller or processor,

(iii) the recipient of the personal data,

(iv) the personal data transferred,

(v) the means by which the transfer is made, or

(vi) relevant legislation, schemes, lists or other arrangements or documents, as they have effect from time to time;

(d) confer a discretion on a person.

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

[sch. 6 para 4]

74AB The data protection test

(1) For the purposes of section 74AA, the data protection test is met in relation to transfers to a third country or international organisation if the standard of the protection provided for data subjects with regard to law enforcement processing of personal data in the country or by the organisation is not materially lower than the standard of the protection provided for data subjects by or under—

(a) this Part, and

(b) Parts 5 to 7, so far as relevant to law enforcement processing.

(2) In considering whether the data protection test is met in relation to transfers of personal data to a third country or international organisation, the Secretary of State must consider, among other things—

(a) respect for the rule of law and for human rights in the country or by the organisation,

(b) the existence, and powers, of an authority responsible for enforcing the protection of data subjects with regard to the processing of personal data in the country or by the organisation,

(c) arrangements for judicial or non-judicial redress for data subjects in connection with such processing,

(d) rules about the transfer of personal data from the country or by the organisation to other countries or international organisations,

(e) relevant international obligations of the country or organisation, and

(f) the constitution, traditions and culture of the country or organisation.

(3) In subsections (1) and (2)—

(a) the references to the protection provided for data subjects are to that protection taken as a whole,

(b) the references to law enforcement processing are to processing by a competent authority for any of the law enforcement purposes or equivalent types of processing in the third country or by the international organisation (as appropriate), and

(c) the references to processing of personal data in the third country or by the international organisation are references only to the processing of personal data transferred from the United Kingdom.

(4) When the data protection test is applied only to certain transfers to a third country or international organisation that are specified or described, or to be specified or described, in regulations (in accordance with section 74AA(4)(b))—

(a) the references in subsections (1) to (3) to personal data are to be read as references only to personal data likely to be the subject of such transfers, and

(b) the reference in subsection (2)(d) to the transfer of personal data to other countries or international organisations is to be read as including the transfer of personal data within the third country or international organisation. [sch. 6 para 4]

74B~~Transfers based on adequacy regulations: review etc~~ Transfers approved by regulations: monitoring [sch. 6 para 5(2)]

~~(1) For so long as regulations under section 74A are in force which specify, or specify a description which includes, a third country, a territory or sector within a third country or an international organisation, the Secretary of State must carry out a review of whether the country, territory, sector or organisation ensures an adequate level of protection of personal data at intervals of not more than 4 years.~~

~~(2) Each review under subsection (1) must take into account all relevant developments in the third country or international organisation.~~ [sch. 6 para 5(3)]

(3) The Secretary of State must, on an ongoing basis, monitor developments in third countries and international organisations that could affect decisions to make regulations giving approval under section 74AA or to amend or revoke such regulations. [sch. 6 para 5(4)]

(4) Where the Secretary of State becomes aware that the data protection test is no longer met in relation to transfers to approved, or of a description approved, in regulations under 74AA, ~~a country, territory, sector or organisation specified, or falling within a description specified, in regulations under section 74A no longer ensures an adequate level of protection of personal data, whether as a result of a review under this section or otherwise~~, the Secretary of State must, to the extent necessary, amend or revoke the regulations. [sch. 6 para 5(5)]

(5) Where regulations under section 74AA are amended or revoked in accordance with subsection (4), the Secretary of State must enter into consultations with the third country or

international organisation concerned with a view to improving the protection provided to data subjects with regard to the processing of personal data in the country or by the organisation ~~remedying the lack of an adequate level of protection~~. [sch. 6 para 5(6)]

(6) The Secretary of State must publish—

(a) a list of the third countries, ~~territories and specified sectors within a third country~~ and international organisations, and the descriptions of such countries, ~~territories, sectors~~ and organisations, which are for the time being approved by regulations under section 74AA as places or persons to which personal data may be transferred ~~specified in regulations under section 74A~~, and [sch. 6 para 5(7)]

(b) a list of the third countries, ~~territories and specified sectors within a third country~~ and international organisations, and the descriptions of such countries, ~~territories, sectors~~ and organisations, which have been but are no longer approved by ~~specified in~~ such regulations. [sch. 6 para 5(8)]

(7) In the case of regulations under section 74AA which approve only certain transfers to a third country or international organisation that are ~~regulations under section 74A which specify that an adequate level of protection of personal data is ensured only for a transfer~~ specified or described in the regulations (in accordance with section 74AA(4)(b))—

~~(a) The duty under subsection (1) is only to carry out a review of the level of protection ensured for such a transfer, and~~ [sch. 6 para 5(9)]

(b) the lists published under subsection (6) must specify or describe the relevant transfers.

75. Transfers ~~on the basis of~~ subject to appropriate safeguards [sch. 6 para 6(2)]

(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.~~ [sch. 6 para 6(3)]

(1A) A transfer of personal data to a third country or an international organisation is made subject to appropriate safeguards only if—

(a) the controller, acting reasonably and proportionately, considers that the data protection test is met in relation to the transfer or that type of transfer (see subsection (5)), or

(b) an appropriate legal instrument binds the intended recipient of the data (see subsection (4)).” [sch. 6 para 6(4)]

(2) The controller must inform the Commissioner about the categories of data transfers that take place in reliance on this section ~~subsection (1)(b)~~. [sch. 6 para 6(5)]

(3) Where a transfer of data takes place in reliance on this section ~~subsection (1)~~— [sch. 6 para 6(6)]

(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 legal instrument is "appropriate", in relation to a transfer of personal data, if—

(a) the instrument is intended to be relied on in connection with the transfer or that type of transfer,

(b) at least one competent authority is a party to the instrument, and

(c) each competent authority that is a party to the instrument, acting reasonably and proportionately, considers that the data protection test is met in relation to the transfers, or types of transfer, intended to be made in reliance on the instrument (see subsection (5)).

(5) For the purposes of this section, the data protection test is met in relation to a transfer, or a type of transfer, of personal data if, after the transfer, the standard of the protection provided for the data subject with regard to that personal data, whether by a binding legal instrument or by other means, would not be materially lower than the standard of the protection provided for the data subject with regard to the personal data by or under—

(a) this Part, and

(b) Parts 5 to 7, so far as they relate to processing by a competent authority for any of the law enforcement purposes.

(6) For the purposes of subsections (1A)(a) and (4)(c), what is reasonable and proportionate is to be determined by reference to all the circumstances, or likely circumstances, of the transfer or type of transfer, including the nature and volume of the personal data transferred.

(7) In this section, references to the protection provided for the data subject are to that protection taken as a whole. [sch. 6 para 6(5)]

76. Transfers ~~on the basis of~~ based on special circumstances [sch. 6 para 7(2)]

(A1) A transfer of personal data to a third country or international organisation is based on special circumstances where—

(a) it is made in the absence of approval by regulations under section 74AA and of compliance with section 75 (appropriate safeguards), and

(b) it is necessary for a special purpose. [sch. 6 para 7(3)]

(1) ~~A transfer of personal data to a third country or international organisation is based on special circumstances where the transfer is necessary —~~ A transfer of personal data is necessary for a special purpose if it 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 or national security of a third country or the United Kingdom,

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

(e) ~~in individual cases~~ in particular circumstances, for a legal purpose.

[sch. 6 para 7(4)]

(2) ~~But subsection (1)(d) and (e) do not apply~~ But a transfer of personal data is not necessary for a special purpose by virtue of subsection (1)(d) or (e) if the controller determines that fundamental rights and freedoms of the data subject override the public interest in the transfer.

[sch. 6 para 7(5)]

(2A) In accordance with the third data protection principle, the amount of personal data transferred in reliance on this section must not be excessive in relation to the special purpose relied on.

[sch. 6 para 7(6)]

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

[sch. 6 para 7(7)]

(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 the United Kingdom 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—

(a) 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 (the "UK authoriser"), or

(b) (subject to subsection (4)) that—

(i) the data is not to be so transferred without such authorisation except where subsection (1A) applies, and

(ii) where a transfer is made without such authorisation, the UK authoriser must be informed without delay." [sch. 6 para 8(2)]

(1A) This subsection applies if—

(a) the transfer is necessary for the prevention of an immediate and serious threat to the public security or national security of a third country or the United Kingdom, and

(b) authorisation from the UK authoriser cannot be obtained in good time."

[sch. 6 para 8(3)]

(2) ~~A competent authority~~ The UK authoriser may give an authorisation under subsection (1) only where the further transfer is necessary for a law enforcement purpose. [sch. 6 para 8(4)]

(3) In deciding whether to give the authorisation, the UK authoriser ~~competent authority~~ must take into account (among any other relevant factors)— [sch. 6 para 8(5)]

(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, 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.~~

(4) In a relevant restricted transfer case—

(a) the transferring controller must make the transfer subject to the condition described in subsection (1)(a), and

(b) the UK authoriser may not authorise a further transfer of personal data under subsection (1)(a) unless the overseas authoriser has authorised the further transfer or subsection (5) applies."

[sch. 6 para 8(6)]

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

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

(b) ~~the authorisation~~ authorisation from the overseas authoriser cannot be obtained in good time.

[sch. 6 para 8(7)]

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

[sch. 6 para 8(8)]

CHAPTER 6 SUPPLEMENTARY

78A National security exemption

(1) A provision mentioned in subsection (2) does not apply to personal data processed for law enforcement purposes if exemption from the provision is required for the purposes of safeguarding national security.

(2) The provisions are—

(a) Chapter 2 of this Part (principles), except for the provisions listed in subsection (3);

(b) Chapter 3 of this Part (rights of the data subject);

(c) in Chapter 4 of this Part—

(i) section 67 (notification of personal data breach to the Commissioner);

(ii) section 68 (communication of personal data breach to the data subject);

(d) Chapter 5 of this Part (transfers of personal data to third countries etc), except for the provisions listed in subsection (4);

(e) in Part 5—

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

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

(f) in Part 6—

(i) sections 142 to 154 and Schedule 15 (Commissioner's notices and powers of entry and inspection);

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

(g) in Part 7, section 187 (representation of data subjects).

(3) The provisions of Chapter 2 of this Part (principles) which are excepted from the list in subsection (2) are—

(a) section 35(1) (the first data protection principle) so far as it requires processing of personal data to be lawful;

(b) section 35(2) to (5) (lawfulness of processing and restrictions on sensitive processing);

(c) section 42 (safeguards: sensitive processing);

(d) Schedule 8 (conditions for sensitive processing).

(4) The provisions of Chapter 5 of this Part (transfers of personal data to third countries etc) which are excepted from the list in subsection (2) are—

(a) the following provisions of section 73—

(i) subsection (1)(a) (conditions for transfer), so far as it relates to the condition in subsection (2) of that section, and subsection (2) (transfer must be necessary for a law enforcement purpose);

(ii) subsections (1)(d), (5) and (6) (conditions for transfer of personal data originally made available by a member State);

(b) section 78 (subsequent transfers). [s. 24(7)]

79. National security: certificate

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

(2) ~~The certificate may—~~

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

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

(3) ~~Subject to subsection (6), a certificate issued under subsection (1) is conclusive evidence that the specific restriction or (as the case may be) any restriction falling within the general description is, or at any time was, a necessary and proportionate measure to protect national security.~~ [s. 24(8)(a)]

(3A) Subject to subsection (5), a certificate signed by a Minister of the Crown certifying that exemption from all or any of the provisions listed in section 78A(2) is, or at any time was, required in relation to any personal data for the purposes of safeguarding national security is conclusive evidence of that fact. [s. 24(8)(b)]

(4) A certificate issued under subsection (3A) ~~(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. [s. 24(8)(c)]

(5) Any person directly affected by the issuing of a certificate under subsection (3A) ~~(1)~~ may appeal to the Tribunal against the certificate. [s. 24(8)(d)]

(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 certificate under subsection (3A) which identifies the personal data to which it applies by means of a general description applies to any personal data, ~~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 certificate does not apply to the personal data in question ~~the restriction does not fall within that description~~. [s. 24(8)(e)]

(8) But, subject to any determination under subsection (9), the certificate ~~restriction~~ is to be conclusively presumed so to apply ~~to fall within the general description~~. [s. 24(8)(f)]

(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 (3A) ~~(1)~~ is to be— [s. 24(8)(g)]

(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 (3A) ~~(1)~~ is— [s. 24(8)(h)]

(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 (3A) ~~(1)~~ on a Minister of the Crown is exercisable only by— [s. 24(8)(i)]

(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.~~ [s. 24(8)(j)]

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 a non-UK recipient.

(2) In this section—

"non-UK 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 non-UK 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).

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

(A1) This Part—

(a) applies to processing of personal data by an intelligence service, and

(b) applies to processing of personal data by a qualifying competent authority where the processing is the subject of a designation notice that is for the time being in force (see sections 82A to 82E). [s. 25(2)(a)]

(1) This Part applies only 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. [s. 25(2)(b)]

(2) In this Part, "intelligence service" means—

(a) the Security Service;

(b) the Secret Intelligence Service;

(c) the Government Communications Headquarters.

(2A) In this Part—

"competent authority" has the same meaning as in Part 3;

"qualifying competent authority" means a competent authority specified or described in regulations made by the Secretary of State. [s. 25(2)(c)]

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

(4) Regulations under this section are subject to the affirmative resolution procedure. [s. 25(2)(d)]

82A Designation of processing by a qualifying competent authority

(1) For the purposes of this Part, the Secretary of State may give a notice designating processing of personal data by a qualifying competent authority (a "designation notice") where—

(a) an application for designation of the processing is made in accordance with this section, and

(b) the Secretary of State considers that designation of the processing is required for the purposes of safeguarding national security.

(2) The Secretary of State may only designate processing by a qualifying competent authority that is carried out by the authority as a joint controller with at least one intelligence service.

(3) The Secretary of State may not designate processing by a qualifying competent authority that consists of the transfer of personal data to—

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

(b) an international organisation.

(4) A designation notice must—

(a) specify or describe the processing and qualifying competent authority that are designated, and

(b) be given to the applicants for the designation (and see also section 82D).

(5) An application for designation of processing of personal data by a qualifying competent authority must be made jointly by—

(a) the qualifying competent authority, and

(b) the intelligence service with which the processing is to be carried out.

(6) An application may be made in respect of more than one qualifying competent authority and in respect of processing with more than one intelligence service.

(7) The application must—

(a) describe the processing, including the intended purposes and means of processing, and

(b) explain why the applicants consider that designation is required for the purposes of safeguarding national security.

(8) Before giving a designation notice, the Secretary of State must consult the Commissioner.

(9) In this section, "joint controller", in relation to processing of personal data, means a controller whose responsibilities for compliance with this Part in relation to the processing are determined in an arrangement under section 104. [s. 25(3)]

82B Duration of designation notice

(1) A designation notice must state when it comes into force.

(2) A designation notice ceases to be in force at the earliest of the following times—

(a) at the end of the period of 5 years beginning with the day on which it comes into force;

(b) (if relevant) at the end of a shorter period specified in the notice;

(c) when the notice is withdrawn under section 82C.

(3) The Secretary of State may give a further designation notice in respect of processing that is, or has been, the subject of a previous designation notice. [s. 25(3)]

82C Review and withdrawal of designation notice

(1) Subsections (2) to (4) apply where processing is the subject of a designation notice for the time being in force.

(2) A person who applied for the designation of the processing must notify the Secretary of State without undue delay if the person considers that the designation is no longer required for the purposes of safeguarding national security.

(3) A person who applied for the designation of the processing must, on a request from the Secretary of State, provide—

(a) a description of the processing that is being, or is intended to be, carried out in reliance on the notice, and

(b) an explanation of why the person considers that designation of the processing continues to be required for the purposes of safeguarding national security.

(4) The Secretary of State must at least annually—

(a) review each designation notice that is for the time being in force, and

(b) consider whether designation of the processing which is the subject of the notice continues to be required for the purposes of safeguarding national security.

(5) The Secretary of State—

(a) may withdraw a designation notice by giving a further notice (a "withdrawal notice") to the persons who applied for the designation, and

(b) must give a withdrawal notice if the Secretary of State considers that designation of some or all of the processing to which the notice applies is no longer required for the purposes of safeguarding national security (whether as a result of a review required under subsection (4) or otherwise).

(6) A withdrawal notice must—

(a) withdraw the designation notice completely, and

(b) state when it comes into force.

(7) In determining when a withdrawal notice required under subsection (5)(b) comes into force, the Secretary of State must consider—

(a) the desirability of the processing ceasing to be designated as soon as possible, and

(b) where relevant, the time needed to effect an orderly transition to new arrangements for the processing of personal data. [s. 25(3)]

82D Records of designation notices

(1) Where the Secretary of State gives a designation notice—

(a) the Secretary of State must send a copy of the notice to the Commissioner, and

(b) the Commissioner must publish a record of the notice.

(2) The record must contain—

(a) the Secretary of State's name,

(b) the date on which the notice was given,

(c) the date on which the notice ceases to have effect (if not previously withdrawn), and

(d) subject to subsection (3), the rest of the text of the notice.

(3) The Commissioner must not publish the text, or a part of the text, of the notice if—

(a) the Secretary of State 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 Secretary of State has notified the Commissioner of that determination.

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

(5) Where the Secretary of State gives a withdrawal notice, the Secretary of State must send a copy of the notice to the Commissioner. [s. 25(3)]

82E Appeal against designation notice

(1) A person directly affected by a designation notice may appeal to the Tribunal against the notice.

(2) If, on an appeal under this section, the Tribunal finds that, applying the principles applied by a court on an application for judicial review, the Secretary of State did not have reasonable grounds for giving the notice, the Tribunal may—

(a) allow the appeal, and

(b) quash the notice. [s. 25(3)]

Definitions

83. Meaning of "controller" and "processor"

(A1) For the purposes of this Part—

(a) an intelligence service is the "controller" in relation to the processing of personal data if it satisfies subsection (1) alone or jointly with others, and

(b) a qualifying competent authority is the "controller" in relation to the processing of personal data that is the subject of a designation notice that is for the time being in force if the authority satisfies subsection (1) jointly with others. [s. 26(4)(a)]

(1) ~~In this Part, "controller" means the intelligence service which, alone or jointly with others~~ This subsection is satisfied by a person who— [s. 26(4)(b)]

(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~~ person on whom 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). [s. 26(4)(c)]

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.

(2A) "Designation notice" has the meaning given in section 82A. [s. 26(5)(a)]

(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.

(6A) "Withdrawal notice" has the meaning given in section 82C. [s. 26(5)(b)]

(7) Sections 3 and 205 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~~ (whether from the data subject or otherwise) must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed by or on behalf of a controller in a manner that is incompatible with the purpose for which ~~it is collected~~ the controller collected it. [s. 6(9)]

(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 under section 165 and the contact details of the Commissioner; [sch. 8 para 16]

(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 under section 165 and the contact details of the Commissioner; [sch. 8 para 17]

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

(2A) A controller is not obliged to provide information under this section in response to a request that is vexatious or excessive (see section 204A). [s. 7(8)(a)]

(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 subsections (2A) to (6), a controller must comply with a request under subsection (1)— [s. 7(8)(b)]

(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.

(11A) In any proceedings where there is an issue as to whether a request is vexatious or excessive, it is for the controller to show that it is. [s. 7(8)(c)]

(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 one month beginning with the relevant time, subject to subsection (14A);

~~—~~

~~(a) the period of 1 month, or~~
~~(b) such longer period, not exceeding 3 months, as may be specified in regulations made by the Secretary of State, beginning with the relevant time;~~ [s. 8(7)(a)]

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

(a) when the controller receives the request,
(b)when the fee (if any) is paid, and
(c) when the controller receives the information (if any) required under subsection (5) in connection with the request.

(14A) The controller may, by giving notice to the data subject, extend the applicable time period by two further months where that is necessary by reason of—
(a) the complexity of requests made by the data subject, or
(b) the number of such requests.

(14B) A notice under subsection (14A) must—
(a) be given before the end of the period of one month beginning with the relevant time, and
(b) state the reasons for the delay. [s. 8(7)(b)]

(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.~~ [s. 7(9)]

(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 entirely [s. 11(4)] 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 and section 97, a decision that has legal effects as regards an individual is to be regarded as significantly affecting the individual.

(4) For the purposes of this section and section 97, a decision is based on entirely automated processing if the decision-making process does not include an opportunity for a human being to accept, reject or influence the decision. [s. 11(4)]

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 entirely automated processing of personal data relating to the data subject, and [s. 11(4)(a)]

(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 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 entirely automated processing.

[s. 11(4)(b)]

(5) If a request is made to the controller under subsection (4), the controller must, before the end of the period of 1 month beginning with receipt of the request—

(a) consider the request, including any information provided by the data subject that is relevant to it, 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.~~ [s. 11(4)(c)]

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 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 time", in relation to a notice under subsection (1), means—

(a) when the controller receives the notice, or

(b) if later, 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 measures, including 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. [s. 12(10)]

104. Joint controllers

(1) Where two or more controllers ~~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. [s. 26(6)]

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

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

(c) in Chapter 4 of this part, section 108 (communication of a personal data breach to the Commissioner); [s. 24(9)]

(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) and (g) and 2;

(e) in Part 6—

(i) sections 142 to 154 and Schedule 15 (Commissioner's notices and powers of entry and inspection);

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

(iii) sections 174 to 176 (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.~~ [s. 101(4)]

The Information Commission

114A The Information Commission

(1) A body corporate called the Information Commission is established

(2) Schedule 12A makes further provision about the Commission. [s. 100(2)]

General functions

115. General functions under the UK GDPR and safeguards

(1) . . . . . .

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

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

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

(and see also the Commissioner's duty under section 2 and section 28(5)).

(3) The Commissioner's functions in relation to the processing of personal data to which the UK 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 UK GDPR are subject to the safeguards in subsections (5) to (9).

(5) The Commissioner's power under Article 58(1)(a) of the UK 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 UK GDPR) is exercisable only by giving an information notice under section 142.

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

(7) The Commissioner's powers under Article 58(1)(e) and (f) of the UK 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 154), or

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

(8) The following powers are exercisable only by giving an enforcement notice under section 149—

(a) the Commissioner's powers under Article 58(2)(c) to (g) and (j) of the UK 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 UK GDPR.

(9) The Commissioner's powers under Articles 58(2)(i) and 83 of the UK GDPR (administrative fines) are exercisable only by giving a penalty notice under section 155.

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

116. Other general functions

(A1) The Commissioner is responsible for monitoring the application of Part 3 of this Act, in order to protect the fundamental rights and freedoms of individuals in relation to processing by a competent authority for any of the law enforcement purposes (as defined in Part 3) and to facilitate the free flow of personal data.

(1) The Commissioner—

(a) . . . . . .

(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 UK 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 or the UK GDPR 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

International role

118. Co-operation between parties to the Data Protection Convention

(1) . . . . . .

(2) . . . . . .

(3) . . . . . .

(4) . . . . . .

(5) Part 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.

(7) Paragraphs (c) and (d) of section 3(14) do not apply to references in this section to personal data, the processing of personal data, a controller or a processor.

119A Standard clauses for transfers to third countries etc

(1) The Commissioner may issue a document specifying standard data protection clauses which the Commissioner considers are capable of securing that the data protection test set out in Article 46 of the UK GDPR is met in relation to transfers of personal data generally or in relation to types of transfer described in the document. ~~Provide appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Article 46 of the UK GDPR (and see also section 17C).~~ [sch. 7 para 17]

(2) The Commissioner may issue a document that amends or withdraws a document issued under subsection (1).

(3) A document issued under this section—

(a) must specify when it comes into force,

(b) may make different provision for different purposes, and

(c) may include transitional provision or savings.

(4) Before issuing a document 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.

(5) After a document is issued under this section—

(a) the Commissioner must send a copy to the Secretary of State, and

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

(6) If, within the 40-day period, either House of Parliament resolves not to approve the document then, with effect from the end of the day on which the resolution is passed, the document is to be treated as not having been issued under this section (so that the document, and any amendment or withdrawal made by the document, is to be disregarded for the purposes of Article 46(2)(d) of the UK GDPR).

(7) Nothing in subsection (6)—

(a) affects any transfer of personal data previously made in reliance on the document, or

(b) prevents a further document being laid before Parliament.

(8) (8)The Commissioner must publish—

(a) a document issued under this section, and

(b) a notice identifying any document which, under subsection (6), is treated as not having been issued under this section.

(9) The Commissioner must keep under review the clauses specified in a document issued under this section for the time being in force.

(10) 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.

(11) In calculating the 40-day period, no account is to be taken of any whole days that fall within a period during which Parliament is dissolved or prorogued or during which both Houses of Parliament are adjourned for more than 4 days. [sch 9. para 15]

(12) In this section, "trade association" includes a body representing controllers or processors.

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

(2A) The Commissioner may contribute to the activities of international organisations with data protection functions.

(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 outside the United Kingdom.

(7) Section 3(14)(c) does not apply to references to personal data and the processing of personal data in this section.

Duties in carrying out functions

120A Principal objective

It is the principal objective of the Commissioner, in carrying out functions under the data protection legislation—

(a) to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest, and

(b) to promote public trust and confidence in the processing of personal data. [s. 27(3)]

120B Duties in relation to functions under the data protection legislation

In carrying out functions under the data protection legislation, the Commissioner must have regard to such of the following as appear to the Commissioner to be relevant in the circumstances—

(a) the desirability of promoting innovation;

(b) the desirability of promoting competition;

(c) the importance of the prevention, investigation, detection and prosecution of criminal offences;

(d) the need to safeguard public security and national security. [s. 27(3)]

120C Strategy

(1) The Commissioner must prepare a strategy for carrying out the Commissioner's functions under the data protection legislation in accordance with the Commissioner's duties under—

(a) sections 120A and 120B,

(b) section 108 of the Deregulation Act 2015 (exercise of regulatory functions: economic growth), and

(c) section 21 of the Legislative and Regulatory Reform Act 2006 (exercise of regulatory functions: principles).

(2) The Commissioner must—

(a) review the strategy from time to time, and

(b) revise the strategy as appropriate.

(3) The Commissioner must publish the strategy and any revised strategy. [s. 27(3)]

120D Duty to consult other regulators

(1) The Commissioner must, at such times as the Commissioner considers appropriate, consult the persons mentioned in subsection (2) about how the manner in which the Commissioner exercises functions under the data protection legislation may affect economic growth, innovation and competition.

(2) The persons are—

(a) such persons exercising regulatory functions as the Commissioner considers appropriate;

(b) such other persons as the Commissioner considers appropriate.

(3) In this section "regulatory function" has the meaning given by section 111 of the Deregulation Act 2015. [s. 27(3)]

Strategic priorities

120E Designation of statement of strategic priorities

(1) The Secretary of State may designate a statement as the statement of strategic priorities for the purposes of this Part if the requirements set out in section 120H are satisfied.

(2) The statement of strategic priorities is a statement prepared by the Secretary of State that sets out the strategic priorities of Her Majesty's government relating to data protection.

(3) The Secretary of State must publish the statement of strategic priorities (including any amended statement following a review under section 120G) in whatever manner the Secretary of State considers appropriate.

(4) In this Part, "the statement of strategic priorities" means the statement for the time being designated under subsection (1).

120F Duties of the Commissioner in relation to strategic priorities

(1) The Commissioner must have regard to the statement of strategic priorities when carrying out functions under the data protection legislation.

(2) But the duty in subsection (1) does not apply when the Commissioner is carrying out functions in relation to a particular person, case or investigation.

(3) Where the Secretary of State designates a statement as the statement of strategic priorities (including any amended statement following a review under section 120G), the Commissioner must—

(a) explain in writing how the Commissioner will have regard to the statement when carrying out functions under the data protection legislation, and

(b) publish a copy of that explanation.

(4) The duty in subsection (3) must be complied with—

(a) within the period of 40 days beginning with the day of the designation, or

(b) within whatever longer period the Secretary of State may allow.

(5) In calculating the period of 40 days mentioned in subsection (4)(a), no account is to be taken of—

(a) Saturdays or Sundays,

(b) Christmas Day or Good Friday, or

(c) a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom.

(6) For a further duty of the Commissioner in relation to the statement of strategic priorities, see section 139(1A)(c). [s. 28(2)]

120G Review of designated statement

(1) The Secretary of State must review the statement of strategic priorities if a period of 3 years has elapsed since the relevant time.

(2) The "relevant time", in relation to the statement of strategic priorities, means—

(a) the time when the statement was first designated under section 120E, or

(b) if later, the time when a review of the statement under this section last took place.

(3) A review under subsection (1) must take place as soon as reasonably practicable after the end of the 3 year period.

(4) The Secretary of State may review the statement of strategic priorities at any other time if—

(a) a Parliamentary general election has taken place since the relevant time,

(b) a significant change in the policy of Her Majesty's government relating to data protection has occurred since the relevant time, or

(c) the Parliamentary requirement in relation to an amended statement was not met on the last review (see subsection (12)).

(5) For the purposes of subsection (4)(b), a significant change in the policy of the government relating to data protection has occurred only if—

(a) the change was not anticipated by the Secretary of State at the relevant time, and

(b) if the change had been so anticipated, it appears to the Secretary of State likely that the statement would have been different in a material way.

(6) On a review under this section, the Secretary of State may—

(a) amend the statement (including by replacing the whole or part of the statement with new content),

(b) leave the statement as it is, or

(c) withdraw the statement's designation as the statement of strategic priorities.

(7) A statement amended under subsection (6)(a) has effect only if the Secretary of State designates the amended statement as the statement of strategic priorities statement under section 120E (and the requirements set out in section 120H apply in relation to any such designation).

(8) Where the designation of a statement is withdrawn under subsection (6)(c), the Secretary of State must publish notice of the withdrawal in whatever manner the Secretary of State considers appropriate.

(9) For the purposes of this section, corrections of clerical or typographical errors are not to be treated as amendments of the statement.

(10) The designation of a statement as the statement of strategic priorities ceases to have effect upon a subsequent designation of an amended statement as the statement of strategic priorities in accordance with subsection (7).

(11) For the purposes of subsection (2)(b), a review of a statement takes place—

(a) in the case of a decision on the review to amend the statement under subsection (6)(a)—

(i) at the time when the amended statement is designated as the statement of strategic priorities under section 120E, or

(ii) if the amended statement is not so designated, at the time when the amended statement was laid before Parliament under section 120H(1);

(b) in the case of a decision on the review to leave the statement as it is under subsection (6)(b), at the time when that decision is taken.

(12) For the purposes of subsection (4)(c), the Parliamentary requirement in relation to an amended statement was not met on the last review if—

(a) on the last review of the statement of strategic priorities to be held under this section, an amended statement was laid before Parliament under section 120H(1), but

(b) the amended statement was not designated because within the period mentioned in section 120H(2) either House of Parliament resolved not to approve it. [s. 28(2)]

120H Parliamentary procedure

(1) Before the Secretary of State designates a statement as the statement of strategic priorities, the Secretary of State must lay the statement before Parliament.

(2) The Secretary of State must then wait until the end of the 40-day period and may not designate the statement if, within that period, either House of Parliament resolves not to approve it.

(3) "The 40-day period" means—

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

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

(4) In calculating the 40-day period, no account is to be taken of any whole days that fall within a period during which Parliament is dissolved or prorogued or during which both Houses are adjourned for more than 4 days. [s. 28(2)]

Codes of practice

121. 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.

122. 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.

123. 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 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 UK 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 UK 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.

124. Data protection and journalism code

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

(a) practical guidance in relation to the processing of personal data for the purposes of journalism 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 processing of personal data for the purposes of journalism.

(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 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 processing of personal data for the purposes of journalism" means such practice in the processing of personal data for those purposes as appears to the Commissioner to be desirable having regard to—

(a) the interests of data subjects and others, ~~including compliance with the requirements of the data protection legislation~~, and
(b)the special importance of the public interest in the freedom of expression and information;

and includes compliance with the requirements of the data protection legislation; [sch 9. para 16]

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

124A Other codes of practice

(1) The Commissioner must prepare appropriate codes of practice giving guidance as to good practice in the processing of personal data if required to do so by regulations made by the Secretary of State.

(2) 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 persons to whom it is to relate.

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

(4) 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.

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

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

(7) 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." [s. 29(2)]

124B Panels to consider codes of practice

(1) This section applies where a code is prepared under section 121, 122, 123, 124 or 124A, subject to subsection (11).

(2) The Commissioner must establish a panel of individuals to consider the code.

(3) The panel must consist of—

(a) individuals the Commissioner considers have expertise in the subject matter of the code, and

(b) individuals the Commissioner considers—

(i) are likely to be affected by the code, or

(ii) represent persons likely to be affected by the code.

(4) Before the panel begins to consider the code, the Commissioner must—

(a) publish the code in draft, and

(b) publish a statement that—

(i) states a panel has been establish to consider the code,

(ii) identifies the members of the panel,

(iii) explains the process by which they were selected, and

(iv) explains the reasons for their selection.

(5) Where at any time it appears to the Commissioner that a member of the panel is not willing or able to serve as a member of the panel, the Commissioner may select another individual to be a member of the panel.

(6) Where the Commissioner selects an individual to be a member of the panel under subsection (5), the Commissioner must publish a statement that—

(a) identifies the member of the panel,

(b) explains the process by which the member was selected, and

(c) explains the reasons for the member's selection.

(7) The Commissioner must make arrangements—

(a) for the members of the panel to consider the code with one another (whether in person or otherwise), and

(b) for the panel to prepare and submit to the Commissioner a report on the code within such reasonable period as is determined by the Commissioner.

(8) If the panel submits to the Commissioner a report on the code within the period determined by the Commissioner, the Commissioner must as soon as reasonably practicable—

(a) make any alterations to the code that the Commissioner considers appropriate in the light of the report, and

(b) publish—

(i) the code in draft,

(ii) the report or a summary of it, and

(iii) in a case where a recommendation in the report to alter the code has not been accepted by the Commissioner, an explanation of why it has not been accepted.

(9) The Commissioner may pay remuneration and expenses to the members of the panel.

(10) This section applies in relation to amendments prepared under section 121, 122, 123, 124 or 124A as it applies in relation to codes prepared under those sections, subject to subsection (11).

(11) The Secretary of State may by regulations provide that this section does not apply, or applies with modifications, in the case of a code or amendments of a code that—

(a) is prepared under section 124A, and

(b) is specified in the regulations.

(12) Regulations under this section are subject to the negative resolution procedure. [s. 30(2)]

124C Impact assessments of codes of practice

(1) Where a code is prepared under section 121, 122, 123, 124 or 124A, the Commissioner must carry out and publish an assessment of—

(a) who would be likely to be affected by the code, and

(b) the effect the code would be likely to have on them.

(2) This section applies in relation to amendments prepared under section 121, 122, 123, 124 or 124A as it applies in relation to codes prepared under those sections. [s. 30(2)]

124D Approval by Secretary of State of codes of practice

(1) Where a code is prepared under section 121, 122, 123, 124 or 124A, the Commissioner must submit the final version to the Secretary of State.

(2) Within the period of 40 days beginning with the day on which the code is submitted to the Secretary of State, the Secretary of State must decide whether to approve the code.

(3) If the Secretary of State approves the code, the Secretary of State must lay the code before Parliament.

(4) If the Secretary of State does not approve the code, the Secretary of State must—

(a) give a statement to the Commissioner that—

(i) states that the Secretary of State does not approve the code, and

(ii) explains the reasons why the Secretary of State does not approve the code, and

(b) publish the statement.

(5) If the Secretary of State does not approve the code, the Commissioner must—

(a) revise the code in the light of the statement given by the Secretary of State, and

(b) submit the revised code to the Secretary of State.

(6) If the Commissioner submits a revised code to the Secretary of State, subsections (2) to (5) and this subsection apply again.

(7) This section applies in relation to amendments prepared under section 121, 122, 123, 124 or 124A as it applies in relation to codes prepared under those sections.

(8) In calculating the period of 40 days mentioned in subsection (2), no account is to be taken of—

(a) Saturdays or Sundays,

(b) Christmas Day or Good Friday, or

(c) a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom." [s. 31(2)]

125. Approval by Parliament of codes prepared under sections 121 to 124A

[s. 31(3)(a) and s. 29(3)(a)]

(1) This section applies where a code is laid before Parliament under section 124D ~~When a code is prepared under section 121, 122, 123 or 124—~~

(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 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 when this Act is passed, and~~

(b) ~~the Secretary of State must lay it before Parliament as soon as reasonably practicable~~. [s. 31(3)(b)]

(3) If, within the 40-day period, either House of Parliament resolves not to approve the code ~~a code prepared under section 121, 122, 123 or 124~~, the Commissioner must not issue the code. [s. 31(3)(c)]

(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 the Commissioner is prevented by subsection (3) from issuing a code that is not a replacement code, the Commissioner must prepare another version of the code. ~~If, as a result of subsection (3), there is no code in force under section 121, 122, 123 or 124, the Commissioner must prepare another version of the code~~. [s. 29(3)(b)]

(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 whole days that fall within a period during which Parliament is dissolved or prorogued or during which both Houses of Parliament are adjourned for more than 4 days. [sch 9. para 17]

(9) This section, other than subsection~~s (2) and~~ (5) applies in relation to amendments prepared under section 121, 122, 123, 124 or 124A as it applies in relation to codes prepared under those sections. [s. 31(3)(d) and s. 29(3)(c)]

126. Publication and review of codes issued under section 125(4)

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

(2) Where an amendment of a code is issued under section 125(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(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 121(2), 122(2), 123(2), ~~or~~ 124(2) or 124A(3) with a view to remedying the situation. [s. 29(4)]

127. Effect of codes issued under section 125(4)

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

(2) A code issued under section 125(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(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(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~~. [s. 29(4)]

Consensual audits

129. Consensual audits

(1) The Commissioner's functions under Article 58(1) of the UK GDPR and paragraph 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 124A ~~128~~. [s. 29(6)]

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) . . . . . .

(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

(1) The Commissioner may require a person other than a data subject or a ~~data protection officer~~ senior responsible individual 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.

(2) In this section and section 135, "senior responsible individual" means an individual designated as the senior responsible individual of a controller or processor under Article 27A of the UK GDPR or section 58A of this Act. [sch.4 para 17]

135. ~~Manifestly unfounded~~ Vexatious or excessive requests by data subjects etc [s. 32(2)(a)]

(1) Where a request to the Commissioner from a data subject or a ~~data protection officer~~ senior responsible individual is ~~manifestly unfounded~~ vexatious or excessive (see section 204A) , the Commissioner may— [sch. 4 para 18 and s. 32(2)(b)]

(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.~~ [s. 32(2)(c)]

(3) In any proceedings where there is an issue as to whether a request described in subsection (1) is ~~manifestly unfounded~~ vexatious or excessive, it is for the Commissioner to show that it is. [s. 32(2)(d)]

(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 UK GDPR.~~ [s. 32(2)(e)]

(5) Article 57(3) of the UK GDPR (performance of Information Commissioner's tasks generally to be free of charge for data subject) has effect subject to this section. [s. 32(2)(f)]

(6) In this section, "request" does not include a complaint under section 165.

[sch. 8 para 18]

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 or 135, ~~or~~

(b) ~~Article 57(4) of the UK GDPR~~. [s. 32(3)]

(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: supplementary

(1) Before making regulations under section 137(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 182).

(2) The Commissioner—

(a) must keep under review the working of regulations under section 137(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(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(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(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(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(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.

(1A) In connection with the Commissioner's functions under the data protection legislation, the report must contain (among other things)—

(a) a review of what the Commissioner has done during the reporting period to comply with the duties under—

(i) sections 120A and 120B,

(ii) section 108 of the Deregulation Act 2015, and

(iii) section 21 of the Legislative and Regulatory Reform Act 2006,

including a review of the operation of the strategy prepared and published under section 120C;

(b) a review of what the Commissioner has done during the reporting period to comply with the duty under section 120D.

(c) a review of how the Commissioner has had regard to the statement of strategic priorities during the reporting period. [s. 27(4)]

(1B) In subsection (1A), "the reporting period" means the period to which the report relates. [s. 27(4)]

(2) ~~The report must include the annual report required under Article 59 of the UK GDPR.~~ [sch 9. para 18]

(2A) The report under this section may include the annual report under section 161A. [s. 38(2)]

(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.

139A Analysis of performance

(1) The Commissioner must prepare and publish an analysis of the Commissioner's performance using key performance indicators.

(2) The analysis must be prepared and published at least annually.

(3) In this section, "key performance indicators" means factors by reference to which the Commissioner's performance can be measured most effectively.

Documents and notices [s. 33]

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

Information notices

142. Information notices

(1) The Commissioner may, by written notice (an "information notice")—

(a) require a controller or processor to provide the Commissioner with information or documents that the Commissioner reasonably requires for the purposes of carrying out the Commissioner's functions under the data protection legislation, or

(b) require any person to provide the Commissioner with information or documents that the Commissioner reasonably requires for the purposes of—

(i) investigating a suspected failure of a type described in section 149(2) or a suspected offence under this Act, or

(ii) determining whether the processing of personal data is carried out by an individual in the course of a purely personal or household activity.

(2) An information notice must state—

(a) whether it is given under subsection (1)(a), (b)(i) or (b)(ii), and

(b) why the Commissioner requires the information or documents.

(3) An information notice—

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

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

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

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

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

(4) An information notice must provide information about—

(a) the consequences of failure to comply with it, and

(b) the rights under sections 162 and 164 (appeals etc).

(5) An information notice may not require a person to provide information or documents 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 or documents 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 or documents are ~~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 or documents to be provided before the end of the period of 24 hours beginning when the notice is given. [s. 34(2)]

(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 UK GDPR, the reference to a controller or processor includes a representative of a controller or processor designated under Article 27 of the UK GDPR (representatives of controllers or processors not established in the United Kingdom).~~ [s. 13(3)(a)]

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

143. 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 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 or documents are ~~is~~ required for the purposes of making such a determination.

(2) An information notice does not require a person to give the Commissioner information or documents 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 or documents to the extent that requiring the person to do so would result in the disclosure ~~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 or documents to the extent that requiring the person to do so would result in the disclosure ~~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 or documents if doing so would, by revealing evidence of the commission of an offence expose the person to proceedings for that offence. [s. 34(3)]

(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 144) 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 UK 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.~~ [s. 13(3)(b)]

144. False statements made in response to information notices

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.

145. Information orders

(1) This section applies if, on an application by the Commissioner, a court is satisfied that a person has failed to comply with a requirement of an information notice.

(2) The court may make an order requiring the person to provide to the Commissioner some or all of the following—

(a) Information or documents referred to in the information notice;

(b) other information or documents which the court is satisfied the Commissioner requires, having regard to the statement included in the notice in accordance with section 142(2)(b).

(3) The order—

(a) may specify the form in which the information or documents must be provided,

(b) must specify the time at which, or the period within which, the information or documents must be provided, and

(c) may specify the place where the information or documents must be provided.

[s. 34(4)]

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 a copy (in such form as may be requested) of—

(i) the documents to which the Commissioner is directed;

(ii) 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) provide the Commissioner with an explanation of such documents, information, equipment or material;

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

(i) 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.

(j) make arrangements for an approved person to prepare a report on a specified matter;

(k) provide to the Commissioner a report prepared in pursuance of such arrangements. [s. 35(2)(a)]

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

(3A) An assessment notice that requires a controller or processor to make arrangements for an approved person to prepare a report may require the arrangements to include specified terms as to—

(a) the preparation of the report;

(b) the contents of the report;

(c) the form in which the report is to be provided;

(d) the date by which the report is to be completed. [s. 35(2)(b)]

(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 (9)).

(5) An assessment notice must provide information about—

(a) the consequences of failure to comply with it, and

(b) the rights under sections 162 and 164 (appeals etc).

(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,

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

(c) does not meet the conditions in subsection (9)(a) to (d),

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 when the notice is given.

(9) If an assessment notice—

(a) states that, in the Commissioner's opinion, there are reasonable grounds for suspecting that a controller or processor has failed or is failing as described in section 149(2) or that an offence under this Act has been or is being committed,

(b) indicates the nature of the suspected failure or offence,

(c) does not specify domestic premises,

(d) states that, in the Commissioner's opinion, it is necessary for the controller or processor to comply with a requirement in the notice in less than 7 days, and

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

subsections (6) and (7) do not apply.

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

(11) 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.

(11A) Where the Commissioner gives an assessment notice that requires the controller or processor to make arrangements for an approved person to prepare a report, the controller or processor is liable for the payment of the approved person's remuneration and expenses under the arrangements. [s. 35(2)(c)]

(12) In this section—

"approved person", in relation to a report, means a person approved to prepare the report in accordance with section 146A; [s. 35(2)(d)]

"domestic premises" means premises, or a part of premises, used as a dwelling;

"specified" means specified in an assessment notice.

146A Assessment notices: approval of person to prepare report etc

(1) This section applies where an assessment notice requires a controller or processor to make arrangements for an approved person to prepare a report.

(2) The controller or processor must, within such period as is specified in the assessment notice, nominate to the Commissioner a person to prepare the report.

(3) If the Commissioner is satisfied that the nominated person is a suitable person to prepare the report, the Commissioner must by written notice to the controller or processor approve the nominated person to prepare the report.

(4) If the Commissioner is not satisfied that the nominated person is a suitable person to prepare the report, the Commissioner must by written notice to the controller or processor—

(a) inform the controller or processor that the Commissioner has decided not to approve the nominated person to prepare the report,

(b) inform the controller or processor of the reasons for that decision, and

(c) approve a person who the Commissioner is satisfied is a suitable person to prepare the report to do so.

(5) If the controller or processor does not nominate a person within the period specified in the assessment notice, the Commissioner must by written notice to the controller or processor approve a person who the Commissioner is satisfied is a suitable person to prepare the report to do so.

(6) It is the duty of the controller or processor to give the person approved to prepare the report all such assistance as the person may reasonably require to prepare the report. [s. 35(3)]

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.

Information notices and assessment notices: destruction of documents etc

148. Destroying or falsifying information and documents etc

(1) This section applies where a person—

(a) has been given an information notice requiring the person to provide the Commissioner with information or a document, or [s. 34(5)]

(b) has been given an assessment notice requiring the person to direct the Commissioner to a document, equipment or other material or to assist the Commissioner to view information.

(2) It is an offence for the person—

(a) to destroy or otherwise dispose of, conceal, block or (where relevant) falsify all or part of the information, document, equipment or material, or

(b) to cause or permit the destruction, disposal, concealment, blocking or (where relevant) falsification of all or part of the information, document, equipment or material,

with the intention of preventing the Commissioner from viewing, or being provided with or directed to, all or part of the information, document, equipment or material.

(3) It is a defence for a person charged with an offence under subsection (2) to prove that the destruction, disposal, concealment, blocking or falsification would have occurred in the absence of the person being given the notice.

Interview notices

148A Interview notices

(1) This section applies where the Commissioner suspects that a controller or processor—

(a) has failed or is failing as described in section 149(2), or

(b) has committed or is committing an offence under this Act.

(2) For the purpose of investigating the suspected failure or offence, the Commissioner may, by written notice (an "interview notice"), require an individual within subsection (3) to—

(a) attend at a place specified in the notice, and

(b) answer questions with respect to any matter relevant to the investigation.

(3) An individual is within this subsection if the individual—

(a) is the controller or processor,

(b) is or was at any time employed by, or otherwise working for, the controller or

(c) is or was at any time concerned in the management or control of the controller or processor.

(4) An interview notice must specify the time at which the individual must attend at the specified place and answer questions (but see the restrictions in subsections (6) and (7)).

(5) An interview notice must—

(a) indicate the nature of the suspected failure or offence that is the subject of the investigation,

(b) provide information about the consequences of failure to comply with the notice, and

(c) provide information about the rights under sections 162 and 164 (appeals etc).

(6) An interview notice may not require an individual to attend at the specified place and answer questions before the end of the period within which an appeal can be brought against the notice.

(7) If an appeal is brought against an interview notice, the individual to whom the notice is given need not attend at the specified place and answer questions pending the determination or withdrawal of the appeal.

(8) If an interview notice—

(a) states that, in the Commissioner's opinion, it is necessary for the individual to attend at the specified place and answer questions 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 individual to attend at the specified place and answer questions before the end of the period of 24 hours beginning when the notice is given.

(9) The Commissioner may cancel or vary an interview notice by written notice to the individual to whom it was given. [s. 36(2)]

148B Interview notices: restrictions

(1) An interview notice does not require an individual to answer questions to the extent that requiring the person to do so would involve an infringement of the privileges of either House of Parliament.

(2) An interview notice does not require an individual to answer questions 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 of obligations, liabilities or rights under the data protection legislation.

(3) An interview notice does not require an individual to answer questions 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.

(4) In subsections (2) and (3), references to the client of a professional legal adviser include references to a person acting on behalf of the client.

(5) An interview notice does not require an individual to answer questions if doing so would, by revealing evidence of the commission of an offence, expose the individual to proceedings for that offence.

(6) The reference to an offence in subsection (5) 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).

(7) A statement made by an individual in response to an interview notice may not be used in evidence against that individual on a prosecution for an offence under this Act (other than an offence under section 148C) unless in the proceedings—

(a) in giving evidence the individual 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 individual or on that individual's behalf.

(8) The Commissioner may not give an interview notice with respect to the processing of personal data for the special purposes.

(9) The Commissioner may not give an interview notice to an individual for the purpose of investigating a suspected failure or offence if the controller or processor suspected of the failure or offence is—

(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 His Majesty's Chief Inspector of Education, Children's Services and Skills by virtue of section 5(1)(a) of the Care Standards Act 2000.

148C False statements made in response to interview notices

It is an offence for an individual, in response to an interview notice—

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

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

[s. 36(2)]

Enforcement notices

149. 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) or (5A), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person— [sch. 8 para 19(2)]

(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 150 and 151).

(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 UK GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);

(b) a provision of or made under Articles 12 to 22D of the UK GDPR or Part 3 or 4 of this Act conferring rights on a data subject; [sch. 3 para 16]

(c) a provision of Articles 25 to 35 ~~39~~ of the UK GDPR or section 64 ~~or 65~~ of this Act (obligations of controllers and processors); [sch. 4 para 19]

(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 44A to 49A of the UK GDPR or in sections 73 to 78 or 109 of this Act. [sch. 7 para 18]

(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 UK 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 UK GDPR (certification of controllers and processors), or

(c) has failed, or is failing, to comply with any other provision of the UK 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.

(5A) The fifth type of failure is where a controller has failed, or is failing, to comply with section 164A or with regulations under section 164B. [sch. 8 para 19(3)]

(6) An enforcement notice given in reliance on subsection (2), (3) ~~or~~ (5) or (5A) may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure. [sch. 8 para 19(4)]

(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 an enforcement notice in respect of the failure, including by amending this section and sections 150 to 152,

(b) may make provision about the giving of an information notice, an assessment notice, an interview notice or a penalty notice, or about powers of entry and inspection, in connection with the failure, including by amending sections 142, 143, 146, 147, 148A, 148B and 155 to 157 and Schedules 15 and 16, and [s. 36(3)]

(c) are subject to the affirmative resolution procedure.

150. 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 149(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 149(2), the Commissioner's power under section 149(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—

(a) the consequences of failure to comply with it, and

(b) the rights under sections 162 and 164 (appeals etc).

(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 24 hours beginning when the notice is given.

(9) In this section, "specified" means specified in an enforcement notice.

151. 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 UK 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 UK GDPR,

(b) section 38(1) of this Act, or

(c) section 89 of this Act.

152. Enforcement notices: restrictions

(1) The Commissioner may not give a controller or processor an enforcement notice in reliance on section 149(2) with respect to the processing of personal data for the special purposes unless—

(a) a determination under section 174 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 149(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 149(2) if the controller is responsible for compliance with the provision, requirement or principle in question.

153. 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

154. Powers of entry and inspection

Schedule 15 makes provision about powers of entry and inspection.

Penalties

155. Penalty notices

(1) If the Commissioner is satisfied that a person—

(a) has failed or is failing as described in section 149(2), (3), (4), ~~or~~ (5) or (5A) [sch. 8 para 20], ~~or~~

(b) has failed to comply with an information notice, an assessment notice, an interview notice or an enforcement notice, or

(c) has failed to comply with a duty imposed on the person by section 146A(6).

[s. 35(4)]

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) 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 UK GDPR applies, the matters listed in Article 83(1) and (2) of the UK 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, including any consultation under section 65;

(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; [sch. 4 para 20]

(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 149(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 156 to 158, 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 157.

156. Penalty notices: restrictions

(1) The Commissioner may not give a controller or processor a penalty notice in reliance on section 149(2) with respect to the processing of personal data for the special purposes unless—

(a) a determination under section 174 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 149(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 209(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 149(2) if the controller is responsible for compliance with the provision, requirement or principle in question.

157. Maximum amount of penalty

(1) In relation to an infringement of a provision of the UK 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 UK 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~~ 50B, 50C, 52, 53, 73, 75, 76, 77 or 78, the higher maximum amount, and [sch. 3 para 16]

(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, an interview notice or an enforcement notice, the maximum amount of the penalty that may be imposed by a penalty notice is the higher maximum amount. [s. 36(5)]

(4A) In relation to an infringement of section 164A or of regulations under section 164B, the maximum amount of the penalty that may be imposed by a penalty notice is the standard maximum amount. [sch. 8 para 21]

(5) The "higher maximum amount" is—

(a) in the case of an undertaking, £17,500,000 or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or

(b) in any other case, £17,500,000.

(6) The "standard maximum amount" is—

(a) in the case of an undertaking, £8,700,000 or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or

(b) in any other case, £8,700,000.

158. 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.

(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 Commissioner 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.

159. Amount of penalties: supplementary

(1) For the purposes of Article 83 of the UK GDPR and section 157, 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 UK GDPR, section 157 and section 158, 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 and report [s. 38(3)]

160. 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) information notices,

(b) assessment notices,

(ba) interview notices, [s. 36(6)(a)]

(c) enforcement notices, and

(d) 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 information notices, the guidance must include—

(a) provision specifying factors to be considered in determining the time at which, or the period within which, information or documents are ~~is~~ to be required to be provided; [s. 34(6)]

(b) provision about the circumstances in which the Commissioner would consider it appropriate to give an information notice to a person in reliance on section 142(7) (urgent cases);

(c) provision about how the Commissioner will determine how to proceed if a person does not comply with an information notice.

(4) 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;

(aa) provision specifying factors to be considered in determining whether to give an assessment notice to a person that imposes a requirement of a sort mentioned in section 146(2)(j);

(ab) provision about the factors the Commissioner may take into account when determining the suitability of a person to prepare a report of a sort mentioned in section 146(2)(j) or (k); [s. 35(5)]

(b) provision about the circumstances in which the Commissioner would consider it appropriate to give an assessment notice in reliance on section 146(8) or (9) (urgent cases);

(c) 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;

(d) provision about the nature of inspections and examinations carried out in accordance with an assessment notice;

(e) provision about the nature of interviews carried out in accordance with an assessment notice;

(f) 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;

(g) provision about how the Commissioner will determine how to proceed if a person does not comply with an assessment notice.

(5) The guidance produced in accordance with subsection (4)(c) 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.

(5A) In relation to interview notices, the guidance must include—

(a) provision specifying factors to be considered in determining whether to give an interview notice to an individual;

(b) provision about the circumstances in which the Commissioner would consider it appropriate to give an interview notice to an individual in reliance on section 148A(8) (urgent cases);

(c) provision about the circumstances in which the Commissioner would consider it appropriate to vary the place or time specified in an interview notice at the request of the individual to whom the notice is given;

(d) provision about the nature of interviews carried out in accordance with an interview notice(e) provision about how the Commissioner will determine how to proceed if an individual does not comply with an interview notice. [s. 36(6)(b)]

(6) In relation to enforcement notices, the guidance must include—

(a) provision specifying factors to be considered in determining whether to give an enforcement notice to a person;

(b) provision about the circumstances in which the Commissioner would consider it appropriate to give an enforcement notice to a person in reliance on section 150(8) (urgent cases);

(c) provision about how the Commissioner will determine how to proceed if a person does not comply with an enforcement notice.

(7) 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 person to make oral representations about the Commissioner's intention to give the person a penalty notice;

(c) provision explaining how the Commissioner will determine the amount of penalties;

(d) provision about how the Commissioner will determine how to proceed if a person does not comply with a penalty notice.

(e) provision about the circumstances in which the Commissioner would consider it necessary to comply with the duty in paragraph 4(B1) of Schedule 16 after the period of 6 months mentioned in that paragraph. [s. 37(4)]

(8) The Commissioner—

(a) may alter or replace guidance produced under this section, and

(b) must publish any altered or replacement guidance.

(9) 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 Commissioner considers appropriate.

(10) Section 161 applies in relation to the first guidance under subsection (1).

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

(12) 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).

161. Approval of first guidance about regulatory action

(1) When the first guidance is produced under section 160(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 whole days that fall within a period during which Parliament is dissolved or prorogued or during which both Houses of Parliament are adjourned for more than 4 days. [sch 9. para 19]

161A Annual report on regulatory action

(1) The Commissioner must produce and publish an annual report on containing the information described in subsections (2) to (5).

(2) The report must include the following information about UK GDPR investigations—

(a) the number of investigations begun, continued or completed by the Commissioner during the reporting period,

(b) the different types of act and omission that were the subject matter of the investigations,

(c) the enforcement powers exercised by the Commissioner in the reporting period in connection with the investigations,

(d) the duration of investigations that ended in the reporting period, and

(e) the different types of outcome in investigations that ended in that period.

(3) The report must include information about the enforcement powers exercised by the Commissioner in the reporting period in connection with—

(a) processing of personal data by a competent authority for any of the law enforcement purposes, and

(b) processing of personal data to which Part 4 applies.

(4) The information included in the report in accordance with subsections (2) and (3) must include information about—

(a) the number of penalty notices given in the reporting period that were given more than 6 months after the notice of intent was given under paragraph 2 of Schedule 16, and

(b) the reasons why that happened.

(5) The report must include a review of how the Commissioner had regard to the guidance published under section 160 when exercising the Commissioner's enforcement powers as described in subsections (2)(c) and (3).

(6) In this section—

"enforcement powers" means the powers under—

(a) Article 58(1)(c) and (d) and (2)(a) and (b) of the UK GDPR,

(b) sections 142 to 159 of this Act,

(c) paragraph 2(a), (b) and (c) of Schedule 13 to this Act,

(d) Schedules 15 and 16 to this Act;

"the law enforcement purposes" has the meaning given in section 31 of this Act;

"the reporting period" means the period to which the report relates;

"UK GDPR investigation" means an investigation required under Article 57(1)(h) of the UK GDPR (investigations on the application of the UK GDPR). [s. 38(4)]

Appeals etc

162. 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;

(ba) an interview notice; [s. 36(7)]

(c) an enforcement notice;

(d) a penalty notice;

(e) a penalty variation notice.

(2) A person who is given an enforcement notice may appeal to the Tribunal against the refusal of an application under section 153 for the cancellation or variation of the notice.

(3) A person who is given a penalty notice or a penalty variation notice may appeal to the Tribunal against the amount of the penalty specified in the notice, whether or not the person appeals against the notice.

(4) Where a determination is made under section 174 in respect of the processing of personal data, the controller or processor may appeal to the Tribunal against the determination.

163. Determination of appeals

(1) Subsections (2) to (4) apply where a person appeals to the Tribunal under section 162(1) or (3).

(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 162(2), 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.

(6) On an appeal under section 162(4), the Tribunal may cancel the Commissioner's determination.

164. Applications in respect of urgent notices

(1) This section applies where an information notice, an assessment notice, an interview notice or an enforcement notice given to a person contains an urgency statement. [s. 36(8)(a)]

(2) The person may apply to the court for either or both of the following—

(a) the disapplication of the urgency statement in relation to some or all of the requirements of the notice;

(b) a change to the time at which, or the period within which, a requirement of the notice must be complied with.

(3) On an application under subsection (2), the court may do any of the following—

(a) direct that the notice is to have effect as if it did not contain the urgency statement;

(b) direct that the inclusion of the urgency statement is not to have effect in relation to a requirement of the notice;

(c) vary the notice by changing the time at which, or the period within which, a requirement of the notice must be complied with;

(d) vary the notice by making other changes required to give effect to a direction under paragraph (a) or (b) or in consequence of a variation under paragraph (c).

(4) The decision of the court on an application under this section is final.

(5) In this section, "urgency statement" means—

(a) in relation to an information notice, a statement under section 142(7)(a),

(b) in relation to an assessment notice, a statement under section 146(8)(a) or (9)(d),

(ba) in relation to an interview notice, a statement under section 148A(8)(a), and [s. 36(8)(b)]

(c) in relation to an enforcement notice, a statement under section 150(8)(a).

Complaints

164A Complaints by data subjects to controllers

(1) A data subject may make a complaint to the controller if the data subject considers that, in connection with personal data relating to the data subject, there is an infringement of the UK GDPR or Part 3 of this Act.

(2) A controller must facilitate the making of complaints under this section by taking steps such as providing a complaint form which can be completed electronically and by other means.

(3) If a controller receives a complaint under this section, the controller must acknowledge receipt of the complaint within the period of 30 days beginning with the day on which it is received.

(4) If a controller receives a complaint under this section, the controller must without undue delay—

(a) take appropriate steps to respond to the complaint, and

(b) inform the complainant of the outcome of the complaint.

(5) The reference in subsection (4)(a) to taking appropriate steps to respond to the complaint includes—

(a) making enquiries into the subject matter of the complaint, to the extent appropriate, and

(b) informing the complainant about progress on the complaint.

164B Controllers to notify the Commissioner of the number of complaints

(1) The Secretary of State may by regulations require a controller to notify the Commissioner of the number of complaints made to the controller under section 164A in periods specified or described in the regulations.

(2) Regulations under this section may provide that a controller is required to make a notification to the Commissioner in respect of a period only in circumstances specified in the regulations.

(3) Regulations under this section may include—

(a) provision about a matter listed in subsection (4), or

(b) provision conferring power on the Commissioner to determine those matters.

(4) The matters are—

(a) the form and manner in which a notification must be made,

(b) the time at which, or period within which a notification must be made, and

(c) how the number of complaints made to a controller during a period is to be calculated.

(5) Regulations under this section are subject to the negative resolution procedure. [s. 39(2)]

165. Complaints by data subjects to the Commissioner [sch. 8 para 22]

(1) ~~Articles 57(1)(f) and 2) and 77 of the UK GDPR (data subjects 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 UK GDPR.~~ -[s. 40(2)(a)]

(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 the UK GDPR or Part 3 or 4 of this Act. [s. 40(2)(b)]

(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 166, 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 a foreign designated authority is necessary.

(5A) Subsection (4) does not apply if the Commissioner refuses to act on the complaint in reliance on section 165A. [s. 40(2)(c)]

(6) . . . . . .

(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;

165A Power of Commissioner to refuse to act on certain complaints

(1) The Commissioner may refuse to act on a complaint under section 165 if condition A, B or C is met.

(2) Condition A is that—

(a) the complaint concerns an infringement of the UK GDPR or Part 3 of this Act, and

(b) the complaint has not been made to the controller under section 164A.

(3) Condition B is that—

(a) the complaint has been made to the controller under section 164A,

(b) the controller has not finished handling the complaint in accordance with subsection (4) of that section, and

(c) the period of 45 days beginning with the day the complaint was made to the controller under that section has not expired.

(4) Condition C is that the complaint is vexatious or excessive (see section 204A).

(5) In any proceedings where there is an issue as to whether a complaint is vexatious or excessive, it is for the Commissioner to show that it is.

(6) If the Commissioner refuses to act on a complaint under section 165, the Commissioner must inform the complainant of—

(a) the refusal and the reasons for it, and

(b) the right under section 166A.

(7) If the Commissioner refuses to act on a complaint under section 165 that does not prevent the complainant making the complaint again. [s. 40(3)]

165B Guidance about responding to complaints and refusing to act

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

(a) how the Commissioner proposes to respond to complaints made under section 165, and

(b) how the Commissioner proposes to exercise the discretion conferred by section 165A to refuse to act on a complaint.

(2) The Commissioner—

(a) may alter or replace guidance produced under this section, and

(b) must publish any altered or replacement guidance.

(3) 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 Commissioner considers appropriate.

(4) The Commissioner must arrange for any guidance under this section (including any altered or replacement guidance) to be laid before Parliament. [s. 40(3)]

166. Orders to progress complaints to the Commissioner

(1) This section applies where, after a data subject makes a complaint under section 165 ~~or Article 77 of the UK GDPR~~, the Commissioner— [sch. 8 para 23]

(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 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.

(1A) But this section does not apply if the Commissioner refuses to act on the complaint in reliance on section 165A. [s. 40(4)]

(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 165(5) applies for the purposes of subsections (1)(a) and (2)(a) as it applies for the purposes of section 165(4)(a).

166A Appeals against refusal of Commissioner to act on complaint

(1) Where the Commissioner refuses to act on a complaint in reliance on section 165A, the person who made the complaint may appeal to the Tribunal.

(2) The Tribunal may review any determination of fact on which the refusal to act was based.

(3) If the Tribunal considers—

(a) that the refusal to act is not in accordance with the law, or

(b) that the Commissioner ought not to have exercised the discretion to refuse to act,

the Tribunal must allow the appeal.

(4) Otherwise, the Tribunal must dismiss the appeal. [s. 40(5)]

Remedies in the court

167. 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 UK 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.

168. Compensation for contravention of the UK GDPR

(1) In Article 82 of the UK 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 UK 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.

169. 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 UK 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.

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 UK 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—

(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).

(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 **F230**UK 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, 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 to data subject

(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 UK GDPR (right of access by the data subject);

(b) Article 20 of the UK 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 167 (including proceedings on an application under Article 79 of the UK GDPR), or

(b) proceedings under Article 82 of the UK GDPR or section 169.

(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 162.

(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 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.

177. Guidance about how to seek redress against media organisations

(1) The Commissioner must produce and publish guidance about the steps that may be taken where an individual considers that a media organisation is failing or has failed to comply with the data protection legislation.

(2) In this section, "media organisation" means a body or other organisation whose activities consist of or include journalism.

(3) The guidance must include provision about relevant complaints procedures, including—

(a) who runs them,

(b) what can be complained about, and

(c) how to make a complaint.

(4) For the purposes of subsection (3), relevant complaints procedures include procedures for making complaints to the Commissioner, the Office of Communications, the British Broadcasting Corporation and other persons who produce or enforce codes of practice for media organisations.

(5) The guidance must also include provision about—

(a) the powers available to the Commissioner in relation to a failure to comply with the data protection legislation,

(b) when a claim in respect of such a failure may be made before a court and how to make such a claim,

(c) alternative dispute resolution procedures,

(d) the rights of bodies and other organisations to make complaints and claims on behalf of data subjects, and

(e) the Commissioner's power to provide assistance in special purpose proceedings.

(6) The Commissioner—

(a) may alter or replace the guidance, and

(b) must publish any altered or replacement guidance.

(7) The Commissioner must produce and publish the first guidance under this section before the end of the period of 1 year beginning when this Act is passed.

178. Review of processing of personal data for the purposes of journalism

(1) The Commissioner must—

(a) review the extent to which, during each review period, the processing of personal data for the purposes of journalism complied with—

(i) the data protection legislation, and

(ii) good practice in the processing of personal data for the purposes of journalism,

(b) prepare a report of the review, and

(c) submit the report to the Secretary of State.

(2) In this section—

"good practice in the processing of personal data for the purposes of journalism" has the same meaning as in section 124;

"review period" means—

(a) the period of 4 years beginning with the day on which Chapter 2 of Part 2 of this Act comes into force, and
(b) each subsequent period of 5 years beginning with the day after the day on which the previous review period ended.

(3) The Commissioner must start a review under this section, in respect of a review period, within the period of 6 months beginning when the review period ends.

(4) The Commissioner must submit the report of a review under this section to the Secretary of State—

(a) in the case of the first review, before the end of the period of 18 months beginning when the Commissioner started the review, and

(b) in the case of each subsequent review, before the end of the period of 12 months beginning when the Commissioner started the review.

(5) The report must include consideration of the extent of compliance (as described in subsection (1)(a)) in each part of the United Kingdom.

(6) The Secretary of State must—

(a) lay the report before Parliament, and

(b) send a copy of the report to—

(i) the Scottish Ministers,

(ii) the Welsh Ministers, and

(iii) the Executive Office in Northern Ireland.

(7) Schedule 17 makes further provision for the purposes of a review under this section.

179. Effectiveness of the media's dispute resolution procedures

(1) The Secretary of State must, before the end of each review period, lay before Parliament a report produced by the Secretary of State or an appropriate person on—

(a) the use of relevant alternative dispute resolution procedures, during that period, in cases involving a failure, or alleged failure, by a relevant media organisation to comply with the data protection legislation, and

(b) the effectiveness of those procedures in such cases.

(2) In this section—

"appropriate person" means a person who the Secretary of State considers has appropriate experience and skills to produce a report described in subsection (1);

"relevant alternative dispute resolution procedures" means alternative dispute resolution procedures provided by persons who produce or enforce codes of practice for relevant media organisations;

"relevant media organisation" means a body or other organisation whose activities consist of or include journalism, other than a broadcaster;

"review period" means—

(a) the period of 3 years beginning when this Act is passed, and
(b) each subsequent period of 3 years.

(3) The Secretary of State must send a copy of the report to—

(a) the Scottish Ministers,

(b) the Welsh Ministers, and

(c) the Executive Office in Northern Ireland.

Jurisdiction of courts

180. 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 subsections (3) and (4).

(2) Those provisions are—

(a) section 145 (information orders);

(b) section 152 (enforcement notices and processing for the special purposes);

(c) section 156 (penalty notices and processing for the special purposes);

(d) section 167 and Article 79 of the UK GDPR (compliance orders);

(e) sections 168 and 169 and Article 82 of the UK GDPR (compensation).

(3) In relation to the processing of personal data to which Part 4 applies, the jurisdiction conferred by the provisions listed in subsection (2) is exercisable only by the High Court or, in Scotland, the Court of Session.

(4) In relation to an information notice which contains a statement under section 142(7), the jurisdiction conferred on a court by section 145 is exercisable only by the High Court or, in Scotland, the Court of Session.

(5) The jurisdiction conferred on a court by section 164 (applications in respect of urgent notices) is exercisable only by the High Court or, in Scotland, the Court of Session.

Definitions

181. Interpretation of Part 6

In this Part—

"assessment notice" has the meaning given in section 146;

"certification provider" has the meaning given in section 17;

"enforcement notice" has the meaning given in section 149;

"information notice" has the meaning given in section 142;

"interview notice" has the meaning given in section 148A [s. 36(9)]

"penalty notice" has the meaning given in section 155;

"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 UK GDPR to represent the controller or processor with regard to the controller's or processor's obligations under the UK GDPR.~~ [s. 13(3)(c)]

PART 7 SUPPLEMENTARY AND FINAL PROVISION

Regulations under this Act

182. 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) . . . . . .

(b) section 30;

(c) section 211;

(d) section 212;

(e) section 213;

(f) paragraph 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.~~ [sch. 7 para 19(2)]

(5) Regulations under this Act may—

(a) make different provision for different purposes;

(b) include consequential, supplementary, incidental, transitional, transitory or saving provision.

(6) For the purposes of this Act, 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. [sch. 7 para 19(3)]

(7) For the purposes of this Act, 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. [sch. 7 para 19(4)]

(8) For the purposes of this Act, ~~where~~ regulations ~~under this Act~~ are subject to "the made affirmative resolution procedure" if—

(a) the statutory instrument containing the regulations must be laid before Parliament after being made, together with an ~~the~~ urgency statement in respect of them, and

(b) the regulations cease to have effect at the end of a period ~~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.

[sch. 7 para 19(5)]

(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.~~ [sch. 7 para 19(6)]

(11) Any provision that may be included in regulations under this Act subject to the negative resolution procedure may be made by regulations made under this Act or another enactment that are subject to the affirmative resolution procedure or the made affirmative resolution procedure. [sch. 7 para 19(7)]

(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) For the purposes of this section, an urgency statement is a reasoned statement that the Secretary of State considers it desirable for regulations to come into force without delay. ~~In this section, "urgency statement" has the meaning given in section 18(4).~~ [sch. 7 para 19(8)]

Changes to the Data Protection Convention

183. 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 relevant processing of personal data, 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.

(2A) In subsection (2)(d), "relevant processing of personal data" means—

(a) processing of personal data described in Article 2(1)(a) or (b) or (1A) of the UK GDPR, and

(b) processing of personal data to which Part 4 of this Act applies.

(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.

Prohibitions and restrictions on processing personal data

183A Protection of prohibitions and restrictions etc on processing

(1) A relevant enactment or rule of law which imposes a duty, or confers a power, to process personal data does not override a requirement under the main data protection legislation relating to the processing of personal data.

(2) Subsection (1) does not apply –

(a) to a relevant enactment forming part of the main data protection legislation, or

(b) to the extent that an enactment makes express provision to the contrary referring to this section or to the main data protection legislation (or a provision of that legislation).

(3) Subsection (1) does not prevent a duty or power to process personal data from being taken into account for the purpose of determining whether it is possible to rely on an exception to a requirement under the main data protection legislation that is available where there is such a duty or power.

(4) In this section —

"the main data protection legislation" means the data protection legislation other than provision of or made under—

(a) Chapter 6 or 8 of the UK GDPR, or

(b) Parts 5 to 7 of this Act;

"relevant enactment" means an enactment so far as passed or made on or after the day on which section 43 of the Data Protection and Digital Information Act 2023 comes into force,

"requirement" includes a prohibition or restriction.

(5) The reference in subsection (1) to an enactment or rule of law which imposes a duty, or confers a power, to process personal data is a reference to an enactment or rule of law which, directly or indirectly, requires or authorises the processing of personal data, including (for example)—

(a) by authorising one person to require another person to process personal data, or
(b) by removing restrictions on processing personal data, and the references in subsection (3) to a duty or power are to be read accordingly." [s. 43(2)]

Rights of the data subject

184. 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, investigation or detection of crime, given Part 5 of the Police Act 1997 (certificates of criminal records etc). [sch 9. para 20]

(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 18 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.

185. 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 UK GDPR (right of access by the data subject);

(b) Article 20 of the UK 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).

186. ~~Data subject's rights and other prohibitions and restrictions~~ Protection of data subject's rights [s. 43(3)(a)]

(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).~~ [s. 43(3)(b)]

(2A) Subsection (1) does not apply—

(a) to an enactment contained in, or made under, a provision falling within subsection (2) or (3), or

(b) to the extent that an enactment makes express provision to the contrary referring to this section or to a provision falling within subsection (2). [s. 43(3)(c)]

(2) The provisions providing obligations and rights are—

(a) Chapter III of the UK 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~~ further provisions referred to in subsection (2A)(a) 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 24, 25 and 26,

(c) ~~in Part 3 of this Act, sections 44(4), 45(4), 48(3) and 78A and 48(3)(ca) and in Part 3 of this Act, section 78A, and~~ [s. 43(3)(a)]

(ca) in Part 3 of this Act, section 78A, and [s. 24(11)]

(d) in Part 4 of this Act, Chapter 6 .

Representation of data subjects

187. Representation of data subjects with their authority

(1) In relation to the processing of personal data to which the UK GDPR applies, Article 80(1) of the UK GDPR (representation of data subjects)—

(a) enables a data subject to authorise a body or other organisation which meets the conditions set out in subsections (3) and (4) to exercise the data subject's rights under sections 164A and 165 (complaints) Articles ~~77~~, 78 and 79 of the UK GDPR (rights ~~to lodge complaints and~~ to an effective judicial remedy) on the data subject's behalf, and [sch. 8 para 24(2)]

(b) also authorises such a body or organisation to exercise the data subject's rights under Article 82 of the UK GDPR (right to compensation).

(2) In relation to the processing of personal data to which the UK 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 of a data subject on the data subject's behalf—

(za) the right under section 164A (complaints to the controller);

(a) rights under section 165~~(2) and (4)(d)~~ (complaints to the Commissioner); [sch. 8 para 24(3)]

(b) rights under section 166(2) (orders for the Commissioner to progress complaints);

(c) rights under section 167(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 UK GDPR or this section.

188. 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 UK GDPR or section 187.

(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.

189. 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) the operation of Article 80(1) of the UK GDPR,

(b) the operation of section 187,

(c) the merits of exercising the power under Article 80(2) of the UK GDPR (power to enable a body or other organisation which meets the conditions in Article 80(1) of the UK GDPR to exercise some or all of a data subject's rights under Articles 77, 78 and 79 of the UK GDPR without being authorised to do so by the data subject),

(d) the merits of making equivalent provision in relation to data subjects' rights under Article 82 of the UK GDPR (right to compensation), and

(e) the merits of making provision for a children's rights organisation to exercise some or all of a data subject's rights under Articles 77, 78, 79 and 82 of the **F255**UK GDPR on behalf of a data subject who is a child, with or without being authorised to do so by the data subject.

(3) "The review period" is the period of 30 months beginning when section 187 comes into force.

(4) In carrying out the review, the Secretary of State must—

(a) consider the particular needs of children separately from the needs of adults,

(b) have regard to the fact that children have different needs at different stages of development,

(c) carry out an analysis of the particular challenges that children face in authorising, and deciding whether to authorise, other persons to act on their behalf under Article 80(1) of the UK GDPR or section 187,

(d) consider the support and advice available to children in connection with the exercise of their rights under Articles 77, 78, 79 and 82 of the UK GDPR by another person on their behalf and the merits of making available other support or advice, and

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

(5) Before preparing the report under subsection (1), the Secretary of State must consult the Commissioner and such other persons as the Secretary of State considers appropriate, including—

(a) persons active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data,

(b) children and parents,

(c) children's rights organisations and other persons who appear to the Secretary of State to represent the interests of children,

(d) child development experts, and

(e) trade associations.

(6) In this section—

"children's rights organisation" means a body or other organisation which—

(a) is active in representing the interests of children, and
(b) has objectives which are in the public interest;

"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.

190. Post-review powers to make provision about representation of data subjects

(1) After the report under section 189(1) is laid before Parliament, the Secretary of State may by regulations—

(a) exercise the powers under Article 80(2) of the UK GDPR in relation to England and Wales and Northern Ireland,

(b) make provision enabling a body or other organisation which meets the conditions in Article 80(1) of the UK GDPR to exercise a data subject's rights under Article 82 of the UK GDPR in England and Wales and Northern Ireland without being authorised to do so by the data subject, and

(c) make provision described in section 189(2)(e) in relation to the exercise in England and Wales and Northern Ireland of the rights of a data subject who is a child.

(2) The powers under subsection (1) 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 166 to 168, 180, 187, 203, 205 and 206;

(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.

(3) The powers under subsection (1)(a) and (b) include power to make provision in relation to data subjects who are children or data subjects who are not children or both.

(4) The provision mentioned in subsection (2)(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.

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

Framework for Data Processing by Government

191. 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.

192. Approval of the Framework

(1) Before issuing a document prepared under section 191, 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 whole days that fall within a period during which Parliament is dissolved or prorogued or during which both Houses of Parliament are adjourned for more than 4 days. [sch 9. para 21]

(7) This section applies in relation to amendments prepared under section 191 as it applies in relation to a document prepared under that section.

193. Publication and review of the Framework

(1) The Secretary of State must publish a document issued under section 192(3).

(2) Where an amendment of a document is issued under section 192(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 192(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 191(4) with a view to remedying the situation.

194. Effect of the Framework

(1) When carrying out processing of personal data which is the subject of a document issued under section 192(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 192(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 192(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 192(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.

Data-sharing: HMRC and reserve forces

195. Reserve forces: data-sharing by HMRC

(1) The Reserve Forces Act 1996 is amended as follows.

(2) After section 125 insert—

"**125Asupply of contact details by HMRC**

(1)This subsection applies to contact details for—

(a)a member of an ex-regular reserve force, or

(b)a person to whom section 66 (officers and former servicemen liable to recall) applies,

which are held by HMRC in connection with a function of HMRC.

(2)HMRC may supply contact details to which subsection (1) applies to the Secretary of State for the purpose of enabling the Secretary of State—

(a)to contact a member of an ex-regular reserve force in connection with the person's liability, or potential liability, to be called out for service under Part 6;

(b)to contact a person to whom section 66 applies in connection with the person's liability, or potential liability, to be recalled for service under Part 7.

(3)Where a person's contact details are supplied under subsection (2) for a purpose described in that subsection, they may also be used for defence purposes connected with the person's service (whether past, present or future) in the reserve forces or regular services.

(4)In this section, "HMRC" means Her Majesty's Revenue and Customs.

125Bprohibition on disclosure of contact details supplied under section 125A

(1)A person who receives information supplied under section 125A may not disclose it except with the consent of the Commissioners for Her Majesty's Revenue and Customs (which may be general or specific).

(2)A person who contravenes subsection (1) is guilty of an offence.

(3)It is a defence for a person charged with an offence under this section to prove that the person reasonably believed—

(a)that the disclosure was lawful, or

(b)that the information had already lawfully been made available to the public.

(4)Subsections (4) to (7) of section 19 of the Commissioners for Revenue and Customs Act 2005 apply to an offence under this section as they apply to an offence under that section.

(5)Nothing in section 107 or 108 (institution of proceedings and evidence) applies in relation to an offence under this section.

125Cdata protection

(1)Nothing in section 125A or 125B authorises the making of a disclosure which contravenes the data protection legislation.

(2)In this section, "the data protection legislation" has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act)."

Offences

196. Penalties for offences

(1) A person who commits an offence under section 119 or 173 or paragraph 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, 144, 148, 148C, 170, 171 or 184 is liable— [s. 36(10)]

(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 or 184.

(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.

197. 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 (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.

198. 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.

199. 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;

(c) section 144;

(d) section 148;

(e) section 170;

(f) section 171;

(g) section 173;

(h) section 184;

(i) paragraph 15 of Schedule 15.

(2) Regulations under section 27(4) of the Police and Criminal Evidence Act 1984 (recordable offences) may repeal subsection (1).

200. 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

201. 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.

202. 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, 82E, 111 or 162, or [s. 26(7)]

(ii) for an order under section 166, 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.

203. 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, 82E, 111 or 162, and [s. 26(8)]

(b) the exercise of the rights of data subjects under section 166, 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.

Interpretation

204. 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 ... Professions Order 2001 (S.I. 2002/254) for the time being extends; ...

(h) a registered pharmacist or a registered pharmacy technician within the meaning of the Pharmacy Order 2010 (S.I. 2010/231) (see 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 the register maintained by Social Work England under section 39(1) of the Children and Social Work Act 2017;

(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)).

204A Vexatious or excessive

(1) For the purposes of this Act, whether a request is vexatious or excessive must be determined having regard to the circumstances of the request, including (so far as relevant)—

(a) the nature of the request,

(b) the relationship between the person making the request (the "sender") and the person receiving it (the "recipient"),

(c) the resources available to the recipient,

(d) the extent to which the request repeats a previous request made by the sender to the recipient,

(e) how long ago any previous request was made, and

(f) whether the request overlaps with other requests made by the sender to the recipient.

(1A) For the purposes of this Act, whether a complaint to the Commissioner is vexatious or excessive must be determined having regard to the circumstances of the complaint, including (so far as relevant)—

(a) the nature of the complaint,

(b) the complainant's relationship with the person who is the subject of the complaint ("the subject") and the Commissioner,

(c) the resources available to the Commissioner,

(d) the extent to which the complaint repeats a previous complaint made by the complainant to the subject or the Commissioner,

(e) how long ago any previous complaint was made, and

(f) whether the complaint overlaps with other complaints made by the complainant to the subject or the Commissioner. [s. 7(10)] and sch. 8 para 25(2)]

(2) For the purposes of this Act, examples of requests and complaints that may be vexatious include requests and complaints that— [s. 7(10)] and sch. 8 para 25(3)]

(a) are intended to cause distress,

(b) are not made in good faith, or

(c) are an abuse of process. [s. 7(10)]

205.

206. 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
(e) an enactment comprised in, or in an instrument made under, Northern Ireland legislation; and
(f) any retained direct EU 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 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) ...
(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.

(1A) In this Act, references to a fundamental right or fundamental freedom (however expressed) are to a fundamental right or fundamental freedom which continues to form part of domestic law on and after IP completion day by virtue of section 4 of the European Union (Withdrawal) Act 2018, as the right or freedom is amended or otherwise modified by the law of the United Kingdom, or of a part of the United Kingdom, from time to time on or after IP completion day.

(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—

(za) section 119A(10) and (11);

(a) section 125(4), (7) and (8);

(b) section 161(3), (5) and (6);

(c) section 176(2);

(d) section 178(2);

(e) section 182(8) ~~and (9);~~ [sch. 7 para 20]

(f) section 183(4);

(g) section 192(3), (5) and (6);

(h) section 197(3) and (4);

(i) paragraph 23(4) and (5) of Schedule 1;

(j) paragraphs 5(4) and 6(4) of Schedule 3;

(k) Schedule 5;

(l) paragraph 11(5) of Schedule 12;

(m) Schedule 15;

(and the references in section 5 to terms used in Part 2 do not include references to a period expressed in hours, days, weeks, months or years).

(3) . . . . . .

(4) In the definition of "the UK GDPR" in section 3(10)—

(a) the reference to Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 is to be treated as a reference to that Regulation as modified by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("the 2019 Regulations"), but

(b) nothing in the definition or in paragraph (a) determines whether, where Regulation (EU) 2016/679 is modified on or after IP completion day by the law of England and Wales, Scotland or Northern Ireland (other than by Schedule 1 to the 2019 Regulations), the reference to Regulation (EU) 2016/679 is then to be read as a reference to that Regulation as modified.

(5) Subsection (4) is not to be read as implying anything about how other references to Regulation (EU) 2016/679 or references to other retained EU law are to be interpreted.

207. 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 182	
assessment notice (in Part 6)	section 181	
biometric data	section 205	
certification provider (in Part 6)	section 181	
the Commission	section 3	[s. 100(4)]
~~the Commissioner~~	~~section 3~~	[s. 101(5)]
competent authority (in Parts 3 and 4)	sections 30 and 82	[s. 26(9)(a)]
consent (to processing of personal data) (in Parts 3 and 4)	sections 33, 40A and 84	[s. 4(5)]
controller	section 3	
data concerning health	section 205	
the Data Protection Convention	section 3	
the data protection legislation	section 3	
data subject	section 3	
designation notice (in Part 4)	section 84	[s. 26(9)(b)]
employee (in Parts 3 and 4)	sections 33 and 84	
enactment	section 205	
enforcement notice (in Part 6)	section 181	
excessive	section 204A	[s. 7(11)]
the EU GDPR	section 3	
filing system	section 3	
FOI public authority (in Chapter 3 of Part 2)	section 21	
genetic data	section 205	
government department	section 205	

health professional	section 204	
health record	section 205	
identifiable living individual	section 3	
inaccurate	section 205	
information notice (in Part 6)	section 181	
intelligence service (in Part 4)	section 82	
international obligation of the United Kingdom	section 205	
international organisation	section 205	
interview notice (in Part 6)	section 181	[s. 36(11)]
the Law Enforcement Directive	section 3	
the law enforcement purposes (in Part 3)	section 31	
the made affirmative resolution procedure	section 182	
Minister of the Crown	section 205	
the negative resolution procedure	section 182	
penalty notice (in Part 6)	section 181	
penalty variation notice (in Part 6)	section 181	
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 UK GDPR and Part 2)	section 7	
public body (in the UK GDPR and Part 2)	section 7	
publish	section 205	
qualifying competent authority (in Part 4)	section 82	[s. 26(9)(b)]
recipient (in Parts 3 and 4)	sections 33 and 84	
~~representative (in Part 6)~~	~~section 181~~	[s. 13(3)(d)]
representative body (in relation to a right of a data subject)	section 187	
restriction of processing (in Parts 3 and 4)	sections 33 and 84	
senior responsible individual (in Part 3)	section 33	[sch. 4 para 21]
social work professional	section 204	
the special purposes (in Part 6)	section 174	

special purposes proceedings (in Part 6)	section 174	
statement of strategic priorities (in Part 5)	section 120E	[s. 28(4)]
subordinate legislation	section 205	
third country (in Part 3)	section 33	
tribunal	section 205	
the Tribunal	section 205	
the UK GDPR	section 3	
vexatious	section 204A	[s. 7(11)]
withdrawal notice (in Part 4)	section 84	[s. 26(9)(b)]

Territorial application

208. Territorial application of this Act

(1) This Act applies only to processing of personal data described in subsections (1A) and (2).

(1A) In the case of the processing of personal data to which Part 2 (the UK GDPR) applies, it applies to the types of such processing to which the UK GDPR applies by virtue of Article 3 of the UK GDPR.

(2) In the case of the processing of personal data to which Part 2 does not apply, it applies where such processing is carried out 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) . . . . . .

(4) Subsections (1), (1A) and (2) have effect subject to any provision in or made under section 120 providing for the Commissioner to carry out functions in relation to other 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) . . . . . .

(7) In this section, references to a person 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), (b) or (c) who maintains, and carries on activities through, an office, branch or agency or other stable arrangements in the United Kingdom,

General

209. 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.

210. Application to the Crown

(1) This Act binds the Crown.

(2) For the purposes of the UK 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 UK 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 UK 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;

(c) section 171;

(d) section 173;

(e) paragraph 15 of Schedule 15.

211. 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 UK 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 UK 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;

(b) section 171;

(c) section 173;

(d) paragraph 15 of Schedule 15.

212. Minor and consequential provision

(1) In Schedule 19—

(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

213. Commencement

(1) Except as provided by subsections (2) and (3), 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) section 182;

(c) sections 204, 205 and 206;

(d) sections 209 and 210;

(e) sections 213(2), 214 and 215;

(f) 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) The following provisions come into force at the end of the period of 2 months beginning when this Act is passed—

(a) section 124;

(b) sections 125, 126 and 127, so far as they relate to a code prepared under section 124;

(c) section 177;

(d) section 178 and Schedule 17;

(e) section 179.

(4) Regulations under this section may make different provision for different areas.

214. Transitional provision

(1) Schedule 20 contains transitional, transitory and saving provision.

(2) 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 or with the EU

GDPR beginning to apply, including provision amending or repealing a provision of Schedule 20.

(3) Regulations under this section that amend or repeal a provision of Schedule 20 are subject to the negative resolution procedure.

(4) Schedule 21 contains further transitional, transitory and saving provision made in connection with the amendment of this Act and the UK GDPR by regulations under section 8 of the European Union (Withdrawal) Act 2018.

215. Extent

(1) This Act extends to England and Wales, Scotland and Northern Ireland, subject to—

(a) subsections (2) to (5), ~~and~~

(b) ~~paragraph 12 of Schedule 12.~~ [s. 101(6)]

(2) Section 199 extends to England and Wales only.

(3) Sections 188, 189 and 190 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.

(5) This subsection and the following provisions also extend to the Isle of Man—

(a) paragraphs 332 and 434 of Schedule 19;

(b) sections 211(1), 212(1) and 213(2), 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.

216. Short title

This Act may be cited as the Data Protection Act 2018.

SCHEDULES

Section 10

SCHEDULE 1 SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL CONVICTIONS ETC DATA

PART 1 CONDITIONS RELATING TO EMPLOYMENT, HEALTH AND RESEARCH ETC

Employment, social security and social protection

1.

(1) This condition is met if—

(a) the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection, and

(b) when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule).

(2) See also the additional safeguards in Part 4 of this Schedule.

(3) In this paragraph—

"social security" includes any of the branches of social security listed in Article 3(1) of Regulation (EC) No. 883/2004 of the European Parliament and of the Council on the co-ordination of social security systems (as amended from time to time);

"social protection" includes an intervention described in Article 2(b) of Regulation (EC) 458/2007 of the European Parliament and of the Council of 25 April 2007 on the European system of integrated social protection statistics (ESSPROS) as it had effect in EU law immediately before IP completion day.

Health or social care purposes

2.

(1) This condition is met if the processing is necessary for health or social care purposes.

(2) In this paragraph "health or social care purposes" means the purposes of—

(a) preventive or occupational medicine,

(b) the assessment of the working capacity of an employee,

(c) medical diagnosis,

(d) the provision of health care or treatment,

(e) the provision of social care, or

(f) the management of health care systems or services or social care systems or services.

(3) See also the conditions and safeguards in Article 9(3) of the UK GDPR (obligations of secrecy) and section 11(1).

Public health

3. This condition is met if the processing—

(a) is necessary for reasons of public interest in the area of public health, and

(b) is carried out—

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

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

Research etc

4. This condition is met if the processing—

(a) is necessary for archiving purposes, scientific or historical research purposes or statistical purposes,

(b) is carried out in accordance with Article 84B of the UK GDPR ~~89(1) of the UK GDPR (as supplemented by section 19)~~, and [s. 23(2)(b)]

(c) is in the public interest.

PART 2 SUBSTANTIAL PUBLIC INTEREST CONDITIONS

Requirement for an appropriate policy document when relying on conditions in this Part

5.

(1) Except as otherwise provided, a condition in this Part of this Schedule is met only if, when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule).

(2) See also the additional safeguards in Part 4 of this Schedule.

Statutory etc and government purposes

6.

(1) This condition is met if the processing—

(a) is necessary for a purpose listed in sub-paragraph (2), and

(b) is necessary for reasons of substantial public interest.

(2) Those purposes are—

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

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

Administration of justice and parliamentary purposes

7. This condition is met if the processing is necessary—

(a) for the administration of justice, or

(b) for the exercise of a function of either House of Parliament.

Equality of opportunity or treatment

8.

(1) This condition is met if the processing—

(a) is of a specified category of personal data, and

(b) is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained,

subject to the exceptions in sub-paragraphs (3) to (5).

(2) In sub-paragraph (1), "specified" means specified in the following table—

Category of personal data	***Groups of people (in relation to a category of personal data)***
Personal data revealing racial or ethnic origin	People of different racial or ethnic origins
Personal data revealing religious or philosophical beliefs	People holding different religious or philosophical beliefs
Data concerning health	People with different states of physical or mental health
Personal data concerning an individual's sexual orientation	People of different sexual orientation

(3) Processing does not meet the condition in sub-paragraph (1) if it is carried out for the purposes of measures or decisions with respect to a particular data subject.

(4) Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to an individual.

(5) Processing does not meet the condition in sub-paragraph (1) if—

(a) an individual who is the data subject (or one of the data subjects) has given notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject (and has not given notice in writing withdrawing that requirement),

(b) the notice gave the controller a reasonable period in which to stop processing such data, and

(c) that period has ended.

Racial and ethnic diversity at senior levels of organisations

9.

(1) This condition is met if the processing—

(a) is of personal data revealing racial or ethnic origin,

(b) is carried out as part of a process of identifying suitable individuals to hold senior positions in a particular organisation, a type of organisation or organisations generally,

(c) is necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation or organisations, and

(d) can reasonably be carried out without the consent of the data subject,

subject to the exception in sub-paragraph (3).

(2) For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b) the controller is not aware of the data subject withholding consent.

(3) Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to an individual.

(4) For the purposes of this paragraph, an individual holds a senior position in an organisation if the individual—

(a) holds a position listed in sub-paragraph (5), or

(b) does not hold such a position but is a senior manager of the organisation.

(5) Those positions are—

(a) a director, secretary or other similar officer of a body corporate;

(b) a member of a limited liability partnership;

(c) a partner in a partnership within the Partnership Act 1890, a limited partnership registered under the Limited Partnerships Act 1907 or an entity of a similar character formed under the law of a country or territory outside the United Kingdom.

(6) In this paragraph, "senior manager", in relation to an organisation, means a person who plays a significant role in—

(a) the making of decisions about how the whole or a substantial part of the organisation's activities are to be managed or organised, or

(b) the actual managing or organising of the whole or a substantial part of those activities.

(7) The reference in sub-paragraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Preventing etc ~~or detecting~~ unlawful acts [sch 9. para 22(2)]

10.

(1) This condition is met if the processing—

(a) is necessary for the purposes of the prevention, investigation or detection of an unlawful act, [sch 9. para 22(3)]

(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and

(c) is necessary for reasons of substantial public interest.

(2) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

(3) In this paragraph—

"act" includes a failure to act;

"competent authority" has the same meaning as in Part 3 of this Act (see section 30).

Protecting the public against dishonesty etc

11.

(1) This condition is met if the processing—

(a) is necessary for the exercise of a protective function,

(b) must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and

(c) is necessary for reasons of substantial public interest.

(2) In this paragraph, "protective function" means a function which is intended to protect members of the public against—

(a) dishonesty, malpractice or other seriously improper conduct,

(b) unfitness or incompetence,

(c) mismanagement in the administration of a body or association, or

(d) failures in services provided by a body or association.

Regulatory requirements relating to unlawful acts and dishonesty etc

12.

(1) This condition is met if—

(a) the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has—

(i) committed an unlawful act, or

(ii) been involved in dishonesty, malpractice or other seriously improper conduct,

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing, and

(c) the processing is necessary for reasons of substantial public interest.

(2) In this paragraph—

"act" includes a failure to act;

"regulatory requirement" means—

(a) a requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or
(b) a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity.

Journalism etc in connection with unlawful acts and dishonesty etc

13.

(1) This condition is met if—

(a) the processing consists of, or is carried out in preparation for, the disclosure of personal data for the special purposes, [sch 9. para 22(4)]

(b) it is carried out in connection with a matter described in sub-paragraph (2),

(c) it is necessary for reasons of substantial public interest,

(d) it is carried out with a view to the publication of the personal data by any person, and

(e) the controller reasonably believes that publication of the personal data would be in the public interest.

(2) The matters mentioned in sub-paragraph (1)(b) are any of the following (whether alleged or established)—

(a) the commission of an unlawful act by a person;

(b) dishonesty, malpractice or other seriously improper conduct of a person;

(c) unfitness or incompetence of a person;

(d) mismanagement in the administration of a body or association;

(e) a failure in services provided by a body or association.

(3) The condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

(4) In this paragraph—

"act" includes a failure to act;

"the special purposes" means—

(a) the purposes of journalism;
(b) academic purposes;
(c) artistic purposes;
(d) literary purposes.

Preventing fraud

14.

(1) This condition is met if the processing—

(a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and

(b) consists of—

(i) the disclosure of personal data by a person as a member of an anti-fraud organisation,

(ii) the disclosure of personal data in accordance with arrangements made by an anti-fraud organisation,

(iia) the processing of personal data carried out in preparation for disclosure described in sub-paragraph (i) or (ii), or [sch 9. para 22(5)]

(iii) the processing of personal data disclosed as described in sub-paragraph (i) or (ii).

(2) In this paragraph, "anti-fraud organisation" has the same meaning as in section 68 of the Serious Crime Act 2007.

Suspicion of terrorist financing or money laundering

15. This condition is met if the processing is necessary for the purposes of making a disclosure in good faith under either of the following—

    (a) section 21CA of the Terrorism Act 2000 (disclosures between certain entities within regulated sector in relation to suspicion of commission of terrorist financing offence or for purposes of identifying terrorist property);

    (b) section 339ZB of the Proceeds of Crime Act 2002 (disclosures within regulated sector in relation to suspicion of money laundering).

Support for individuals with a particular disability or medical condition

16.

(1) This condition is met if the processing—

(a) is carried out by a not-for-profit body which provides support to individuals with a particular disability or medical condition,

(b) is of a type of personal data falling within sub-paragraph (2) which relates to an individual falling within sub-paragraph (3),

(c) is necessary for the purposes of—

(i) raising awareness of the disability or medical condition, or

(ii) providing support to individuals falling within sub-paragraph (3) or enabling such individuals to provide support to each other,

(d) can reasonably be carried out without the consent of the data subject, and

(e) is necessary for reasons of substantial public interest.

(2) The following types of personal data fall within this sub-paragraph—

(a) personal data revealing racial or ethnic origin;

(b) genetic data or biometric data;

(c) data concerning health;

(d) personal data concerning an individual's sex life or sexual orientation.

(3) An individual falls within this sub-paragraph if the individual is or has been a member of the body mentioned in sub-paragraph (1)(a) and—

(a) has the disability or condition mentioned there, has had that disability or condition or has a significant risk of developing that disability or condition, or

(b) is a relative or carer of an individual who satisfies paragraph (a) of this sub-paragraph.

(4) For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b) the controller is not aware of the data subject withholding consent.

(5) In this paragraph—

"carer" means an individual who provides or intends to provide care for another individual other than—

(a) under or by virtue of a contract, or
(b) as voluntary work;

"disability" has the same meaning as in the Equality Act 2010 (see section 6 of, and Schedule 1 to, that Act).

(6) The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Counselling etc

17.

(1) This condition is met if the processing—

(a) is necessary for the provision of confidential counselling, advice or support or of another similar service provided confidentially,

(b) is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(c) is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(b) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the service mentioned in sub-paragraph (1)(a).

Safeguarding of children and of individuals at risk

18.

(1) This condition is met if—

(a) the processing is necessary for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

Safeguarding of economic well-being of certain individuals

19.

(1) This condition is met if the processing—

(a) is necessary for the purposes of protecting the economic well-being of an individual at economic risk who is aged 18 or over,

(b) is of data concerning health,

(c) is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) In this paragraph, "individual at economic risk" means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness or disability.

Insurance

20.

(1) This condition is met if the processing—

(a) is necessary for an insurance purpose,

(b) is of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health, and

(c) is necessary for reasons of substantial public interest,

subject to sub-paragraphs (2) and (3).

(2) Sub-paragraph (3) applies where—

(a) the processing is not carried out for the purposes of measures or decisions with respect to the data subject, and

(b) the data subject does not have and is not expected to acquire—

(i) rights against, or obligations in relation to, a person who is an insured person under an insurance contract to which the insurance purpose mentioned in sub-paragraph (1)(a) relates, or

(ii) other rights or obligations in connection with such a contract.

(3) Where this sub-paragraph applies, the processing does not meet the condition in sub-paragraph (1) unless, in addition to meeting the requirements in that sub-paragraph, it can reasonably be carried out without the consent of the data subject.

(4) For the purposes of sub-paragraph (3), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b) the controller is not aware of the data subject withholding consent.

(5) In this paragraph—

"insurance contract" means a contract of general insurance or long-term insurance;

"insurance purpose" means—

(a) advising on, arranging, underwriting or administering an insurance contract,
(b) administering a claim under an insurance contract, or
(c) exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law.

(6) The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

(7) Terms used in the definition of "insurance contract" in sub-paragraph (5) and also in an order made under section 22 of the Financial Services and Markets Act 2000 (regulated activities) have the same meaning in that definition as they have in that order.

Occupational pensions

21.

(1) This condition is met if the processing—

(a) is necessary for the purpose of making a determination in connection with eligibility for, or benefits payable under, an occupational pension scheme,

(b) is of data concerning health which relates to a data subject who is the parent, grandparent, great-grandparent or sibling of a member of the scheme,

(c) is not carried out for the purposes of measures or decisions with respect to the data subject, and

(d) can reasonably be carried out without the consent of the data subject.

(2) For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b) the controller is not aware of the data subject withholding consent.

(3) In this paragraph—

"occupational pension scheme" has the meaning given in section 1 of the Pension Schemes Act 1993;

"member", in relation to a scheme, includes an individual who is seeking to become a member of the scheme.

(4) The reference in sub-paragraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Political parties

22.

(1) This condition is met if the processing—

(a) is of personal data revealing political opinions,

(b) is carried out by a person or organisation included in the register maintained under section 23 of the Political Parties, Elections and Referendums Act 2000, and

(c) is necessary for the purposes of the person's or organisation's political activities,

subject to the exceptions in sub-paragraphs (2) and (3).

(2) Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to a person.

(3) Processing does not meet the condition in sub-paragraph (1) if—

(a) an individual who is the data subject (or one of the data subjects) has given notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject (and has not given notice in writing withdrawing that requirement),

(b) the notice gave the controller a reasonable period in which to stop processing such data, and

(c) that period has ended.

(4) In this paragraph, "political activities" include campaigning, fund-raising, political surveys and case-work.

Elected representatives responding to requests

23.

(1) This condition is met if—

(a) the processing is carried out—

(i) by an elected representative or a person acting with the authority of such a representative,

(ii) in connection with the discharge of the elected representative's functions, and

(iii) in response to a request by an individual that the elected representative take action on behalf of the individual, and

(b) the processing is necessary for the purposes of, or in connection with, the action reasonably taken by the elected representative in response to that request,

subject to sub-paragraph (2).

(2) Where the request is made by an individual other than the data subject, the condition in sub-paragraph (1) is met only if the processing must be carried out without the consent of the data subject for one of the following reasons—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) obtaining the consent of the data subject would prejudice the action taken by the elected representative;

(d) the processing is necessary in the interests of another individual and the data subject has withheld consent unreasonably.

(3) In this paragraph, "elected representative" means—

(a) a member of the House of Commons;

(b) a member of the National Assembly for Wales;

(c) a member of the Scottish Parliament;

(d) a member of the Northern Ireland Assembly;

(e) . . . . . .

(f) an elected member of a local authority within the meaning of section 270(1) of the Local Government Act 1972, namely—

(i) in England, a county council, a district council, a London borough council or a parish council;

(ii) in Wales, a county council, a county borough council or a community council;

(g) an elected mayor of a local authority within the meaning of Part 1A or 2 of the Local Government Act 2000;

(h) a mayor for the area of a combined authority established under section 103 of the Local Democracy, Economic Development and Construction Act 2009;

(i) the Mayor of London or an elected member of the London Assembly;

(j) an elected member of—

(i) the Common Council of the City of London, or

(ii) the Council of the Isles of Scilly;

(k) an elected member of a council constituted under section 2 of the Local Government etc (Scotland) Act 1994;

(l) an elected member of a district council within the meaning of the Local Government Act (Northern Ireland) 1972 (c. 9 (N.I.));

(m) a police and crime commissioner.

(4) For the purposes of sub-paragraph (3), a person who is—

(a) a member of the House of Commons immediately before Parliament is dissolved,

(b) a member of the National Assembly for Wales immediately before that Assembly is dissolved,

(c) a member of the Scottish Parliament immediately before that Parliament is dissolved, or

(d) a member of the Northern Ireland Assembly immediately before that Assembly is dissolved,

is to be treated as if the person were such a member until the end of the fourth day after the day on which the subsequent general election in relation to that Parliament or Assembly is held.

(5) For the purposes of sub-paragraph (3), a person who is an elected member of the Common Council of the City of London and whose term of office comes to an end at the end of the day preceding the annual Wardmotes is to be treated as if he or she were such a member until the end of the fourth day after the day on which those Wardmotes are held.

Disclosure to elected representatives

24. (1)This condition is met if—

(a) the processing consists of, or is carried out in preparation for, the disclosure of personal data— [sch 9. para 22(6)]

(i) to an elected representative or a person acting with the authority of such a representative, and

(ii) in response to a communication to the controller from that representative or person which was made in response to a request from an individual,

(b) the personal data is relevant to the subject matter of that communication, and

(c) the disclosure is necessary for the purpose of responding to that communication,

subject to sub-paragraph (2).

(2) Where the request to the elected representative came from an individual other than the data subject, the condition in sub-paragraph (1) is met only if the disclosure must be made without the consent of the data subject for one of the following reasons—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) obtaining the consent of the data subject would prejudice the action taken by the elected representative;

(d) the processing is necessary in the interests of another individual and the data subject has withheld consent unreasonably.

(3) In this paragraph, "elected representative" has the same meaning as in paragraph 23.

Informing elected representatives about prisoners

25.

(1) This condition is met if—

(a) the processing consists of the processing of personal data about a prisoner for the purpose of informing a member of the House of Commons, a member of the National Assembly for Wales or a member of the Scottish Parliament about the prisoner, and

(b) the member is under an obligation not to further disclose the personal data.

(2) The references in sub-paragraph (1) to personal data about, and to informing someone about, a prisoner include personal data about, and informing someone about, arrangements for the prisoner's release.

(3) In this paragraph—

"prison" includes a young offender institution, a remand centre, a secure training centre or a secure college;

"prisoner" means a person detained in a prison.

Publication of legal judgments

26. This condition is met if the processing—

(a) consists of the publication of a judgment or other decision of a court or tribunal, or

(b) is necessary for the purposes of publishing such a judgment or decision.

Anti-doping in sport

27.

(1) This condition is met if the processing is necessary—

(a) for the purposes of measures designed to eliminate doping which are undertaken by or under the responsibility of a body or association that is responsible for eliminating doping in a sport, at a sporting event or in sport generally, or

(b) for the purposes of providing information about doping, or suspected doping, to such a body or association.

(2) The reference in sub-paragraph (1)(a) to measures designed to eliminate doping includes measures designed to identify or prevent doping.

(3) If the processing consists of the disclosure of personal data to a body or association described in sub-paragraph (1)(a), or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

Standards of behaviour in sport

28.

(1) This condition is met if the processing—

(a) is necessary for the purposes of measures designed to protect the integrity of a sport or a sporting event,

(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and

(c) is necessary for reasons of substantial public interest.

(2) In sub-paragraph (1)(a), the reference to measures designed to protect the integrity of a sport or a sporting event is a reference to measures designed to protect a sport or a sporting event against—

(a) dishonesty, malpractice or other seriously improper conduct, or

(b) failure by a person participating in the sport or event in any capacity to comply with standards of behaviour set by a body or association with responsibility for the sport or event.

PART 3 ADDITIONAL CONDITIONS RELATING TO CRIMINAL CONVICTIONS ETC

Consent

29. This condition is met if the data subject has given consent to the processing.

Protecting individual's vital interests

30. This condition is met if—

(a) the processing is necessary to protect the vital interests of an individual, and

(b) the data subject is physically or legally incapable of giving consent.

Processing by not-for-profit bodies

31. This condition is met if the processing is carried out—

(a) in the course of its legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim, and

(b) on condition that—

(i) the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and

(ii) the personal data is not disclosed outside that body without the consent of the data subjects.

Personal data in the public domain

32. This condition is met if the processing relates to personal data which is manifestly made public by the data subject.

Legal claims

33. This condition is met if the processing—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Judicial acts

34. This condition is met if the processing is necessary when a court or tribunal is acting in its judicial capacity.

Administration of accounts used in commission of indecency offences involving children

35.

(1) This condition is met if—

(a) the processing is of personal data about a conviction or caution for an offence listed in sub-paragraph (2),

(b) the processing is necessary for the purpose of administering an account relating to the payment card used in the commission of the offence or cancelling that payment card, and

(c) when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule).

(2) Those offences are an offence under—

(a) section 1 of the Protection of Children Act 1978 (indecent photographs of children),

(b) Article 3 of the Protection of Children (Northern Ireland) Order 1978 (S.I. 1978/1047 (N.I. 17)) (indecent photographs of children),

(c) section 52 of the Civic Government (Scotland) Act 1982 (indecent photographs etc of children),

(d) section 160 of the Criminal Justice Act 1988 (possession of indecent photograph of child),

(e) Article 15 of the Criminal Justice (Evidence etc) (Northern Ireland) Order 1988 (S.I. 1988/1847 (N.I. 17)) (possession of indecent photograph of child), or

(f) section 62 of the Coroners and Justice Act 2009 (possession of prohibited images of children),

or incitement to commit an offence under any of those provisions.

(3) See also the additional safeguards in Part 4 of this Schedule.

(4) In this paragraph—

"caution" means a caution given to a person in England and Wales or Northern Ireland in respect of an offence which, at the time when the caution is given, is admitted;

"conviction" has the same meaning as in the Rehabilitation of Offenders Act 1974 or the Rehabilitation of Offenders (Northern Ireland) Order 1978 (S.I. 1978/1908 (N.I. 27));

"payment card" includes a credit card, a charge card and a debit card.

Extension of conditions in Part 2 of this Schedule referring to substantial public interest

36. This condition is met if the processing would meet a condition in Part 2 of this Schedule but for an express requirement for the processing to be necessary for reasons of substantial public interest.

Extension of insurance conditions

37. This condition is met if the processing—

(a) would meet the condition in paragraph 20 in Part 2 of this Schedule (the "insurance condition"), or

(b) would meet the condition in paragraph 36 by virtue of the insurance condition,

but for the requirement for the processing to be processing of a category of personal data specified in paragraph 20(1)(b).

PART 4 APPROPRIATE POLICY DOCUMENT AND ADDITIONAL SAFEGUARDS

Application of this Part of this Schedule

38. This Part of this Schedule makes provision about the processing of personal data carried out in reliance on a condition in Part 1, 2 or 3 of this Schedule which requires the controller to have an appropriate policy document in place when the processing is carried out.

Requirement to have an appropriate policy document in place

39. The controller has an appropriate policy document in place in relation to the processing of personal data in reliance on a condition described in paragraph 38 if the controller has produced a document which—

(a) explains the controller's procedures for securing compliance with the principles in Article 5 of the UK GDPR (principles relating to processing of personal data) in connection with the processing of personal data 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 condition, giving an indication of how long such personal data is likely to be retained.

Additional safeguard: retention of appropriate policy document

40.

(1) Where personal data is processed in reliance on a condition described in paragraph 38, 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.

(2) "Relevant period", in relation to the processing of personal data in reliance on a condition described in paragraph 38, means a period which—

(a) begins when the controller starts to carry out processing of personal data in reliance on that condition, and

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

Additional safeguard: record of processing

41. A record maintained by the controller, ~~or the controller's representative~~ [s. 13(3)(e)], under Article 30A [sch. 4 para 22] of the UK GDPR in respect of the processing of personal data in reliance on a condition described in paragraph 38 must include the following information—

(a) which condition is relied on,

(b) how the processing satisfies Article 6 of the UK GDPR (lawfulness of processing), and

(c) whether the personal data is retained and erased in accordance with the policies described in paragraph 39(b) and, if it is not, the reasons for not following those policies.

Section 15

SCHEDULE 2EXEMPTIONS ETC FROM THE UK GDPR

PART 1ADAPTATIONS AND RESTRICTIONS AS DESCRIBED IN ARTICLES 6(3) AND 23(1)

UK GDPR provisions to be adapted or restricted: "the listed GDPR provisions"

1. In this Part of this Schedule, "the listed GDPR provisions" means—

(a) the following provisions of the UK GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the UK GDPR)—

(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 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(iv) Article 16 (right to rectification);

(v) Article 17(1) and (2) (right to erasure);

(vi) Article 18(1) (restriction of processing);

(vii) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);

(viii) Article 20(1) and (2) (right to data portability);

(ix) Article 21(1) (objections to processing);

(x) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (i) to (ix); and

(b) the following provisions of the UK GDPR (the application of which may be adapted by virtue of Article 6(3) of the UK GDPR)—

(i) Article 5(1)(a) (lawful, fair and transparent processing), other than the lawfulness requirements set out in Article 6;

~~(ii) Article 5(1)(b) (purpose limitation).~~ [s. 6(10)]

Crime and taxation: general

2.

(1) The listed GDPR provisions and Article 34(1) and (4) of the UK GDPR (communication of personal data breach to the data subject) do not apply to personal data processed for any of the following purposes—

(a) the prevention, investigation or detection of crime, [sch 9. para 23(2)]

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of a tax or duty or an imposition of a similar nature,

to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

(2) Sub-paragraph (3) applies where—

(a) personal data is processed by a person ("Controller 1") for any of the purposes mentioned in sub-paragraph (1)(a) to (c), and

(b) another person ("Controller 2") obtains the data from Controller 1 for the purpose of discharging statutory functions and processes it for the purpose of discharging statutory functions.

(3) Controller 2 is exempt from the obligations in the following provisions of the UK GDPR—

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided),

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers), and

(d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in paragraphs (a) to (c),

to the same extent that Controller 1 is exempt from those obligations by virtue of sub-paragraph (1).

Crime and taxation: risk assessment systems

3.

(1) The UK GDPR provisions listed in sub-paragraph (3) do not apply to personal data which consists of a classification applied to the data subject as part of a risk assessment system falling within sub-paragraph (2) to the extent that the application of those provisions would prevent the system from operating effectively.

(2) A risk assessment system falls within this sub-paragraph if—

(a) it is operated by a government department, a local authority or another authority administering housing benefit, and

(b) it is operated for the purposes of—

(i) the assessment or collection of a tax or duty or an imposition of a similar nature, or

(ii) the prevention, investigation or detection of crime or apprehension or prosecution of offenders, where the offence concerned involves the unlawful use of public money or an unlawful claim for payment out of public money. [sch 9. para 23(3)]

(3) The UK GDPR provisions referred to in sub-paragraph (1) are the following provisions of the UK GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the UK GDPR)—

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in paragraphs (a) to (c).

Immigration

4.

(1) The UK GDPR provisions listed in sub-paragraph (2) do not apply to personal data processed by the Secretary of State for any of the following purposes—

(a) the maintenance of effective immigration control, or

(b) the investigation or detection of activities that would undermine the maintenance of effective immigration control,

to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) and (b).

(1A)But sub-paragraph (1) does not apply unless the Secretary of State has an immigration exemption policy document in place.

(1B)For the purposes of sub-paragraph (1A), the Secretary of State has an immigration exemption policy document in place if the Secretary of State has produced a document which explains the Secretary of State's policies and processes for—

(a) determining the extent to which the application of any of the UK GDPR provisions listed in sub-paragraph (2) would be likely to prejudice any of the matters mentioned in sub-paragraph (1)(a) and (b), and

(b) where it is determined that any of those provisions do not apply in relation to personal data processed for any of the purposes mentioned in sub-paragraph (1)(a) and (b), preventing—

(i) the abuse of that personal data, and

(ii) any access to, or transfer of, it otherwise than in accordance with the UK GDPR.

(1C)Paragraphs 4A and 4B make provision about additional safeguards in connection with the exemption in this paragraph.

(2) The UK GDPR provisions referred to in sub-paragraphs (1) and (1B) are the following provisions of the UK GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the UK GDPR)—

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(d) Article 17(1) and (2) (right to erasure);

(e) Article 18(1) (restriction of processing);

(f) Article 21(1) (objections to processing);

(g) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (a) to (f).

(That is, the listed GDPR provisions other than Article 16 (right to rectification), Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing) and Article 20(1) and (2) (right to data portability) and, subject to sub-paragraph (2)(g) of this paragraph, the provisions of Article 5 listed in paragraph 1(b).)

Immigration: additional safeguard: decisions for the purposes of paragraph 4(1) and requirement to have regard to immigration exemption policy document

4A.

(1) The Secretary of State must—

(a) determine the extent to which the application of the relevant UK GDPR provisions would be likely to prejudice any of the matters mentioned in paragraph 4(1)(a) and (b) on a case by case basis, and

(b) have regard, when making such a determination, to the immigration exemption policy document.

(2) The Secretary of State must also—

(a) review the immigration exemption policy document and (if appropriate) update it from time to time;

(b) publish it, and any update to it, in such manner as the Secretary of State considers appropriate.

(3) In this paragraph and paragraph 4B "the relevant UK GDPR provisions" means the provisions of the UK GDPR listed in paragraph 4(2).

Immigration: additional safeguard: record etc of decision that exemption applies

4B.

(1) Where the Secretary of State determines in any particular case that the application of any of the relevant UK GDPR provisions would be likely to prejudice any of the matters mentioned in paragraph 4(1)(a) and (b), the Secretary of State must—

(a) keep a record of that determination and the reasons for it, and

(b) inform the data subject of that determination.

(2) But the Secretary of State is not required to comply with sub-paragraph (1)(b) if doing so may be prejudicial to any of the matters mentioned in paragraph 4(1)(a) and (b).

Information required to be disclosed by law etc or in connection with legal proceedings

5.

(1) The listed GDPR provisions do not apply to personal data consisting of information that the controller is obliged by an enactment to make available to the public, to the extent that

the application of those provisions would prevent the controller from complying with that obligation.

(2) The listed GDPR provisions do not apply to personal data where disclosure of the data is required by an enactment, a rule of law or an order of a court or tribunal, to the extent that the application of those provisions would prevent the controller from making the disclosure.

(3) The listed GDPR provisions do not apply to personal data where disclosure of the data—

(a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights,

to the extent that the application of those provisions would prevent the controller from making the disclosure.

PART 2 RESTRICTIONS AS DESCRIBED IN ARTICLE 23(1): RESTRICTIONS OF RULES IN ARTICLES 13 TO 21 AND 34

UK GDPR provisions to be restricted: "the listed GDPR provisions"

6. In this Part of this Schedule, "the listed GDPR provisions" means the following provisions of the UK GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the UK GDPR)—

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(d) Article 16 (right to rectification);

(e) Article 17(1) and (2) (right to erasure);

(f) Article 18(1) (restriction of processing);

(g) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);

(h) Article 20(1) and (2) (right to data portability);

(i) Article 21(1) (objections to processing);

(j) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (a) to (i).

Functions designed to protect the public etc

7. The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a function that—

(a) is designed as described in column 1 of the Table, and

(b) meets the condition relating to the function specified in column 2 of the Table,

to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

TABLE

Description of function design	***Condition***
1. The function is designed to protect members of the public against— (a) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate, or (b) financial loss due to the conduct of discharged or undischarged bankrupts.	The function is— (a) conferred on a person by an enactment, (b) a function of the Crown, a Minister of the Crown or a government department, or (c) of a public nature, and is exercised in the public interest.
2. The function is designed to protect members of the public against— (a) dishonesty, malpractice or other seriously improper conduct, or (b) unfitness or incompetence.	The function is— (a) conferred on a person by an enactment, (b) a function of the Crown, a Minister of the Crown or a government department, or (c) of a public nature, and is exercised in the public interest.
3. The function is designed— (a) to protect charities or community interest companies against misconduct or mismanagement (whether by trustees, directors or other persons) in their administration, (b) to protect the property of charities or community interest companies from loss or misapplication, or (c) to recover the property of charities or community interest companies.	The function is— (a) conferred on a person by an enactment, (b) a function of the Crown, a Minister of the Crown or a government department, or (c) of a public nature, and is exercised in the public interest.
4. The function is designed— (a) to secure the health, safety and welfare of persons at work, or (b) to protect persons other than those at work against risk to health or safety arising out of or in connection with the action of persons at work.	The function is— (a) conferred on a person by an enactment, (b) a function of the Crown, a Minister of the Crown or a government department, or (c) of a public nature, and is exercised in the public interest.
5. The function is designed to protect members of the public against— (a) maladministration by public bodies, (b) failures in services provided by public bodies, or (c) a failure of a public body to provide a service which it is a function of the body to provide.	The function is conferred by any enactment on— (a) the Parliamentary Commissioner for Administration, (b) the Commissioner for Local Administration in England, (c) the Health Service Commissioner for England, (d) the Public Services Ombudsman for Wales, (e) the Northern Ireland Public Services Ombudsman, (f) the Prison Ombudsman for Northern Ireland, or (g) the Scottish Public Services Ombudsman.

6. The function is designed— (a) to protect members of the public against conduct which may adversely affect their interests by persons carrying on a business, (b) to regulate agreements or conduct which have as their object or effect the prevention, restriction or distortion of competition in connection with any commercial activity, or (c) to regulate conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market.	The function is conferred on the Competition and Markets Authority by an enactment.

Audit functions

8.

(1) The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a function listed in sub-paragraph (2) to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

(2) The functions are any function that is conferred by an enactment on—

(a) the Comptroller and Auditor General;

(b) the Auditor General for Scotland;

(c) the Auditor General for Wales;

(d) the Comptroller and Auditor General for Northern Ireland.

Functions of the Bank of England

9.

(1) The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a relevant function of the Bank of England to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

(2) "Relevant function of the Bank of England" means—

(a) a function discharged by the Bank acting in its capacity as a monetary authority (as defined in section 244(2)(c) and (2A) of the Banking Act 2009);

(b) a public function of the Bank within the meaning of section 349 of the Financial Services and Markets Act 2000;

(c) a function conferred on the Prudential Regulation Authority by or under the Financial Services and Markets Act 2000 or by another enactment.

Regulatory functions relating to legal services, the health service and children's services

10.

(1) The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a function listed in sub-paragraph (2) to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

(2) The functions are—

(a) a function of the Legal Services Board;

(b) the function of considering a complaint under the scheme established under Part 6 of the Legal Services Act 2007 (legal complaints);

(c) the function of considering a complaint under—

(i) section 14 of the NHS Redress Act 2006,

(ii) section 113(1) or (2) or section 114(1) or (3) of the Health and Social Care (Community Health and Standards) Act 2003,

(iii) section 24D or 26 of the Children Act 1989, or

(iv) Part 2A of the Public Services Ombudsman (Wales) Act 2005 **F316**or Part 5 of the Public Services Ombudsman (Wales) Act 2019;

(d) the function of considering a complaint or representations under Chapter 1 of Part 10 of the Social Services and Well-being (Wales) Act 2014 (anaw 4).

Regulatory functions of certain other persons

11. The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a function that—

(a) is a function of a person described in column 1 of the Table, and

(b) is conferred on that person as described in column 2 of the Table,

to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

TABLE

Person on whom function is conferred	***How function is conferred***
1. The Commissioner.	By or under— (a) the data protection legislation; (b) the Freedom of Information Act 2000; (c) section 244 of the Investigatory Powers Act 2016; (d) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426); (e) the Environmental Information Regulations 2004 (S.I. 2004/3391); (f) the INSPIRE Regulations 2009 (S.I. 2009/3157); (g) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; (h) the Re-use of Public Sector Information Regulations 2015 (S.I. 2015/1415); (i) the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (S.I. 2016/696).
2. The Scottish Information Commissioner.	By or under— (a) the Freedom of Information (Scotland) Act 2002 (asp 13); (b) the Environmental Information (Scotland) Regulations 2004 (S.S.I. 2004/520); (c) the INSPIRE (Scotland) Regulations 2009 (S.S.I. 2009/440).
3. The Pensions Ombudsman.	By or under Part 10 of the Pension Schemes Act 1993 or any corresponding legislation having equivalent effect in Northern Ireland.
4. The Board of the Pension Protection Fund.	By or under sections 206 to 208 of the Pensions Act 2004 or any corresponding legislation having equivalent effect in Northern Ireland.

5. The Ombudsman for the Board of the Pension Protection Fund.	By or under any of sections 209 to 218 or 286(1) of the Pensions Act 2004 or any corresponding legislation having equivalent effect in Northern Ireland.
6. The Pensions Regulator.	By an enactment.
7. The Financial Conduct Authority.	By or under the Financial Services and Markets Act 2000 or by another enactment.
8. The Financial Ombudsman.	By or under Part 16 of the Financial Services and Markets Act 2000.
9. The investigator of complaints against the financial regulators.	By or under Part 6 of the Financial Services Act 2012.
. . .	. . .
11. The monitoring officer of a relevant authority.	By or under the Local Government and Housing Act 1989.
12. The monitoring officer of a relevant Welsh authority.	By or under the Local Government Act 2000.
13. The Public Services Ombudsman for Wales.	By or under the Local Government Act 2000.
14. The Charity Commission.	By or under— (a) the Charities Act 1992; (b) the Charities Act 2006; (c) the Charities Act 2011.

12. In the Table in paragraph 11—

the "Financial Ombudsman" means the scheme operator within the meaning of Part 16 of the Financial Services and Markets Act 2000 (see section 225 of that Act);

the "investigator of complaints against the financial regulators" means the person appointed under section 84(1)(b) of the Financial Services Act 2012;

"relevant authority" has the same meaning as in section 5 of the Local Government and Housing Act 1989, and "monitoring officer", in relation to such an authority, means a person designated as such under that section;

"relevant Welsh authority" has the same meaning as "relevant authority" in section 49(6) of the Local Government Act 2000, and "monitoring officer", in relation to such an authority, has the same meaning as in Part 3 of that Act.

Parliamentary privilege

13. The listed GDPR provisions and Article 34(1) and (4) of the UK GDPR (communication of personal data breach to the data subject) do not apply to personal data where this is required for the purpose of avoiding an infringement of the privileges of either House of Parliament.

Judicial appointments, judicial independence and judicial proceedings

14.

(1) The listed GDPR provisions do not apply to personal data processed for the purposes of assessing a person's suitability for judicial office or the office of Queen's Counsel.

(2) The listed GDPR provisions do not apply to personal data processed by—

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

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

(3) As regards personal data not falling within sub-paragraph (1) or (2), the listed GDPR provisions do not apply to the extent that the application of those provisions would be likely to prejudice judicial independence or judicial proceedings.

Crown honours, dignities and appointments

15.

(1) The listed GDPR provisions do not apply to personal data processed for the purposes of the conferring by the Crown of any honour or dignity.

(2) The listed GDPR provisions do not apply to personal data processed for the purposes of assessing a person's suitability for any of the following offices—

(a) archbishops and diocesan and suffragan bishops in the Church of England;

(b) deans of cathedrals of the Church of England;

(c) deans and canons of the two Royal Peculiars;

(d) the First and Second Church Estates Commissioners;

(e) lord-lieutenants;

(f) Masters of Trinity College and Churchill College, Cambridge;

(g) the Provost of Eton;

(h) the Poet Laureate;

(i) the Astronomer Royal.

(3) The Secretary of State may by regulations amend the list in sub-paragraph (2) to—

(a) remove an office, or

(b) add an office to which appointments are made by Her Majesty.

(4) Regulations under sub-paragraph (3) are subject to the affirmative resolution procedure.

PART 3RESTRICTION FOR THE PROTECTION OF RIGHTS OF OTHERS

Protection of the rights of others: general

16.

(1) Article 15(1) to (3) of the UK GDPR (confirmation of processing, access to data and safeguards for third country transfers), and Article 5 of the UK GDPR so far as its provisions correspond to the rights and obligations provided for in Article 15(1) to (3), do not oblige a controller to disclose information to the data subject to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information.

(2) Sub-paragraph (1) does not remove the controller's obligation where—

(a) the other individual has consented to the disclosure of the information to the data subject, or

(b) it is reasonable to disclose the information to the data subject without the consent of the other individual.

(3) In determining whether it is reasonable to disclose the information without consent, the controller must have regard to all the relevant circumstances, including—

(a) the type of information that would be disclosed,

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

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

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

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

(4) For the purposes of this paragraph—

(a) "information relating to another individual" includes information identifying the other individual as the source of information;

(b) an individual can be identified from information to be provided to a data subject by a controller if the individual can be identified from—

(i) that information, or

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

Assumption of reasonableness for health workers, social workers and education workers

17.

(1) For the purposes of paragraph 16(2)(b), it is to be considered reasonable for a controller to disclose information to a data subject without the consent of the other individual where—

(a) the health data test is met,

(b) the social work data test is met, or

(c) the education data test is met.

(2) The health data test is met if—

(a) the information in question is contained in a health record, and

(b) the other individual is a health professional who has compiled or contributed to the health record or who, in his or her capacity as a health professional, has been involved in the diagnosis, care or treatment of the data subject.

(3) The social work data test is met if—

(a) the other individual is—

(i) a children's court officer,

(ii) a person who is or has been employed by a person or body referred to in paragraph 8 of Schedule 3 in connection with functions exercised in relation to the information, or

(iii) a person who has provided for reward a service that is similar to a service provided in the exercise of any relevant social services functions, and

(b) the information relates to the other individual in an official capacity or the other individual supplied the information—

(i) in an official capacity, or

(ii) in a case within paragraph (a)(iii), in connection with providing the service mentioned in paragraph (a)(iii).

(4) The education data test is met if—

(a) the other individual is an education-related worker, or

(b) the other individual is employed by an education authority (within the meaning of the Education (Scotland) Act 1980) in pursuance of its functions relating to education and—

(i) the information relates to the other individual in his or her capacity as such an employee, or

(ii) the other individual supplied the information in his or her capacity as such an employee.

(5) In this paragraph—

"children's court officer" means a person referred to in paragraph 8(1)(q), (r), (s), (t) or (u) of Schedule 3;

"education-related worker" means a person referred to in paragraph 14(4)(a) or (b) or 16(4)(a), (b) or (c) of Schedule 3 (educational records);

"relevant social services functions" means functions specified in paragraph 8(1)(a), (b), (c) or (d) of Schedule 3.

PART 4 RESTRICTIONS AS DESCRIBED IN ARTICLE 23(1): RESTRICTIONS OF RULES IN ARTICLES 13 TO 15

UK GDPR provisions to be restricted: "the listed GDPR provisions"

18. In this Part of this Schedule, "the listed GDPR provisions" means the following provisions of the UK GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the UK GDPR)—

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (a) to (c).

Legal professional privilege

19. The listed GDPR provisions do not apply to personal data that consists of—

(a) information in respect of which a claim to legal professional privilege or, in Scotland, confidentiality of communications, could be maintained in legal proceedings, or

(b) information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser.

Self incrimination

20.

(1) A person need not comply with the listed GDPR provisions to the extent that compliance would, by revealing evidence of the commission of an offence, expose the person to proceedings for that offence.

(2) The reference to an offence in sub-paragraph (1) 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), or

(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).

(3) Information disclosed by any person in compliance with Article 15 of the UK GDPR is not admissible against the person in proceedings for an offence under this Act.

Corporate finance

21.

(1) The listed GDPR provisions do not apply to personal data processed for the purposes of or in connection with a corporate finance service provided by a relevant person to the extent that either Condition A or Condition B is met.

(2) Condition A is that the application of the listed GDPR provisions would be likely to affect the price of an instrument.

(3) Condition B is that—

(a) the relevant person reasonably believes that the application of the listed GDPR provisions to the personal data in question could affect a decision of a person—

(i) whether to deal in, subscribe for or issue an instrument, or

(ii) whether to act in a way likely to have an effect on a business activity (such as an effect on the industrial strategy of a person, the capital structure of an undertaking or the legal or beneficial ownership of a business or asset), and

(b) the application of the listed GDPR provisions to that personal data would have a prejudicial effect on the orderly functioning of financial markets or the efficient allocation of capital within the economy.

(4) In this paragraph—

"corporate finance service" means a service consisting in—

(a) underwriting in respect of issues of, or the placing of issues of, any instrument,
(b) services relating to such underwriting, or
(c) advice to undertakings on capital structure, industrial strategy and related matters and advice and service relating to mergers and the purchase of undertakings;

"instrument" means an instrument listed in section C of Annex 1 to Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments, and references to an instrument include an instrument not yet in existence but which is to be or may be created;

"price" includes value;

"relevant person" means—

(a) a person who, by reason of a permission under Part 4A of the Financial Services and Markets Act 2000, is able to carry on a corporate finance service without contravening the general prohibition;
(b) an EEA firm of the kind mentioned in paragraph 5(a) or (b) of Schedule 3 to that Act which has qualified for authorisation under paragraph 12 of that Schedule, and may lawfully carry on a corporate finance service;
(c) a person who is exempt from the general prohibition in respect of any corporate finance service—
(i) as a result of an exemption order made under section 38(1) of that Act, or
(ii) by reason of section 39(1) of that Act (appointed representatives);
(d) a person, not falling within paragraph (a), (b) or (c), who may lawfully carry on a corporate finance service without contravening the general prohibition;
(e) a person who, in the course of employment, provides to their employer a service falling within paragraph (b) or (c) of the definition of "corporate finance service";
(f) a partner who provides to other partners in the partnership a service falling within either of those paragraphs.

(5) In the definition of "relevant person" in sub-paragraph (4), references to "the general prohibition" are to the general prohibition within the meaning of section 19 of the Financial Services and Markets Act 2000.

Management forecasts

22. The listed GDPR provisions do not apply to personal data processed for the purposes of management forecasting or management planning in relation to a business or other activity to the extent that the application of those provisions would be likely to prejudice the conduct of the business or activity concerned.

Negotiations

23. The listed GDPR provisions do not apply to personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject to the extent that the application of those provisions would be likely to prejudice those negotiations.

Confidential references

24. The listed GDPR provisions do not apply to personal data consisting of a reference given (or to be given) in confidence for the purposes of—
    (a) the education, training or employment (or prospective education, training or employment) of the data subject,
    (b) the placement (or prospective placement) of the data subject as a volunteer,
    (c) the appointment (or prospective appointment) of the data subject to any office, or
    (d) the provision (or prospective provision) by the data subject of any service.

Exam scripts and exam marks

25.
    (1) The listed GDPR provisions do not apply to personal data consisting of information recorded by candidates during an exam.
    (2) Where personal data consists of marks or other information processed by a controller—
        (a) for the purposes of determining the results of an exam, or
        (b) in consequence of the determination of the results of an exam,

the duty in Article 12(3) or (4) of the UK GDPR for the controller to provide information requested by the data subject within a certain time period, as it applies to Article 15 of the UK GDPR (confirmation of processing, access to data and safeguards for third country transfers), is modified as set out in sub-paragraph (3).

(3)Where a question arises as to whether the controller is obliged by Article 15 of the UK GDPR to disclose personal data, and the question arises before the day on which the exam results are announced, the controller must provide the information mentioned in Article 12(3) or (4)—

(a)before the end of the period of 5 months beginning when the question arises, or

(b)if earlier, before the end of the period of 40 days beginning with the announcement of the results.

(4)In this paragraph, "exam" means an academic, professional or other examination used for determining the knowledge, intelligence, skill or ability of a candidate and may include an exam consisting of an assessment of the candidate's performance while undertaking work or any other activity.

(5)For the purposes of this paragraph, the results of an exam are treated as announced when they are first published or, if not published, first communicated to the candidate.

PART 5EXEMPTIONS ETC … FOR REASONS OF FREEDOM OF EXPRESSION AND INFORMATION

Journalistic, academic, artistic and literary purposes

26.

(1) In this paragraph, "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) Sub-paragraph (3) applies to the processing of personal data carried out for the special purposes if—
  (a) the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material, and
  (b) the controller reasonably believes that the publication of the material would be in the public interest.

(3) The listed GDPR provisions do not apply to the extent that the controller reasonably believes that the application of those provisions would be incompatible with the special purposes.

(4) In determining whether publication would be in the public interest the controller must take into account the special importance of the public interest in the freedom of expression and information.

(5) In determining whether it is reasonable to believe that publication would be in the public interest, the controller must have regard to any of the codes of practice or guidelines listed in sub-paragraph (6) that is relevant to the publication in question.

(6) The codes of practice and guidelines are—
  (a) BBC Editorial Guidelines;
  (b) Ofcom Broadcasting Code;
  (c) Editors' Code of Practice.

(7) The Secretary of State may by regulations amend the list in sub-paragraph (6).

(8) Regulations under sub-paragraph (7) are subject to the affirmative resolution procedure.

(9) For the purposes of this paragraph, the listed GDPR provisions are the following provisions of the UK GDPR (which may be exempted or derogated from by virtue of Article 85(2) of the UK GDPR)—
  (a) in Chapter II of the UK GDPR (principles)—
    (i) Article 5(1)(a) to (e) (principles relating to processing);
    (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 data);
    (vi) Article 10 (data relating to criminal convictions etc);
    (vii) Article 11(2) (processing not requiring identification);
  (b) in Chapter III of the UK 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 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(iv) Article 16 (right to rectification);

(v) Article 17(1) and (2) (right to erasure);

(vi) Article 18(1)(a), (b) and (d) (restriction of processing);

(vii) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);

(viii) Article 20(1) and (2) (right to data portability);

(ix) Article 21(1) (objections to processing);

(c) in Chapter IV of the UK GDPR (controller and processor)—

(i) Article 34(1) and (4) (communication of personal data breach to the data subject);

~~(ii) Article 36 (requirement for controller to consult Commissioner prior to high risk processing);~~ [sch. 4 para 23]

(d) in Chapter V of the UK GDPR (transfers of data to third countries etc), Article 44A (general principles for transfers); [sch. 7 para 21]

PART 6 DEROGATIONS ETC FOR RESEARCH, STATISTICS AND ARCHIVING

Research and statistics

27.

(1) The listed GDPR provisions do not apply to personal data processed for—

(a) scientific or historical research purposes, or

(b) statistical purposes,

to the extent that the application of those provisions would prevent or seriously impair the achievement of the purposes in question.

This is subject to sub-paragraphs (3) and (4).

(2) For the purposes of this paragraph, the listed GDPR provisions are the following provisions of the UK GDPR—

(a) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(b) Article 16 (right to rectification);

(c) Article 18(1) (restriction of processing);

(d) Article 21(1) (objections to processing).

(3) The exemption in sub-paragraph (1) is available only where—

(a) the personal data is processed in accordance with Article 84B of the UK GDPR ~~89(1) of the UK GDPR (as supplemented by section 19)~~, and [s. 23(2)(c)(i)]

(b) as regards the disapplication of Article 15(1) to (3), the results of the research or any resulting statistics are not made available in a form which identifies a data subject.

(4) Where processing for a purpose described in sub-paragraph (1) serves at the same time another purpose, the exemption in sub-paragraph (1) is available only where the personal data is processed for a purpose referred to in that sub-paragraph.

Archiving in the public interest

28.

(1) The listed GDPR provisions do not apply to personal data processed for archiving purposes in the public interest to the extent that the application of those provisions would prevent or seriously impair the achievement of those purposes.

This is subject to sub-paragraphs (3) and (4).

(2) For the purposes of this paragraph, the listed GDPR provisions are the following provisions of the UK GDPR—

(a) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(b) Article 16 (right to rectification);

(c) Article 18(1) (restriction of processing);

(d) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);

(e) Article 20(1) (right to data portability);

(f) Article 21(1) (objections to processing).

(3) The exemption in sub-paragraph (1) is available only where the personal data is processed in accordance with Article 84B of the UK GDPR ~~Article 89(1) of the UK GDPR (as supplemented by section 19)~~. [s. 23(2)(c)(ii)]

(4) Where processing for a purpose described in sub-paragraph (1) serves at the same time another purpose, the exemption in sub-paragraph (1) is available only where the personal data is processed for a purpose referred to in that sub-paragraph.

Section 15

SCHEDULE 3EXEMPTIONS ETC FROM THE UK GDPR: HEALTH, SOCIAL WORK, EDUCATION AND CHILD ABUSE DATA – NO CHANGES

Section 15

SCHEDULE 4EXEMPTIONS ETC FROM THE UK GDPR: DISCLOSURE PROHIBITED OR RESTRICTED BY AN ENACTMENT – NO CHANGES

Section 17

SCHEDULE 5 ACCREDITATION OF CERTIFICATION PROVIDERS: REVIEWS AND APPEALS – NO CHANGES

SCHEDULE 6THE APPLIED GDPR AND THE APPLIED CHAPTER 2 – NO CHANGES

SCHEDULE 7COMPETENT AUTHORITIES – NO CHANGES

SCHEDULE 8CONDITIONS FOR SENSITIVE PROCESSING UNDER PART 3

Statutory etc purposes

1. This condition is met if the processing—

(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and

(b) is necessary for reasons of substantial public interest.

Administration of justice

2. This condition is met if the processing is necessary for the administration of justice.

Protecting individual's vital interests

3. This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual.

Safeguarding of children and of individuals at risk

4.

(1) This condition is met if—

(a) the processing is necessary for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

Personal data already in the public domain

5. This condition is met if the processing relates to personal data which is manifestly made public by the data subject.

Legal claims

6. This condition is met if the processing—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Judicial acts

7. This condition is met if the processing is necessary when a court or other judicial authority is acting in its judicial capacity.

Preventing fraud

8.

(1) This condition is met if the processing—

(a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and

(b) consists of—

(i) the disclosure of personal data by a competent authority as a member of an anti-fraud organisation,

(ii) the disclosure of personal data by a competent authority in accordance with arrangements made by an anti-fraud organisation,

(iia) the processing of personal data carried out in preparation for disclosure described in sub-paragraph (i) or (ii), or [sch 9. para 24]

(iii) the processing of personal data disclosed as described in sub-paragraph (i) or (ii).

(2) In this paragraph, "anti-fraud organisation" has the same meaning as in section 68 of the Serious Crime Act 2007.

Archiving etc

9. This condition is met if the processing is necessary—

(a) for archiving purposes in the public interest,

(b) for scientific or historical research purposes, or

(c) for statistical purpses.

Section 86

SCHEDULE 9CONDITIONS FOR PROCESSING UNDER PART 4 – NO CHANGES

Section 86

SCHEDULE 10CONDITIONS FOR SENSITIVE PROCESSING UNDER PART 4 – NO CHANGES

Section 112

SCHEDULE 11 OTHER EXEMPTIONS UNDER PART 4

Preliminary

1. In this Schedule, "the listed provisions" means—

(a) Chapter 2 of Part 4 (the data protection principles), except section 86(1)(a) and (2) and Schedules 9 and 10;

(b) Chapter 3 of Part 4 (rights of data subjects);

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

Crime

2. The listed provisions do not apply to personal data processed for any of the following purposes—

(a) the prevention, investigation and detection of crime, or [sch 9. para 25]

(b) the apprehension and prosecution of offenders,

to the extent that the application of the listed provisions would be likely to prejudice any of the matters mentioned in paragraph (a) or (b).

Information required to be disclosed by law etc or in connection with legal proceedings

3.

(1) The listed provisions do not apply to personal data consisting of information that the controller is obliged by an enactment to make available to the public, to the extent that the application of the listed provisions would prevent the controller from complying with that obligation.

(2) The listed provisions do not apply to personal data where disclosure of the data is required by an enactment, a rule of law or the order of a court, to the extent that the application of the listed provisions would prevent the controller from making the disclosure.

(3) The listed provisions do not apply to personal data where disclosure of the data—

(a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights,

to the extent that the application of the listed provisions would prevent the controller from making the disclosure.

Parliamentary privilege

4. The listed provisions do not apply to personal data where this is required for the purpose of avoiding an infringement of the privileges of either House of Parliament.

Judicial proceedings

5. The listed provisions do not apply to personal data to the extent that the application of the listed provisions would be likely to prejudice judicial proceedings.

Crown honours and dignities

6. The listed provisions do not apply to personal data processed for the purposes of the conferring by the Crown of any honour or dignity.

Armed forces

7. The listed provisions do not apply to personal data to the extent that the application of the listed provisions would be likely to prejudice the combat effectiveness of any of the armed forces of the Crown.

Economic well-being

8. The listed provisions do not apply to personal data to the extent that the application of the listed provisions would be likely to prejudice the economic well-being of the United Kingdom.

Legal professional privilege

9. The listed provisions do not apply to personal data that consists of—

(a) information in respect of which a claim to legal professional privilege or, in Scotland, confidentiality of communications, could be maintained in legal proceedings, or

(b) information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser.

Negotiations

10. The listed provisions do not apply to personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject to the extent that the application of the listed provisions would be likely to prejudice the negotiations.

Confidential references given by the controller

11. The listed provisions do not apply to personal data consisting of a reference given (or to be given) in confidence by the controller for the purposes of—
    (a) the education, training or employment (or prospective education, training or employment) of the data subject,
    (b) the appointment (or prospective appointment) of the data subject to any office, or
    (c) the provision (or prospective provision) by the data subject of any service.

Exam scripts and marks

12.
    (1) The listed provisions do not apply to personal data consisting of information recorded by candidates during an exam.
    (2) Where personal data consists of marks or other information processed by a controller—
        (a) for the purposes of determining the results of an exam, or
        (b) in consequence of the determination of the results of an exam,

        section 94 has effect subject to sub-paragraph (3).
    (3) Where the relevant time falls before the results of the exam are announced, the period mentioned in section 94(10)(b) is extended until the earlier of—
        (a) the end of the period of 5 months beginning with the relevant time, and
        (b) the end of the period of 40 days beginning with the announcement of the results.
    (4) In this paragraph—
        "exam" means an academic, professional or other examination used for determining the knowledge, intelligence, skill or ability of a candidate and may include an exam consisting of an assessment of the candidate's performance while undertaking work or any other activity;

        "the relevant time" has the same meaning as in section 94.
    (5) For the purposes of this paragraph, the results of an exam are treated as announced when they are first published or, if not published, first communicated to the candidate.

Research and statistics

13.
    (1) The listed provisions do not apply to personal data processed for—
        (a) scientific or historical research purposes, or
        (b) statistical purposes,

to the extent that the application of those provisions would prevent or seriously impair the achievement of the purposes in question.

(2) The exemption in sub-paragraph (1) is available only where—

(a) the personal data is processed subject to appropriate safeguards for the rights and freedoms of data subjects, and

(b) the results of the research or any resulting statistics are not made available in a form which identifies a data subject.

Archiving in the public interest

14.

(1) The listed provisions do not apply to personal data processed for archiving purposes in the public interest to the extent that the application of those provisions would prevent or seriously impair the achievement of those purposes.

(2) The exemption in sub-paragraph (1) is available only where the personal data is processed subject to appropriate safeguards for the rights and freedoms of data subjects.

~~SCHEDULE 12THE INFORMATION COMMISSIONER~~

~~*Status and capacity*~~

~~1(1)The Commissioner is to continue to be a corporation sole.~~

~~(2)The Commissioner and the Commissioner's officers and staff are not to be regarded as servants or agents of the Crown.~~

~~*Appointment*~~

~~2(1)The Commissioner is to be appointed by Her Majesty by Letters Patent.~~

~~(2)No recommendation may be made to Her Majesty for the appointment of a person as the Commissioner unless the person concerned has been selected on merit on the basis of fair and open competition.~~

~~(3)The Commissioner is to hold office for such term not exceeding 7 years as may be determined at the time of the Commissioner's appointment, subject to paragraph 3.~~

~~(4)A person cannot be appointed as the Commissioner more than once.~~

~~*Resignation and removal*~~

~~3(1)The Commissioner may be relieved of office by Her Majesty at the Commissioner's own request.~~

~~(2)The Commissioner may be removed from office by Her Majesty on an Address from both Houses of Parliament.~~

~~(3)No motion is to be made in either House of Parliament for such an Address unless a Minister of the Crown has presented a report to that House stating that the Minister is satisfied that one or both of the following grounds is made out—~~

~~(a)the Commissioner is guilty of serious misconduct;~~

~~(b)the Commissioner no longer fulfils the conditions required for the performance of the Commissioner's functions.~~

~~*Salary etc*~~

~~4(1)The Commissioner is to be paid such salary as may be specified by a resolution of the House of Commons.~~

~~(2)There is to be paid in respect of the Commissioner such pension as may be specified by a resolution of the House of Commons.~~

~~(3)A resolution for the purposes of this paragraph may—~~

~~(a)specify the salary or pension,~~

~~(b)specify the salary or pension and provide for it to be increased by reference to such variables as may be specified in the resolution, or~~

~~(c)provide that the salary or pension is to be the same as, or calculated on the same basis as, that payable to, or in respect of, a person employed in a specified office under, or in a specified capacity in the service of, the Crown.~~

~~(4)A resolution for the purposes of this paragraph may take effect from—~~

~~(a)the date on which it is passed, or~~

~~(b)from an earlier date or later date specified in the resolution.~~

~~(5)A resolution for the purposes of this paragraph may make different provision in relation to the pension payable to, or in respect of, different holders of the office of Commissioner.~~

~~(6)A salary or pension payable under this paragraph is to be charged on and issued out of the Consolidated Fund.~~

~~(7)In this paragraph, "pension" includes an allowance or gratuity and a reference to the payment of a pension includes a reference to the making of payments towards the provision of a pension.~~

~~*Officers and staff*~~

~~5(1)The Commissioner—~~

~~(a)must appoint one or more deputy commissioners, and~~

~~(b)may appoint other officers and staff.~~

~~(2)The Commissioner is to determine the remuneration and other conditions of service of people appointed under this paragraph.~~

~~(3)The Commissioner may pay pensions, allowances or gratuities to, or in respect of, people appointed under this paragraph, including pensions, allowances or gratuities paid by way of compensation in respect of loss of office or employment.~~

~~(4)The references in sub-paragraph (3) to paying pensions, allowances or gratuities includes making payments towards the provision of pensions, allowances or gratuities.~~

~~(5)In making appointments under this paragraph, the Commissioner must have regard to the principle of selection on merit on the basis of fair and open competition.~~

~~(6)The Employers' Liability (Compulsory Insurance) Act 1969 does not require insurance to be effected by the Commissioner.~~

~~*Carrying out of the Commissioner's functions by officers and staff*~~

~~6(1)The functions of the Commissioner are to be carried out by the deputy commissioner or deputy commissioners if—~~

~~(a)there is a vacancy in the office of the Commissioner, or~~

~~(b)the Commissioner is for any reason unable to act.~~

~~(2)When the Commissioner appoints a second or subsequent deputy commissioner, the Commissioner must specify which deputy commissioner is to carry out which of the Commissioner's functions in the circumstances referred to in sub-paragraph (1).~~

~~(3)A function of the Commissioner may, to the extent authorised by the Commissioner, be carried out by any of the Commissioner's officers or staff.~~

~~*Authentication of the seal of the Commissioner*~~

~~7The application of the seal of the Commissioner is to be authenticated by—~~

~~(a)the Commissioner's signature, or~~

~~(b)the signature of another person authorised for the purpose.~~

~~*Presumption of authenticity of documents issued by the Commissioner*~~

~~8A document purporting to be an instrument issued by the Commissioner and to be—~~

~~(a)duly executed under the Commissioner's seal, or~~

~~(b)signed by or on behalf of the Commissioner,~~

~~is to be received in evidence and is to be deemed to be such an instrument unless the contrary is shown.~~

~~*Money*~~

~~9The Secretary of State may make payments to the Commissioner out of money provided by Parliament.~~

~~*Fees etc and other sums*~~

~~10(1)All fees, charges, penalties and other sums received by the Commissioner in carrying out the Commissioner's functions are to be paid by the Commissioner to the Secretary of State.~~

~~(2)Sub-paragraph (1) does not apply where the Secretary of State, with the consent of the Treasury, otherwise directs.~~

~~(3)Any sums received by the Secretary of State under sub-paragraph (1) are to be paid into the Consolidated Fund.~~

~~*Accounts*~~

~~11(1)The Commissioner must—~~

~~(a)keep proper accounts and other records in relation to the accounts, and~~

~~(b)prepare in respect of each financial year a statement of account in such form as the Secretary of State may direct.~~

~~(2)The Commissioner must send a copy of the statement to the Comptroller and Auditor General—~~

~~(a)on or before 31 August next following the end of the year to which the statement relates, or~~

~~(b)on or before such earlier date after the end of that year as the Treasury may direct.~~

~~(3)The Comptroller and Auditor General must examine, certify and report on the statement.~~

~~(4)The Commissioner must arrange for copies of the statement and the Comptroller and Auditor General's report to be laid before Parliament.~~

~~(5)In this paragraph, "financial year" means a period of 12 months beginning with 1 April.~~

~~*Scotland*~~

~~12Paragraphs 1(1), 7 and 8 do not extend to Scotland.~~ [s. 101(7)]

SCHEDULE 12A THE INFORMATION COMMISSION

Section 114A

Status

1.

(1) The Commission is not to be regarded—

(a) as a servant or agent of the Crown, or

(b) as enjoying any status, immunity or privilege of the Crown.

(2) The Commission's property is not to be regarded—

(a) as property of the Crown, or

(b) as property held on behalf of the Crown.

Number of members

2.

(1) The number of members of the Commission is to be determined by the Secretary of State.

(2) That number must not be—

(a) less than 3, or

(b) more than 14.

(3) The Secretary of State may by regulations substitute a different number for the number for the time being specified in sub-paragraph (2)(b).

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

Membership: general

3.

(1) The Commission is to consist of—

(a) the non-executive members, and

(b) the executive members.

(2) The non-executive members are—

(a) a chair appointed by His Majesty by Letters Patent on the recommendation of the Secretary of State, and

(b) such other members as the Secretary of State may appoint.

(3) The executive members are—

(a) a chief executive appointed by the non-executive members, and

(b) such other members, if any, as the non-executive members may appoint.

(4) The non-executive members must consult the Secretary of State before appointing the chief executive.

(5) The non-executive members must consult the chief executive about whether there should be any executive members within sub-paragraph (3)(b) and, if so, how many there should be.

(6) The Secretary of State may by direction set a maximum and a minimum number of executive members.

(7) The Commission may appoint one of the non-executive members as a deputy to the chair.

Membership: non-executive members to outnumber executive members

4. The Secretary of State must exercise the powers conferred on the Secretary of State by paragraphs 2 and 3 so as to secure that the number of non-executive members of the Commission is, so far as practicable, at all times greater than the number of executive members.

Membership: selection on merit etc

5.

(1) The Secretary of State may not recommend a person for appointment as the chair of the Commission unless the person has been selected on merit on the basis of fair and open competition.

(2) A person may not be appointed as a member of the Commission unless the person has been selected on merit on the basis of fair and open competition.

Membership: conflicts of interests

6.

(1) Before—

(a) recommending a person for appointment as the chair of the Commission, or

(b) appointing a person as a non-executive member of the Commission,

the Secretary of State must be satisfied that the person does not have a conflict of interest.

(2) The Secretary of State must check from time to time that none of the non-executive members has a conflict of interest.

(3) The Secretary of State may require a non-executive member to provide whatever information the Secretary of State considers necessary for the purpose of checking that the member does not have a conflict of interest.

(4) A non-executive member who is required to provide information under sub-paragraph (3) must provide it within such period as may be specified by the Secretary of State.

(5) In this Schedule, "conflict of interest", in relation to a person, means a financial or other interest which is likely to affect prejudicially the discharge by the person of the person's functions as a member of the Commission.

Tenure of the chair

7.

(1) The chair of the Commission holds and vacates office in accordance with the terms of the chair's appointment, subject to the provisions of this paragraph.

(2) The chair must be appointed for a term of not more than 7 years.

(3) On the recommendation of the Secretary of State, His Majesty may by Letters Patent extend the term of the chair's appointment but not so the term as extended is more than 7 years.

(4) A person cannot be appointed as the chair more than once.

(5) The chair may be relieved from office by His Majesty at the chair's own request.

(6) The chair may be removed from office by His Majesty on an Address from both Houses of Parliament.

(7) No motion is to be made in either House of Parliament for such an Address unless the Secretary of State has presented a report to that House stating that the Secretary of State is satisfied that—

(a) the chair is guilty of serious misconduct,

(b) the chair has a conflict of interest (see paragraph 6(5)),

(c) the chair has failed to comply with paragraph 6(4), or

(d) the chair is unable, unfit or unwilling to carry out the chair's functions.

Tenure of deputy chair

8.

(1) A deputy chair of the Commission may resign that office by giving written notice to the Commission.

(2) A deputy chair of the Commission ceases to hold that office on ceasing to be a non-executive member of the Commission.

(3) A deputy chair of the Commission may be removed from that office by the Commission.

Tenure of the other non-executive members

9.

(1) This paragraph applies to a non-executive member of the Commission appointed by the Secretary of State.

(2) The member holds and vacates office in accordance with the terms of their appointment, subject to the provisions of this paragraph.

(3) The member must be appointed for a term of not more than 7 years.

(4) The Secretary of State may extend the term of the member's appointment but not so that the term as extended is more than 7 years.

(5) The Secretary of State may not appoint the member as a nonexecutive member of the Commission on a subsequent occasion.

(6) The member may resign from office by giving written notice to the Secretary of State and the Commission.

(7) The Secretary of State may remove the member from office by written notice if satisfied that—

(a) the member is guilty of serious misconduct,

(b) the member has a conflict of interest (see paragraph 6(5)),

(c) the member has failed to comply with paragraph 6(4), or

(d) the member is unable, unfit or unwilling to carry out the member's functions.

(8) At the time of removing the member from office the Secretary of State must make public the decision to do so.

(9) The Secretary of State must—

(a) give the member a statement of reasons for the removal, and

(b) if asked to do so by the member, publish the statement.

Remuneration and pensions of non-executive members

10.

(1) The Commission may pay to the non-executive members of the Commission such remuneration and allowances as the Secretary of State may determine.

(2) The Commission may pay, or make provision for paying, to or in respect of the non-executive members of the Commission, such sums by way of pensions, allowances or gratuities (including pensions, allowances or gratuities paid by way of compensation in respect of loss of office) as the Secretary of State may determine.

(3) The Commission may make a payment to a person of such amount as the Secretary of State may determine where—

(a) the person ceases to be a non-executive member of the Commission otherwise than on the expiry of the person's term of office, and

(b) it appears to the Secretary of State that there are special circumstances which make it appropriate for the person to receive compensation.

Executive members: terms and conditions

11.

(1) The executive members of the Commission are to be employees of the Commission.

(2) The executive members are to be employed by the Commission on such terms and conditions, including those as to remuneration, as the non-executive members of the Commission may determine.

(3) The Commission must—

(a) pay to or in respect of the executive members of the Commission such pensions, allowances or gratuities (including pensions, allowances or gratuities paid by way of compensation in respect of loss of office) as the nonexecutive members of the Commission may determine, and

(b) provide and maintain for them such pension schemes (whether contributory or not) as the non-executive members of the Commission may determine.

Other staff: appointment, terms and conditions

12.

(1) The Commission may—

(a) appoint other employees, and

(b) make such other arrangements for the staffing of the Commission as it considers appropriate.

(2) In appointing an employee, the Commission must have regard to the principle of selection on merit on the basis of fair and open competition.

(3) Employees appointed by the Commission are to be appointed on such terms and conditions, including those as to remuneration, as the Commission may determine.

(4) The Commission may—

(a) pay to or in respect of those employees such pensions, allowances or gratuities (including pensions, allowances or gratuities paid by way of compensation in respect of loss of employment) as the Commission may determine, and

(b) provide and maintain for them such pension schemes (whether contributory or not) as the Commission may determine.

Committees

13.

(1) The Commission may establish committees.

(2) A committee of the Commission may consist of or include persons who are neither members nor employees of the Commission.

(3) But a committee of the Commission to which functions are delegated under paragraph 14(1)(c) must include at least one person who is either a member or an employee of the Commission.

(4) Where a person who is neither a member nor an employee of the Commission is a member of a committee of the Commission, the Commission may pay to that person such remuneration and expenses as it may determine.

Delegation of functions

14.

(1) The Commission may delegate any of its functions to—

(a) a member of the Commission,

(b) an employee of the Commission, or

(c) a committee of the Commission.

(2) A function is delegated under sub-paragraph (1) to the extent and on the terms that the Commission determines.

(3) A committee of the Commission may delegate any function delegated to it to a member of the committee.

(4) A function is delegated under sub-paragraph (3) to the extent and on the terms that the committee determines.

(5) The power of a committee of the Commission to delegate a function, and to determine the extent and terms of the delegation, is subject to the Commission's power to direct what a committee established by it may and may not do.

(6) The delegation of a function by the Commission or a committee of the Commission under this paragraph does not prevent the Commission or the committee from exercising that function.

Advice from committees

15. The Commission may require a committee of the Commission to give the Commission advice about matters relating to the discharge of the Commission's functions.

Proceedings

16.

(1) The Commission may make arrangements for regulating—

(a) its own procedure, and

(b) the procedure of a committee of the Commission.

(2) The non-executive members of the Commission may by majority make arrangements for regulating the procedure for the carrying out of the separate functions which are conferred on them under this Schedule.

(3) Arrangements under this paragraph may include arrangements as to quorum and the making of decisions by a majority.

(4) The Commission must publish arrangements which it makes under this paragraph.

(5) This paragraph is subject to paragraph 18.

Records of proceedings

17. The Commission must make arrangements for the keeping of proper records of—

(a) its proceedings,

(b) the proceedings of a committee of the Commission,

(c) the proceedings at a meeting of the non-executive members of the Commission,

(d) anything done by a member or employee of the Commission under paragraph 14(1), and

(e) anything done by a member of a committee of the Commission under paragraph 14(3).

Disqualification for acting in relation to certain matters

18.

(1) This paragraph applies if—

(a) a member of the Commission has a direct or indirect interest in a matter falling to be considered at a meeting of the Commission,

(b) a non-executive member of the Commission has a direct or indirect interest in a matter falling to be considered at a meeting of the non-executive members, or

(c) a member of a committee of the Commission has a direct or indirect interest in a matter falling to be considered at a meeting of the committee.

(2) The member with the interest must declare it.

(3) The declaration must be recorded in the minutes of the meeting.

(4) The member with the interest may not take part in a discussion or decision at the meeting relating to the matter, unless—

(a) in the case of a meeting of the Commission, the other members of the Commission who are present have resolved unanimously that the interest is to be disregarded,

(b) in the case of a meeting of the non-executive members, the other non-executive members who are present have so resolved, or

(c) in the case of a meeting of a committee, the other members of the committee who are present have so resolved in the manner authorised by the Commission.

(5) In giving authorisation for the purposes of sub-paragraph (4)(c), the Commission must secure that a resolution for those purposes does not allow a member to take part in a discussion or decision at a meeting of a committee to which functions are delegated under paragraph 14(1)(c) unless the number of other members of the committee in favour of the resolution—

(a) is not less than two thirds of those who are both present and entitled to vote on the resolution, and

(b) is not less than its quorum.

(6) For the purposes of this paragraph, a notification given at or sent to a meeting of the Commission that a person—

(a) is a member of a company or firm, and

(b) is to be regarded as interested in any matter involving that company or firm,

is to be regarded as compliance with sub-paragraph (2) in relation to any such matter for the purposes of that meeting and subsequent meetings of the Commission, of the non-executive members or of a committee.

(7) For the purposes of this paragraph, a notification given at or sent to a meeting of the non-executive members of the Commission or of a committee of the Commission that—

(a) a person is a member of a company or firm, and

(b) is to be regarded as interested in any matter involving that company or firm,

is to be regarded as compliance with sub-paragraph (2) in relation to any such matter for the purposes of that meeting and subsequent meetings of the non-executive members or (as the case may be) of the committee.

(8) A notification described in sub-paragraph (6) or (7) remains in force until it is withdrawn.

(9) A person required to make a declaration for the purposes of this paragraph in relation to any meeting—

(a) is not required to attend the meeting, but

(b) is to be taken to have complied with the requirements of this paragraph if the person takes reasonable steps to secure that notice of the person's interest is read out, and taken into consideration, at the meeting in question.

Validity of proceedings

19.

(1) The validity of proceedings of the Commission, of the nonexecutive members of the Commission or of a committee of the Commission is not affected by—

(a) a vacancy in the membership of the Commission or of the committee,

(b) a defect in the appointment of a member of the Commission,

(c) a failure of the Secretary of State to comply with the requirements of paragraph 4, or

(d) a failure to comply with arrangements under paragraph 16 or with a requirement under paragraph 18.

(2) Nothing in sub-paragraph (1)(d) validates proceedings of a meeting which is inquorate unless it is inquorate by reason only of a matter within sub-paragraph (1)(b) or (c).

Money

20. The Secretary of State may make payments to the Commission.

Fees etc and other sums

21.

(1) All fees, charges, penalties and other sums received by the Commission in carrying out its functions are to be paid to the Secretary of State.

(2) Sub-paragraph (1) does not apply where the Secretary of State otherwise directs.

(3) Any sums received by the Secretary of State under this paragraph are to be paid into the Consolidated Fund.

Accounts

22.

(1) The Commission must keep proper accounts and proper records in relation to them.

(2) The Commission must prepare a statement of accounts in respect of each financial year in the form specified by the Secretary of State.

(3) The Commission must send a copy of each statement of accounts to the Secretary of State and the Comptroller and Auditor General before the end of August next following the financial year to which the statement relates.

(4) The Comptroller and Auditor General must—

(a) examine, certify and report on the statement of accounts, and

(b) send a copy of the certified statement and the report to the Secretary of State.

(5) The Secretary of State must lay before Parliament each document received under sub-paragraph (4)(b).

(6) In this paragraph "financial year" means—

(a) the period beginning with the date on which the Commission is established and ending with the 31 March following that date, and

(b) each successive period of 12 months.

Authentication of seal and presumption of authenticity of documents

23.

(1) The application of the Commission's seal must be authenticated by the signature of—

(a) the chair of the Commission, or

(b) another person authorised for that purpose by the Commission.

(2) A document purporting to be duly executed under the Commission's seal or signed on its behalf—

(a) is to be received in evidence, and

(b) is to be taken to be executed or signed in that way, unless the contrary is shown.

(3) This paragraph does not extend to Scotland.

Interpretation

24. In this Schedule—

(a) references to pensions, allowances or gratuities include references to any similar benefits provided on death or retirement; and

(b) references to the payment of pensions, allowances or gratuities to or in respect of a person includes references to the making of payments towards the provision of pensions, allowances or gratuities to be paid to or in respect of a person.

[sch. 13 para 1]

SCHEDULE 13 OTHER GENERAL FUNCTIONS OF THE COMMISSIONER – NO CHANGES
SCHEDULE 14CO-OPERATION AND MUTUAL ASSISTANCE – NO CHANGES
SCHEDULE 15POWERS OF ENTRY AND INSPECTION – NO CHANGES

SCHEDULE 16PENALTIES

Meaning of "penalty"

1. In this Schedule, "penalty" means a penalty imposed by a penalty notice.

Notice of intent to impose penalty

2.

(1) Before giving a person a penalty notice, the Commissioner must, by written notice (a "notice of intent") inform the person that the Commissioner intends to give a penalty notice.

~~(2) The Commissioner may not give a penalty notice to a person in reliance on a notice of intent after the end of the period of 6 months beginning when the notice of intent is given, subject to sub-paragraph (3).~~

~~(3) The period for giving a penalty notice to a person may be extended by agreement between the Commissioner and the person.~~ [s.37(2)]

Contents of notice of intent

3.

(1) A notice of intent must contain the following information—

(a) the name and address of the person to whom the Commissioner proposes to give a penalty notice;

(b) the reasons why the Commissioner proposes to give a penalty notice (see sub-paragraph (2));

(c) an indication of the amount of the penalty the Commissioner proposes to impose, including any aggravating or mitigating factors that the Commissioner proposes to take into account.

(2) The information required under sub-paragraph (1)(b) includes—

(a) a description of the circumstances of the failure, and

(b) where the notice is given in respect of a failure described in section 149(2), the nature of the personal data involved in the failure.

(3) A notice of intent must also—

(a) state that the person may make written representations about the Commissioner's intention to give a penalty notice, and

(b) specify the period within which such representations may be made.

(4) The period specified for making written representations must be a period of not less than 21 days beginning when the notice of intent is given.

(5) If the Commissioner considers that it is appropriate for the person to have an opportunity to make oral representations about the Commissioner's intention to give a penalty notice, the notice of intent must also—

(a) state that the person may make such representations, and

(b) specify the arrangements for making such representations and the time at which, or the period within which, they may be made.

Giving a penalty notice

4.

(A1) This paragraph applies where the Commissioner gives a notice of intent to a person.

(B1) Within the period of 6 months beginning with the day the notice is given, or as soon as reasonably practicable thereafter, the Commission must give to the person—

(a) a penalty notice, or

(b) written notice that the Commissioner has decided not to give a penalty notice to the person.

(1) But the Commissioner may not give a penalty notice to the person before a time, or before the end of a period, specified in the notice of intent for making oral or written representations.

(2) When deciding whether to give a penalty notice to ~~a~~ the person and determining the amount of the penalty, the Commissioner must consider any oral or written representations made by the person in accordance with the notice of intent. [s. 37(3)]

Contents of penalty notice

5.

(1) A penalty notice must contain the following information—

(a) the name and address of the person to whom it is addressed;

(b) details of the notice of intent given to the person;

(c) whether the Commissioner received oral or written representations in accordance with the notice of intent;

(d) the reasons why the Commissioner proposes to impose the penalty (see sub-paragraph (2));

(e) the reasons for the amount of the penalty, including any aggravating or mitigating factors that the Commissioner has taken into account;

(f) details of how the penalty is to be paid;

(g) details of the rights of appeal under section 162;

(h) details of the Commissioner's enforcement powers under this Schedule.

(2) The information required under sub-paragraph (1)(d) includes—

(a) a description of the circumstances of the failure, and

(b) where the notice is given in respect of a failure described in section 149(2), the nature of the personal data involved in the failure.

Period for payment of penalty

6.

(1) A penalty must be paid to the Commissioner within the period specified in the penalty notice.

(2) The period specified must be a period of not less than 28 days beginning when the penalty notice is given.

Variation of penalty

7.

(1) The Commissioner may vary a penalty notice by giving written notice (a "penalty variation notice") to the person to whom it was given.

(2) A penalty variation notice must specify—

(a) the penalty notice concerned, and

(b) how it is varied.

(3) A penalty variation notice may not—

(a) reduce the period for payment of the penalty;

(b) increase the amount of the penalty;

(c) otherwise vary the penalty notice to the detriment of the person to whom it was given.

(4) If—

(a) a penalty variation notice reduces the amount of the penalty, and

(b) when that notice is given, an amount has already been paid that exceeds the amount of the reduced penalty,

the Commissioner must repay the excess.

Cancellation of penalty

8.

(1) The Commissioner may cancel a penalty notice by giving written notice to the person to whom it was given.

(2) If a penalty notice is cancelled, the Commissioner—

(a) may not take any further action under section 155 or this Schedule in relation to the failure to which that notice relates, and

(b) must repay any amount that has been paid in accordance with that notice.

Enforcement of payment

9.

(1) The Commissioner must not take action to recover a penalty unless—

(a) the period specified in accordance with paragraph 6 has ended,

(b) any appeals against the penalty notice have been decided or otherwise ended,

(c) if the penalty notice has been varied, any appeals against the penalty variation notice have been decided or otherwise ended, and

(d) the period for the person to whom the penalty notice was given to appeal against the penalty, and any variation of it, has ended.

(2) In England and Wales, a penalty is recoverable—

(a) if the county court so orders, as if it were payable under an order of that court;

(b) if the High Court so orders, as if it were payable under an order of that court.

(3) In Scotland, a penalty may be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

(4) In Northern Ireland, a penalty is recoverable—

(a) if a county court so orders, as if it were payable under an order of that court

(b) if the High Court so orders, as if it were payable under an order of that court.

Section 178

SCHEDULE 17 REVIEW OF PROCESSING OF PERSONAL DATA FOR THE PURPOSES OF JOURNALISM

Interpretation

1. In this Schedule—

"relevant period" means—

(a) the period of 18 months beginning when the Commissioner starts the first review under section 178, and
(b) the period of 12 months beginning when the Commissioner starts a subsequent review under that section;

"the relevant review", in relation to a relevant period, means the review under section 178 which the Commissioner must produce a report about by the end of that period.

Information notices

2.

(1) This paragraph applies where the Commissioner gives an information notice during a relevant period.

(2) If the information notice—

(a) states that, in the Commissioner's opinion, the information or documents are required for the purposes of the relevant review, and

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

subsections (5) and (6) of section 142 do not apply but the notice must not require the information or documents to be provided before the end of the period of 24 hours beginning when the notice is given. [s. 34(7)]

Assessment notices

3.

(1) Sub-paragraph (2) applies where the Commissioner gives an assessment notice to a person during a relevant period.

(2) If the 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 for the purposes of the relevant review, and

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

subsections (6) and (7) of section 146 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 when the notice is given.

(3) During a relevant period, section 147 has effect as if for subsection (5) there were substituted—

"(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 unless a determination under section 174 with respect to the data or the processing has taken effect."

Interview notices

3A

(1) Sub-paragraph (2) applies where the Commissioner gives an interview notice to an individual during a relevant period.

(2) If the interview notice—

(a) states that, in the Commissioner's opinion, it is necessary for the individual to comply with a requirement in the notice for the purposes of the relevant review, and

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

subsections (6) and (7) of section 148A do not apply but the notice must not require the individual to comply with the requirement before the end of the period of 24 hours beginning when the notice is given.

(3) During a relevant period, section 148B has effect as if for subsection (8) there were substituted—

"(8) The Commissioner may not give an individual an interview notice with respect to the processing of personal data for the special purposes unless a determination under section 174 with respect to the data or the processing has taken effect. [s. 36(11)(a)]

Applications in respect of urgent notices

4. Section 164 applies where an information notice, assessment notice or interview notice ~~or assessment notice~~ contains a statement under paragraph 2(2)(a) ~~or~~ 3(2)(a), or 3A(2)(a) as it applies where such a notice contains a statement under section 142(7)(a) ~~or~~ 146(8)(a) or 148A(8)(a). [s. 36(11)(b)]

SCHEDULE 18RELEVANT RECORDS – NO CHANGES
SCHEDULE 19MINOR AND CONSEQUENTIAL AMENDMENTS – NO CHANGES

SCHEDULE 20TRANSITIONAL PROVISION ETC

PART 1GENERAL
Interpretation

1.

(1) In this Schedule—

"the 1984 Act" means the Data Protection Act 1984;

"the 1998 Act" means the Data Protection Act 1998;

"the 2014 Regulations" means the Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 (S.I. 2014/3141);

"data controller" has the same meaning as in the 1998 Act (see section 1 of that Act);

"the old data protection principles" means the principles set out in—

(a) Part 1 of Schedule 1 to the 1998 Act, and
(b)regulation 30 of the 2014 Regulations.

(2) A provision of the 1998 Act that has effect by virtue of this Schedule is not, by virtue of that, part of the data protection legislation (as defined in section 3).

PART 2 RIGHTS OF DATA SUBJECTS – NO CHANGES
PART 3THE UK GDPR AND PART 2 OF THIS ACT – NO CHANGES
PART 4LAW ENFORCEMENT AND INTELLIGENCE SERVICES PROCESSING – NO CHANGES
PART 5NATIONAL SECURITY CERTIFICATES – NO CHANGES
PART 6THE INFORMATION COMMISSIONER – NO CHANGES
PART 7ENFORCEMENT ETC UNDER THE 1998 ACT – NO CHANGES
PART 8ENFORCEMENT ETC UNDER THIS ACT – NO CHANGES

PART 9OTHER ENACTMENTS

Powers to disclose information to the Commissioner

47.

(1) The following provisions (as amended by Schedule 19 to this Act) have effect after the relevant time as if the matters they refer to included a matter in respect of which the Commissioner could exercise a power conferred by a provision of Part 5 of the 1998 Act, as it has effect by virtue of this Schedule—

(a) section 11AA(1)(a) of the Parliamentary Commissioner Act 1967 (disclosure of information by Parliamentary Commissioner);

(b) sections 33A(1)(a) and 34O(1)(a) of the Local Government Act 1974 (disclosure of information by Local Commissioner);

(c) section 18A(1)(a) of the Health Service Commissioners Act 1993 (disclosure of information by Health Service Commissioner);

(d) paragraph 1 of the entry for the Information Commissioner in Schedule 5 to the Scottish Public Services Ombudsman Act 2002 (asp 11) (disclosure of information by the Ombudsman);

(e) section 34X(3)(a) of the Public Services Ombudsman (Wales) Act 2005 (disclosure of information by the Ombudsman);

(f) section 18(6)(a) of the Commissioner for Older People (Wales) Act 2006 (disclosure of information by the Commissioner);

(g) section 22(3)(a) of the Welsh Language (Wales) Measure 2011 (nawm 1) (disclosure of information by the Welsh Language Commissioner);

(h) section 49(3)(a) of the Public Services Ombudsman Act (Northern Ireland) 2016 (c. 4 (N.I.))(disclosure of information by the Ombudsman);

(i) section 44(3)(a) of the Justice Act (Northern Ireland) 2016 (c. 21 (N.I.)) (disclosure of information by the Prison Ombudsman for Northern Ireland).

(2) The following provisions (as amended by Schedule 19 to this Act) have effect after the relevant time as if the offences they refer to included an offence under any provision of the

1998 Act other than paragraph 12 of Schedule 9 to that Act (obstruction of execution of warrant)—

(a) section 11AA(1)(b) of the Parliamentary Commissioner Act 1967;

(b) sections 33A(1)(b) and 34O(1)(b) of the Local Government Act 1974;

(c) section 18A(1)(b) of the Health Service Commissioners Act 1993;

(d) paragraph 2 of the entry for the Information Commissioner in Schedule 5 to the Scottish Public Services Ombudsman Act 2002 (asp 11);

(e) section 34X(5) of the Public Services Ombudsman (Wales) Act 2005 (disclosure of information by the Ombudsman);

(f) section 18(8) of the Commissioner for Older People (Wales) Act 2006;

(g) section 22(5) of the Welsh Language (Wales) Measure 2011 (nawm 1);

(h) section 49(5) of the Public Services Ombudsman Act (Northern Ireland) 2016 (c. 4 (N.I.));

(i) section 44(3)(b) of the Justice Act (Northern Ireland) 2016 (c. 21 (N.I.)).

(3) In this paragraph, "the relevant time", in relation to a provision of a section or Schedule listed in sub-paragraph (1) or (2), means the time when the amendment of the section or Schedule by Schedule 19 to this Act comes into force.

Codes etc required to be consistent with the Commissioner's data-sharing code

48.

(1) This paragraph applies in relation to the code of practice issued under each of the following provisions—

(a) section 19AC of the Registration Service Act 1953 (code of practice about disclosure of information by civil registration officials);

(b) section 43 of the Digital Economy Act 2017 (code of practice about disclosure of information to improve public service delivery);

(c) section 52 of that Act (code of practice about disclosure of information to reduce debt owed to the public sector);

(d) section 60 of that Act (code of practice about disclosure of information to combat fraud against the public sector);

(e) section 70 of that Act (code of practice about disclosure of information for research purposes).

(2) During the relevant period, the code of practice does not have effect to the extent that it is inconsistent with the code of practice prepared under section 121 of this Act (data-sharing code) and issued under section 125(4) of this Act (as altered or replaced from time to time).

(3) In this paragraph, "the relevant period", in relation to a code issued under a section mentioned in sub-paragraph (1), means the period—

(a) beginning when the amendments of that section in Schedule 19 to this Act come into force, and

(b) ending when the code is first reissued under that section.

49.

(1) This paragraph applies in relation to the original statement published under section 45E of the Statistics and Registration Service Act 2007 (statement of principles and procedures in connection with access to information by the Statistics Board).

(2) During the relevant period, the statement does not have effect to the extent that it is inconsistent with the code of practice prepared under section 121 of this Act (data-sharing code) and issued under section 125(4) of this Act (as altered or replaced from time to time).

(3) In this paragraph, "the relevant period" means the period—

(a) beginning when the amendments of section 45E of the Statistics and Registration Service Act 2007 in Schedule 19 to this Act come into force, and

(b) ending when the first revised statement is published under that section.

Consumer Credit Act 1974

50. In section 159(1)(a) of the Consumer Credit Act 1974 (correction of wrong information) (as amended by Schedule 19 to this Act), the reference to information given under Article 15(1) to (3) of the UK GDPR includes information given at any time under section 7 of the 1998 Act.

Freedom of Information Act 2000

51. Paragraphs 52 to 55 make provision about the Freedom of Information Act 2000 ("the 2000 Act").

52.

(1) This paragraph applies where a request for information was made to a public authority under the 2000 Act before the relevant time.

(2) To the extent that the request is dealt with after the relevant time, the amendments of sections 2 and 40 of the 2000 Act in Schedule 19 to this Act have effect for the purposes of determining whether the authority deals with the request in accordance with Part 1 of the 2000 Act.

(3) To the extent that the request was dealt with before the relevant time—

(a) the amendments of sections 2 and 40 of the 2000 Act in Schedule 19 to this Act do not have effect for the purposes of determining whether the authority dealt with the request in accordance with Part 1 of the 2000 Act, but

(b) the powers of the Commissioner and the Tribunal, on an application or appeal under the 2000 Act, do not include power to require the authority to take steps which it would not be required to take in order to comply with Part 1 of the 2000 Act as amended by Schedule 19 to this Act.

(4) In this paragraph—

"public authority" has the same meaning as in the 2000 Act;

"the relevant time" means the time when the amendments of sections 2 and 40 of the 2000 Act in Schedule 19 to this Act come into force.

53.

(1) Tribunal Procedure Rules made under paragraph 7(1)(b) of Schedule 6 to the 1998 Act (appeal rights under the 2000 Act) and in force immediately before the relevant time have effect after that time as if they were also made under section 61 of the 2000 Act (as inserted by Schedule 19 to this Act).

(2) In this paragraph, "the relevant time" means the time when the repeal of paragraph 7(1)(b) of Schedule 6 to the 1998 Act comes into force.

54.

(1) The repeal of paragraph 8 of Schedule 6 to the 1998 Act (obstruction etc in proceedings before the Tribunal) does not affect the application of that paragraph after the relevant time in relation to an act or omission before that time in relation to an appeal under the 2000 Act.

(2) In this paragraph, "the relevant time" means the time when the repeal of paragraph 8 of Schedule 6 to the 1998 Act comes into force.

55.

(1) The amendment of section 77 of the 2000 Act in Schedule 19 to this Act (offence of altering etc record with intent to prevent disclosure: omission of reference to section 7 of the 1998 Act) does not affect the application of that section after the relevant time in relation to a case in which—

(a) the request for information mentioned in section 77(1) of the 2000 Act was made before the relevant time, and

(b) when the request was made, section 77(1)(b) of the 2000 Act was satisfied by virtue of section 7 of the 1998 Act.

(2) In this paragraph, "the relevant time" means the time when the repeal of section 7 of the 1998 Act comes into force.

Freedom of Information (Scotland) Act 2002

56.

(1) This paragraph applies where a request for information was made to a Scottish public authority under the Freedom of Information (Scotland) Act 2002 ("the 2002 Act") before the relevant time.

(2) To the extent that the request is dealt with after the relevant time, the amendments of the 2002 Act in Schedule 19 to this Act have effect for the purposes of determining whether the authority deals with the request in accordance with Part 1 of the 2002 Act.

(3) To the extent that the request was dealt with before the relevant time—

(a) the amendments of the 2002 Act in Schedule 19 to this Act do not have effect for the purposes of determining whether the authority dealt with the request in accordance with Part 1 of the 2002 Act, but

(b) the powers of the Scottish Information Commissioner and the Court of Session, on an application or appeal under the 2002 Act, do not include power to require the authority to take steps which it would not be required to take in order to comply with Part 1 of the 2002 Act as amended by Schedule 19 to this Act.

(4) In this paragraph—

"Scottish public authority" has the same meaning as in the 2002 Act;

"the relevant time" means the time when the amendments of the 2002 Act in Schedule 19 to this Act come into force.

Access to Health Records (Northern Ireland) Order 1993 (S.I. 1993/1250 (N.I. 4))

57. Until the first regulations under Article 5(4)(a) of the Access to Health Records (Northern Ireland) Order 1993 (as amended by Schedule 19 to this Act) come into force, the maximum amount of a fee that may be required for giving access under that Article is £10.

Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2450)

58.

(1) The repeal of a provision of the 1998 Act does not affect its operation for the purposes of the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("the PECR 2003") (see regulation~~s~~ 2 of~~, 31 and 31B of, and Schedule 1 to,~~ those Regulations).

[s. 86(9)]

(2) Where subordinate legislation made under a provision of the 1998 Act is in force immediately before the repeal of that provision, neither the revocation of the subordinate legislation nor the repeal of the provision of the 1998 Act affect the application of the subordinate legislation for the purposes of the PECR 2003 after that time.

(3) Part 3 of Schedule 19 to this Act (modifications) does not have effect in relation to the PECR 2003.

(4) Part 7 of this Schedule does not have effect in relation to the provisions of the 1998 Act as applied by the PECR 2003.

Health and Personal Social Services (Quality, Improvement and Regulation) (Northern Ireland) Order 2003 (S.I. 2003/431 (N.I. 9))

59. Part 3 of Schedule 19 to this Act (modifications) does not have effect in relation to the reference to an accessible record within the meaning of section 68 of the 1998 Act in Article 43 of the Health and Personal Social Services (Quality, Improvement and Regulation) (Northern Ireland) Order 2003.

Environmental Information Regulations 2004 (S.I. 2004/3391)

60.

(1) This paragraph applies where a request for information was made to a public authority under the Environmental Information Regulations 2004 ("the 2004 Regulations") before the relevant time.

(2) To the extent that the request is dealt with after the relevant time, the amendments of the 2004 Regulations in Schedule 19 to this Act have effect for the purposes of determining whether the authority deals with the request in accordance with Parts 2 and 3 of those Regulations.

(3) To the extent that the request was dealt with before the relevant time—

(a) the amendments of the 2004 Regulations in Schedule 19 to this Act do not have effect for the purposes of determining whether the authority dealt with the request in accordance with Parts 2 and 3 of those Regulations, but

(b) the powers of the Commissioner and the Tribunal, on an application or appeal under the 2000 Act (as applied by the 2004 Regulations), do not include power to require the authority to take steps which it would not be required to take in order to comply with Parts 2 and 3 of those Regulations as amended by Schedule 19 to this Act.

(4) In this paragraph—

"public authority" has the same meaning as in the 2004 Regulations;

"the relevant time" means the time when the amendments of the 2004 Regulations in Schedule 19 to this Act come into force.

Environmental Information (Scotland) Regulations 2004 (S.S.I. 2004/520)

61.

(1) This paragraph applies where a request for information was made to a Scottish public authority under the Environmental Information (Scotland) Regulations 2004 ("the 2004 Regulations") before the relevant time.

(2) To the extent that the request is dealt with after the relevant time, the amendments of the 2004 Regulations in Schedule 19 to this Act have effect for the purposes of determining whether the authority deals with the request in accordance with those Regulations.

(3) To the extent that the request was dealt with before the relevant time—

(a) the amendments of the 2004 Regulations in Schedule 19 to this Act do not have effect for the purposes of determining whether the authority dealt with the request in accordance with those Regulations, but

(b) the powers of the Scottish Information Commissioner and the Court of Session, on an application or appeal under the 2002 Act (as applied by the 2004 Regulations), do not include power to require the authority to take steps which it would not be

required to take in order to comply with those Regulations as amended by Schedule 19 to this Act.

(4) In this paragraph—

"Scottish public authority" has the same meaning as in the 2004 Regulations;

"the relevant time" means the time when the amendments of the 2004 Regulations in Schedule 19 to this Act come into force.

Section 213

SCHEDULE 21FURTHER TRANSITIONAL PROVISION ETC

PART 1INTERPRETATION

The applied GPDR

1. In this Schedule, "the applied GDPR" means the EU GDPR as applied by Chapter 3 of Part 2 before IP completion day.

PART 2CONTINUATION OF EXISTING ACTS ETC

Merger of the directly applicable GDPR and the applied GDPR

2.

(1) On and after IP completion day, references in an enactment to the UK GDPR (including the reference in the definition of "the data protection legislation" in section 3(9)) include

(a) the EU GDPR as it was directly applicable to the United Kingdom before IP completion day, read with Chapter 2 of Part 2 of this Act as it had effect before IP completion day, and

(b) the applied GDPR, read with Chapter 3 of Part 2 of this Act as it had effect before IP completion day.

(2) On and after IP completion day, references in an enactment to, or to a provision of, Chapter 2 of Part 2 of this Act (including general references to this Act or to Part 2 of this Act) include that Chapter or that provision as applied by Chapter 3 of Part 2 of this Act as it had effect before IP completion day.

(3) Sub-paragraphs (1) and (2) have effect—

(a) in relation to references in this Act, except as otherwise provided;

(b) in relation to references in other enactments, unless the context otherwise requires.

3.

(1) Anything done in connection with the EU GDPR as it was directly applicable to the United Kingdom before IP completion day, the applied GDPR or this Act—

(a) if in force or effective immediately before IP completion day, continues to be in force or effective on and after IP completion day, and

(b) if in the process of being done immediately before IP completion day, continues to be done on and after IP completion day.

(2) References in this paragraph to anything done include references to anything omitted to be done.

PART 3 TRANSFERS TO THIRD COUNTRIES AND INTERNATIONAL ORGANISATIONS

UK GDPR: ~~adequacy decisions and adequacy regulations~~ transfers approved by regulations

[sch. 7 para 22(2)]

4.

(1) On and after IP completion day, for the purposes of the UK GDPR and Part 2 of this Act, a transfer of personal data to a third country or an international organisation is to be treated as approved by regulations made under Article 45A of the UK GDPR ~~based on adequacy regulations~~ if, at the time of the transfer, paragraph 5 specifies, or specifies a description which includes— [sch. 7 para 22(3)(a)]

(a) in the case of a third country, the country or a relevant territory or sector within the country, or

(b) in the case of an international organisation, the organisation.

(2) Sub-paragraph (1) has effect subject to provision in paragraph 5 providing that only particular transfers to the country, territory, sector or organisation may rely on a particular provision of paragraph 5 for the purposes of sub-paragraph (1).

(3) The Secretary of State may by regulations—

(a) repeal sub-paragraphs (1) and (2) and paragraph 5;

(b) amend paragraph 5 so as to omit a third country, territory, sector or international organisation specified, or of a description specified, in that paragraph;

(c) amend paragraph 5 so as to replace a reference to, or description of, a third country, territory, sector or organisation with a narrower reference or description, including by specifying or describing particular transfers of personal data and making provision described in sub-paragraph (2).

(4) Regulations under this paragraph may, among other things——

(a) identify a transfer of personal data by any means, including by reference to the controller or processor, the recipient, the personal data transferred or the means by which the transfer is made or by reference to relevant legislation, schemes, lists or other arrangements or ~~lists or other~~ documents, as they have effect from time to time; [sch. 7 para 22(3)(b)]

(b) confer a discretion on a person.

(5) Regulations under this paragraph are subject to the negative resolution procedure.

~~(6) Sub-paragraphs (1) and (2) have effect in addition to section 17A(2) and (3).~~

[sch. 7 para 22(3)(c)]

5.

(1) The following are specified for the purposes of paragraph 4(1)—

(a) an EEA state;

(b) Gibraltar;

(c) a Union institution, body, office or agency set up by, or on the basis of, the Treaty on the European Union, the Treaty on the Functioning of the European Union or the Euratom Treaty;

(d) an equivalent institution, body, office or agency set up by, or on the basis of, the Treaties establishing the European Economic Area;

(e) a third country which is the subject of a decision listed in sub-paragraph (2), other than a decision that, immediately before IP completion day, had been repealed or was suspended;

(f) a third country, territory or sector within a third country or international organisation which is the subject of an adequacy decision made by the European Commission before IP completion day on the basis of Article 45(3) of the EU GDPR, other than a decision that, immediately before IP completion day, had been repealed or was suspended.

(2) The decisions mentioned in sub-paragraph (1)(e) are the following—

(a) Commission Decision 2000/518/EC of 26th July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland;

(b) Commission Decision 2002/2/EC of 20th December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act;

(c) Commission Decision 2003/490/EC of 30th June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina;

(d) Commission Decision 2003/821/EC of 21st November 2003 on the adequate protection of personal data in Guernsey;

(e) Commission Decision 2004/411/EC of 28th April 2004 on the adequate protection of personal data in the Isle of Man;

(f) Commission Decision 2008/393/EC of 8th May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey;

(g) Commission Decision 2010/146/EU of 5th March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data;

(h) Commission Decision 2010/625/EU of 19th October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra;

(i) Commission Decision 2011/61/EU of 31st January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data;

(j) Commission Implementing Decision 2012/484/EU of 21st August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data;

(k) Commission Implementing Decision 2013/65/EU of 19th December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand;

(l) Commission Implementing Decision (EU) 2019/419 of 23rd January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information.

(3) Where a decision described in sub-paragraph (1)(e) or (f) states that an adequate level of protection of personal data is ensured only for a transfer specified or described in the decision, only such a transfer may rely on that provision and that decision for the purposes of paragraph 4(1).

(4) The references to a decision in sub-paragraphs (1)(e) and (f) and (2) are to the decision as it had effect in EU law immediately before IP completion day, subject to sub-paragraphs (5) and (6).

(5) For the purposes of this paragraph, where a reference to legislation, a list or another document in a decision described in sub-paragraph (1)(e) or (f) is a reference to the legislation, list or document as it has effect from time to time, it is to be treated as a reference to the legislation, list or other document as it has effect at the time of the transfer.

(6) For the purposes of this paragraph, where a decision described in sub-paragraph (1)(e) or (f) relates to—

(a) transfers from the European Union (or the European Community) or the European Economic Area, or

(b) transfers to which the EU GDPR applies,

it is to be treated as relating to equivalent transfers to or from the United Kingdom or transfers to which the UK GDPR applies (as appropriate).

6.

(1) In the provisions listed in sub-paragraph (2)—

(a) references to regulations made under Article 45A of the UK GDPR ~~section 17A~~ (other than references to making such regulations) include the provision made in paragraph 5; [sch. 7 para 22(4)(a)]

(b) references to the revocation of such regulations include the repeal of all or part of paragraph 5.

(2) ~~Those provisions are—~~

(a) ~~Articles 13(1)(f), 14(1)(f), 45(1) and (7), 46(1) and 49(1) of the UK GDPR;~~

(b) ~~sections 17B(1), (3), (6) and (7) and 18(2) of this Act.~~[sch. 7 para 22(4)(b)]

Those provisions are Articles 13(1)(f), 14(1)(f), 45C, 49(1) and 49A(1) of the UK GDPR.

(3) In its application to transfers treated as approved by virtue of paragraph 1, Article 45C(5) of the UK GDPR (transfers approved by regulations: monitoring) has effect as if the reference to Article 45A(4)(b) were omitted. [sch. 7 para 22(4)(c)]

~~*UK GDPR: transfers subject to appropriate safeguards provided by standard data protection clauses*~~

~~7.—~~

~~(1) Subject to paragraph 8, the requirement for safeguards to be provided under Article 46(1A)(a)(i) of the UK GDPR may be satisfied the appropriate safeguards referred to in Article 46(1) of the UK GDPR may be provided for on and after IP completion day as described in this paragraph.~~

~~(2) The safeguards may be provided for by any standard data protection clauses included in an arrangement which, if the arrangement had been entered into immediately before IP completion day, would have provided for the appropriate safeguards referred to in Article 46(1) of the EU GDPR by virtue of Article 46(2)(c) or (d) or (5) of the EU GDPR.~~

~~(3) The safeguards may be provided for by a version of standard data protection clauses described in sub-paragraph (2) incorporating changes where—~~

~~(a) all of the changes are made in consequence of the withdrawal of the United Kingdom from the EU, of or provision made by regulations under section 8 or 23 of the European Union (Withdrawal) Act 2018 or of the amendment of Chapter 5 of the UK GDPR by the Data Protection and Digital Information Act 2022 (or both), and~~

~~(b) none of the changes alters the effect of the clauses.~~

~~(4) The following changes are to be treated as falling within sub-paragraph (3)(a) and (b)—~~

~~(a) changing references to adequacy decisions made by the European Commission into references to equivalent provision made by regulations under section 17A or by or under paragraphs 4 to 6 of this Schedule;~~

~~(aa) changing references to provision made by regulations under section 17A into references to provision made by regulations made under Article 45A of the UK GDPR;~~

~~(b) changing references to transferring personal data outside the European Union or the European Economic Area into references to transferring personal data outside the United Kingdom.~~

~~(5) In the case of a transfer of personal data made under arrangements entered into before IP completion day, the safeguards may be provided for on and after IP completion day by standard data protection clauses not falling within sub-paragraph (2) which—~~

~~(a) formed part of the arrangements immediately before IP completion day, and~~

~~(b) at that time, provided for the appropriate safeguards referred to in Article 46(1) of the EU GDPR by virtue of Article 46(2)(c) or (d) or (5) of the EU GDPR.~~

~~(6) The Secretary of State and the Commissioner must keep the operation of this paragraph under review.~~

~~(7) In this paragraph, "adequacy decision" means a decision made on the basis of—~~

~~(a) Article 45(3) of the EU GDPR, or~~

~~(b) Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.~~

~~(8) This paragraph has effect in addition to Article 46(2) and (3) of the UK GDPR.~~

~~8.~~

~~(1) Paragraph 7 does not apply to the extent that it has been disapplied by—~~

~~(a) regulations made by the Secretary of State, or~~

~~(b) a document issued by the Commissioner.~~

~~(2) Regulations under this paragraph are subject to the negative resolution procedure.~~

~~(3) Subsections (3) to (8) and (10) to (12) of section 119A apply in relation to a document issued by the Commissioner under this paragraph as they apply to a document issued by the Commissioner under section 119A(2).~~ [sch. 7 para 22(5)]

UK GDPR: transfers subject to appropriate safeguards provided by binding corporate rules

9.

(1) ~~The appropriate safeguards referred to in Article 46(1) of the UK GDPR may be provided for~~ The requirement for safeguards to be provided under Article 46(1A)(a)(i) of the UK GDPR may be satisfied on and after IP completion day as described in sub-paragraphs (2) to (4), subject to sub-paragraph (5). [sch. 7 para 22(6)(a)]

(2) The safeguards may be provided for by any binding corporate rules authorised by the Commissioner which, immediately before IP completion day, provided for the appropriate safeguards referred to in Article 46(1) of the EU GDPR by virtue of Article 46(5) of the EU GDPR.

(3) The safeguards may be provided for by a version of binding corporate rules described in sub-paragraph (2) incorporating changes where—

(a) all of the changes are made in consequence of the withdrawal of the United Kingdom from the EU, of ~~or~~ provision made by regulations under section 8 or 23 of the European Union (Withdrawal) Act 2018 or of the amendment of Chapter 5 of the UK GDPR by the Data Protection and Digital Information Act 2023 ~~(or both)~~, and

(b) none of the changes alters the effect of the rules. [sch. 7 para 22(6)(b)]

(4) The following changes are to be treated as falling within sub-paragraph (3)(a) and (b)—

(a) changing references to adequacy decisions made by the European Commission into references to equivalent provision made by regulations under section 17A or by or under paragraphs 4 to 6 of this Schedule;

(aa) changing references to provision made by regulations under section 17A into references to provision made by regulations made under Article 45A of the UK GDPR; [sch. 7 para 22(6)(c)]

(b) changing references to transferring personal data outside the European Union or the European Economic Area into references to transferring personal data outside the United Kingdom.

(5) Sub-paragraphs (2) to (4) cease to apply in relation to binding corporate rules if, on or after IP completion day, the Commissioner withdraws the authorisation of the rules (or, where sub-paragraph (3) is relied on, the authorisation of the rules mentioned in sub-paragraph (2)).

(5A)For the purposes of sub-paragraph (2), binding corporate rules which, immediately before IP completion day, provided for the appropriate safeguards referred to in Article 46(1) of the EU GDPR by virtue of Article 46(5) of the EU GDPR but which were authorised other than by the Commissioner are to be treated as authorised by the Commissioner where—

(a) a valid notification of the rules has been made to the Commissioner,

(b) the Commissioner has approved them, and

(c) that approval has not been withdrawn.

(5B)A notification is valid if it—

(a) is made by a controller or processor established in the United Kingdom,

(b) is made to the Commissioner before the end of the period of 6 months beginning with IP completion day, and

(c) includes—

(i) the name and contact details of the data protection officer or other contact point for the controller or processor, and

(ii) such other information as the Commissioner may reasonably require.

(5C)Where a valid notification is made the Commissioner must, without undue delay—

(a) decide whether or not to approve the rules, and

(b) notify the controller or processor of that decision.

(6) The Commissioner must keep the operation of this paragraph under review.

(7) In this paragraph—

"adequacy decision" means a decision made on the basis of—

(a) Article 45(3) of the EU GDPR, or

(b) Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

"binding corporate rules" has the meaning given in Article 4(20) of the UK GDPR.

(8) This paragraph has effect in addition to Article 46(2) and (3) of the UK GDPR.

Part 3 (law enforcement processing): ~~adequacy decisions and adequacy regulations~~ transfers approved by regulations [sch. 7 para 22(7)]

10.

On and after IP completion day, for the purposes of Part 3 of this Act, a transfer of personal data to a third country or an international organisation is to be treated as approved by regulations made under section 74AA ~~based on adequacy regulations~~ if, at the time of the transfer, paragraph 11 specifies, or specifies a description which includes— [sch. 7 para 22(8)(a)]

(a) in the case of a third country, the country or a relevant territory or sector within the country, or

(b) in the case of an international organisation, the organisation.

(2) Sub-paragraph (1) has effect subject to provision in paragraph 11 providing that only particular transfers to the country, territory, sector or organisation may rely on a particular provision of paragraph 11 for the purposes of sub-paragraph (1).

(3) The Secretary of State may by regulations—

(a) repeal sub-paragraphs (1) and (2) and paragraph 11;

(b) amend paragraph 11 so as to omit a third country, territory, sector or international organisation specified, or of a description specified, in that paragraph;

(c) amend paragraph 11 so as to replace a reference to, or description of, a third country, territory, sector or organisation with a narrower reference or description, including by specifying or describing particular transfers of personal data and by making provision described in sub-paragraph (2).

(4) Regulations under this paragraph may, among other things—

(a) identify a transfer of personal data by any means, including by reference to the controller or processor, the recipient, the personal data transferred or the means by which the transfer is made or by reference to relevant legislation, schemes, lists or

other arrangements or ~~lists or other~~ documents, as they have effect from time to time; [sch. 7 para 22(8)(b)]

(b) confer a discretion on a person.

(5) Regulations under this paragraph are subject to the negative resolution procedure.

(6) ~~Sub-paragraphs (1) and (2) have effect in addition to section 74A(2) and (3).~~ [sch. 7 para 22(8)(c)]

11.

(1) The following are specified for the purposes of paragraph 10(1)—

(a) an EEA state;

(aa)Switzerland;

(b) Gibraltar;

(c) a third country, a territory or sector within a third country or an international organisation which is the subject of an adequacy decision made by the European Commission before IP completion day on the basis of Article 36(3) of the Law Enforcement Directive, other than a decision that, immediately before IP completion day, had been repealed or was suspended.

(2) Where a decision described in sub-paragraph (1)(c) states that an adequate level of protection of personal data is ensured only for a transfer specified or described in the decision, only such a transfer may rely on that provision and that decision for the purposes of paragraph 10(1).

(3) The reference to a decision in sub-paragraph (1)(c) is to the decision as it had effect in EU law immediately before IP completion day, subject to sub-paragraphs (4) and (5).

(4) For the purposes of this paragraph, where a reference to legislation, a list or another document in a decision described in sub-paragraph (1)(c) is a reference to the legislation, list or document as it has effect from time to time, it is to be treated as a reference to the legislation, list or other document as it has effect at the time of the transfer.

(5) For the purposes of this paragraph, where a decision described in sub-paragraph (1)(c) relates to—

(a) transfers from the European Union (or the European Community) or the European Economic Area, or

(b) transfers to which the Law Enforcement Directive applies,

it is to be treated as relating to equivalent transfers from the United Kingdom or transfers to which Part 3 of this Act applies (as appropriate).

12.

(1) In section 74B and 76(A1) ~~(1), (3), (6) and (7)~~

(a) references to regulations made under section 74AA (other than references to making such regulations) include the provision made in paragraph 11;

(b) references to the revocation of such regulations include the repeal of all or part of paragraph 11.

(2) In its application to transfers treated as approved by virtue of paragraph 10, section 74B(7) (transfers approved by regulations: monitoring) has effect as if the reference to section 74AA(4)(b) were omitted. [sch. 7 para 22(9)]

PART 4REPEAL OF PROVISIONS IN CHAPTER 3 OF PART 2 – NO CHANGE
PART 5THE INFORMATION COMMISSIONER – NO CHANGE
PART 6ENFORCEMENT – NO CHANGE