Data Protection Bill [HL]

EXPLANATORY NOTES

Explanatory notes to the Bill, prepared by the Department for Digital, Culture, Media and Sport and the Home Office, are published separately as HL Bill 66—EN.

EUROPEAN CONVENTION ON HUMAN RIGHTS

Lord Ashton of Hyde has made the following statement under section 19(1)(a) of the Human Rights Act 1998:

In my view the provisions of the Data Protection Bill [HL] are compatible with the Convention rights.

Data Protection Bill [HL]

CONTENTS

PART 1

PRELIMINARY

1 Overview
2 Terms relating to the processing of personal data

PART 2

GENERAL PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

3 Processing to which this Part applies
4 Definitions

CHAPTER 2

THE GDPR

Meaning of certain terms used in the GDPR

5 Meaning of "controller"
6 Meaning of "public authority" and "public body"

Lawfulness of processing

7 Lawfulness of processing: public interest etc
8 Child's consent in relation to information society services

Special categories of personal data

9 Special categories of personal data and criminal convictions etc data
10 Special categories of personal data etc: supplementary

Rights of the data subject

11 Limits on fees that may be charged by controllers
12 Obligations of credit reference agencies
13 Automated decision-making authorised by law: safeguards

Restrictions on data subject's rights

14 Exemptions etc
15 Power to make further exemptions etc by regulations

Accreditation of certification providers

16 Accreditation of certification providers

Transfers of personal data to third countries etc

17 Transfers of personal data to third countries etc

Specific processing situations

18 Processing for archiving, research and statistical purposes: safeguards

CHAPTER 3

OTHER GENERAL PROCESSING

Scope

19 Processing to which this Chapter applies

Application of the GDPR

20 Application of the GDPR to processing to which this Chapter applies
21 Power to make provision in consequence of regulations related to the GDPR

Exemptions etc

22 Manual unstructured data held by FOI public authorities
23 Manual unstructured data used in longstanding historical research
24 National security and defence exemption
25 National security: certificate
26 National security and defence: modifications to Articles 9 and 32 of the applied GDPR

PART 3

LAW ENFORCEMENT PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

Scope

27 Processing to which this Part applies

Definitions

28 Meaning of "competent authority"
29 "The law enforcement purposes"
30 Meaning of "controller" and "processor"
31 Other definitions

CHAPTER 2

PRINCIPLES

32 Overview and general duty of controller
33 The first data protection principle
34 The second data protection principle
35 The third data protection principle
36 The fourth data protection principle
37 The fifth data protection principle
38 The sixth data protection principle
39 Safeguards: archiving
40 Safeguards: sensitive processing

CHAPTER 3

RIGHTS OF THE DATA SUBJECT

Overview and scope

41 Overview and scope

Information: controller's general duties

42 Information: controller's general duties

Data subject's right of access

43 Right of access by the data subject

Data subject's rights to rectification or erasure etc

44 Right to rectification
45 Right to erasure or restriction of processing
46 Rights under section 44 or 45: supplementary

Automated individual decision-making

47 Right not to be subject to automated decision-making
48 Automated decision-making authorised by law: safeguards

Supplementary

49 Exercise of rights through the Commissioner
50 Form of provision of information etc
51 Manifestly unfounded or excessive requests by the data subject
52 Meaning of "applicable time period"

CHAPTER 4

CONTROLLER AND PROCESSOR

Overview and scope

53 Overview and scope

General obligations

54 General obligations of the controller
55 Data protection by design and default
56 Joint controllers
57 Processors
58 Processing under the authority of the controller or processor
59 Records of processing activities
60 Logging
61 Co-operation with the Commissioner
62 Data protection impact assessment
63 Prior consultation with the Commissioner

Obligations relating to security

64 Security of processing
65 Notification of a personal data breach to the Commissioner

Obligations relating to personal data breaches

66 Communication of a personal data breach to the data subject

Data protection officers

67 Designation of a data protection officer
68 Position of data protection officer
69 Tasks of data protection officer

CHAPTER 5

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES ETC

Overview and interpretation

70 Overview and interpretation

General principles for transfers

71 General principles for transfers of personal data
72 Transfers on the basis of an adequacy decision
73 Transfers on the basis of appropriate safeguards
74 Transfers on the basis of special circumstances

Transfers to particular recipients

75 Transfers of personal data to persons other than relevant authorities

Subsequent transfers

76 Subsequent transfers

CHAPTER 6

SUPPLEMENTARY

77 National security: certificates by the Minister
78 Special processing restrictions
79 Reporting of infringements

PART 4

INTELLIGENCE SERVICES PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

Scope

80 Processing to which this Part applies

Definitions

81 Meaning of "controller" and "processor"
82 Other definitions

CHAPTER 2

PRINCIPLES

Overview

83 Overview

The data protection principles

84 The first data protection principle
85 The second data protection principle
86 The third data protection principle
87 The fourth data protection principle
88 The fifth data protection principle

89 The sixth data protection principle

CHAPTER 3

RIGHTS OF THE DATA SUBJECT

Overview

90 Overview

Rights

91 Right to information
92 Right of access
93 Right of access: supplementary
94 Right not to be subject to automated decision-making
95 Right to intervene in automated decision-making
96 Right to information about decision-making
97 Right to object to processing
98 Rights to rectification and erasure

CHAPTER 4

CONTROLLER AND PROCESSOR

Overview

99 Overview

General obligations

100 General obligations of the controller
101 Data protection by design
102 Joint controllers
103 Processors
104 Processing under the authority of the controller or processor

Obligations relating to security

105 Security of processing

Obligations relating to personal data breaches

106 Communication of a personal data breach

CHAPTER 5

TRANSFERS OF PERSONAL DATA OUTSIDE THE UNITED KINGDOM

107 Transfers of personal data outside the United Kingdom

CHAPTER 6

EXEMPTIONS

108 National security
109 National security: certificate
110 Other exemptions
111 Power to make further exemptions

PART 5

THE INFORMATION COMMISSIONER

The Commissioner

112 The Information Commissioner

General functions

113 General functions under the GDPR and safeguards
114 Other general functions
115 Competence in relation to courts etc

International role

116 Co-operation and mutual assistance
117 Inspection of personal data in accordance with international obligations
118 Further international role

Codes of practice

119 Data-sharing code
120 Direct marketing code
121 Approval of data-sharing and direct marketing codes
122 Publication and review of data-sharing and direct marketing codes
123 Effect of data-sharing and direct marketing codes
124 Other codes of practice

Consensual audits

125 Consensual audits

Information provided to the Commissioner

126 Disclosure of information to the Commissioner
127 Confidentiality of information
128 Guidance about privileged communications

Fees

129 Fees for services
130 Manifestly unfounded or excessive requests by data subjects etc
131 Guidance about fees

Charges

132 Charges payable to the Commissioner by controllers
133 Regulations under section 132: supplementary

Reports etc

134 Reporting to Parliament
135 Publication by the Commissioner
136 Notices from the Commissioner

PART 6

ENFORCEMENT

Information notices

137 Information notices
138 Information notices: restrictions
139 Failure to comply with an information notice

Assessment notices

140 Assessment notices
141 Assessment notices: restrictions

Enforcement notices

142 Enforcement notices
143 Enforcement notices: supplementary
144 Enforcement notices: rectification and erasure of personal data etc
145 Enforcement notices: restrictions
146 Enforcement notices: cancellation and variation

Powers of entry and inspection

147 Powers of entry and inspection

Penalties

148 Penalty notices
149 Penalty notices: restrictions
150 Maximum amount of penalty
151 Fixed penalties for non-compliance with charges regulations
152 Amount of penalties: supplementary

Guidance

153 Guidance about regulatory action

Appeals

154 Rights of appeal
155 Determination of appeals

Complaints

156 Complaints by data subjects
157 Orders to progress complaints

Remedies in the court

158 Compliance orders
159 Compensation for contravention of the GDPR
160 Compensation for contravention of other data protection legislation

Offences relating to personal data

161 Unlawful obtaining etc of personal data
162 Re-identification of de-identified personal data
163 Alteration etc of personal data to prevent disclosure

The special purposes

164 The special purposes
165 Provision of assistance in special purposes proceedings
166 Staying special purposes proceedings

Jurisdiction of courts

167 Jurisdiction

Definitions

168 Interpretation of Part 6

PART 7

SUPPLEMENTARY AND FINAL PROVISION

Regulations under this Act

169 Regulations and consultation

Changes to the Data Protection Convention

170 Power to reflect changes to the Data Protection Convention

Rights of the data subject

171 Prohibition of requirement to produce relevant records
172 Avoidance of certain contractual terms relating to health records
173 Representation of data subjects
174 Data subject's rights and other prohibitions and restrictions

Offences

175 Penalties for offences
176 Prosecution
177 Liability of directors etc

178 Recordable offences
179 Guidance about PACE codes of practice

The Tribunal

180 Disclosure of information to the Tribunal
181 Proceedings in the First-tier Tribunal: contempt
182 Tribunal Procedure Rules

Definitions

183 Meaning of "health professional" and "social work professional"
184 Other definitions
185 Index of defined expressions

Territorial application

186 Territorial application of this Act

General

187 Children in Scotland
188 Application to the Crown
189 Application to Parliament
190 Minor and consequential amendments

Final

191 Commencement
192 Transitional provision
193 Extent
194 Short title

Schedule 1 — Special categories of personal data and criminal convictions etc data
Part 1 — Conditions relating to employment, health and research etc
Part 2 — Substantial public interest conditions
Part 3 — Additional conditions relating to criminal convictions etc
Part 4 — Appropriate policy document and additional safeguards
Schedule 2 — Exemptions etc from the GDPR
Part 1 — Adaptations and restrictions based on Articles 6(3) and 23(1)
Part 2 — Restrictions based on Article 23(1): Restrictions of rules in Articles 13 to 21
Part 3 — Restriction based on Article 23(1): Protection of rights of others
Part 4 — Restrictions based on Article 23(1): Restrictions of rules in Articles 13 to 15
Part 5 — Exemptions etc based on Article 85(2) for reasons of freedom of expression and information
Part 6 — Derogations etc based on Article 89 for research, statistics and archiving

Schedule 3 — Exemptions etc from the GDPR: health, social work, education and child abuse data
Part 1 — GDPR provisions to be restricted: "the listed GDPR provisions"
Part 2 — Health data
Part 3 — Social work data
Part 4 — Education data
Part 5 — Child abuse data
Schedule 4 — Exemptions etc from the GDPR: disclosure prohibited or restricted by an enactment
Schedule 5 — Accreditation of certification providers: reviews and appeals
Schedule 6 — The applied GDPR and the applied Chapter 2
Part 1 — Modifications to the GDPR
Part 2 — Modifications to Chapter 2 of Part 2
Schedule 7 — Competent authorities
Schedule 8 — Conditions for sensitive processing under Part 3
Schedule 9 — Conditions for processing under Part 4
Schedule 10 — Conditions for sensitive processing under Part 4
Schedule 11 — Other exemptions under Part 4
Schedule 12 — The Information Commissioner
Schedule 13 — Other general functions of the Commissioner
Schedule 14 — Co-operation and mutual assistance
Part 1 — Law Enforcement Directive
Part 2 — Data Protection Convention
Schedule 15 — Powers of entry and inspection
Schedule 16 — Penalties
Schedule 17 — Relevant records
Schedule 18 — Minor and consequential amendments

A

B I L L

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 conduct; and for connected purposes.

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

PART 1

PRELIMINARY

1 Overview

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

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

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

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

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

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

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

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

2 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)(b)).

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

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

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

(4) "Processing", in relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, 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)(b) and sections 4(7), 27(2) and 80(3), which make provision about references to processing in the different Parts of this Act).

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

(6) "Controller" and "processor", in relation to the processing of personal data to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies, have the same meaning as in that Chapter or Part (see sections 4, 5, 30 and 81).

(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 112).

(9) "The data protection legislation" means—

(a) the GDPR,

(b) the applied GDPR,

(c) this Act,

(d) regulations made under this Act, and

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

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

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

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

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

(14) In Parts 5 to 7, except where otherwise provided—

(a) references to the GDPR are to the GDPR read with Chapter 2 of Part 2 and include the applied GDPR read with Chapter 3 of Part 2;

(b) references to processing and personal data are to processing and personal data to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies.

(15) There is an index of defined expressions in section 185.

PART 2

GENERAL PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

3 Processing to which this Part applies

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

(2) Chapter 2 of this Part—

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

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

(3) Chapter 3 of this Part—

(a) applies to certain types of processing of personal data to which the GDPR does not apply (see section 19), and

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

4 Definitions

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

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

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

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

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

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

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

(8) Sections 2 and 184 include definitions of other expressions used in this Part.

CHAPTER 2

THE GDPR

Meaning of certain terms used in the GDPR

5 Meaning of "controller"

(1) The definition of "controller" in Article 4(7) of the GDPR has effect subject to—
- (a) subsection (2),
- (b) section 188, and
- (c) section 189.

(2) For the purposes of the GDPR, where personal data is processed only—
- (a) for purposes for which it is required by an enactment to be processed, and
- (b) by means by which it is required by an enactment to be processed,

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

6 Meaning of "public authority" and "public body"

(1) For the purposes of the GDPR, the following (and only the following) are "public authorities" and "public bodies" under the law of the United Kingdom—
- (a) a public authority as defined by the Freedom of Information Act 2000, subject to subsection (2),
- (b) a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002 (asp 13), subject to subsection (2), and
- (c) an authority or a body specified by the Secretary of State in regulations.

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

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

Lawfulness of processing

7 Lawfulness of processing: public interest etc

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

(a) the administration of justice,

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

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

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

8 Child's consent in relation to information society services

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

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

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

Special categories of personal data

9 Special categories of personal data and criminal convictions etc data

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

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

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

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

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

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

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

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

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

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

(6) The Secretary of State may by regulations—

(a) amend Schedule 1 by adding, varying or omitting conditions or safeguards, and

(b) make consequential amendments of this section.

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

10 Special categories of personal data etc: supplementary

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

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

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

(2) In Article 10 of the GDPR and this section, 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

11 Limits on fees that may be charged by controllers

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

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

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

(2) The Secretary of State may by regulations—

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

(b) specify what the guidance must include.

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

12 Obligations of credit reference agencies

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

(2) The controller's obligations under Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country

transfers) are taken to apply only to personal data relating to the data subject's financial standing, unless the data subject has indicated a contrary intention.

(3) Where the controller discloses personal data in pursuance of Article 15(1) to (3) of the GDPR, the disclosure must be accompanied by a statement informing the data subject of the data subject's rights under section 159 of the Consumer Credit Act 1974 (correction of wrong information).

13 Automated decision-making authorised by law: safeguards

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

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

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

(b) significantly affects the data subject.

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

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

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

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

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

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

(b) the data subject may, before the end of the period of 21 days beginning with receipt of the notification, request the controller to—

(i) reconsider the decision, or

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

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

(6) 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.

(7) Regulations under subsection (6)—

(a) may amend this section, and

(b) are subject to the affirmative resolution procedure.

Restrictions on data subject's rights

14 Exemptions etc

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

(2) In Schedule 2—

(a) Part 1 makes provision adapting or restricting the application of rules contained in Articles 13 to 21 of the GDPR in specified circumstances, as allowed for by Article 6(3) and Article 23(1) of the GDPR;

(b) Part 2 makes provision restricting the application of rules contained in Articles 13 to 21 of the GDPR in specified circumstances, as allowed for by Article 23(1) of the GDPR;

(c) Part 3 makes provision restricting the application of Article 15 of the GDPR where this is necessary to protect the rights of others, as allowed for by Article 23(1) of the GDPR;

(d) Part 4 makes provision restricting the application of rules contained in Articles 13 to 15 of the GDPR in specified circumstances, as allowed for by Article 23(1) of the GDPR;

(e) Part 5 makes provision containing exemptions or derogations from Chapters II, III and VII of the GDPR for reasons relating to freedom of expression, as allowed for by Article 85(2) of the GDPR;

(f) Part 6 makes provision containing derogations from rights contained in Articles 15, 16, 18, 19, 20 and 21 of the GDPR for scientific or historical research purposes, statistical purposes and archiving purposes, as allowed for by Article 89(2) and (3) of the GDPR.

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

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

(5) In connection with the safeguarding of national security and with defence, see Chapter 3 of this Part and the exemption in section 24.

15 Power to make further exemptions etc by regulations

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

(a) the power in Article 6(3) for Member State law to lay down a legal basis containing specific provisions to adapt the application of rules of the GDPR where processing is necessary for compliance with a legal obligation, for the performance of a task in the public interest or in the exercise of official authority;

(b) the power in Article 23(1) to make a legislative measure restricting the scope of the obligations and rights mentioned in that Article where

necessary and proportionate to safeguard certain objectives of general public interest;

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

(d) the powers in Article 89 for Member State law to provide for derogations from the rights mentioned in paragraphs (2) and (3) of that Article where necessary for scientific or historical research purposes, statistical purposes or archiving purposes.

(2) Regulations under this section may include provision amending or repealing any provision of section 14 and Schedules 2 to 4.

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

Accreditation of certification providers

16 Accreditation of certification providers

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

(a) the Commissioner, or

(b) the national accreditation body.

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

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

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

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

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

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

(4) The Commissioner may only publish a statement under subsection (3)(a) if satisfied that the national accreditation body meets any additional requirements established by the Commissioner under Article 43(1)(b) of the GDPR.

(5) 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.

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

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

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

(9) In this section—

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

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

Transfers of personal data to third countries etc

17 Transfers of personal data to third countries etc

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

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

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

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

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

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

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

Specific processing situations

18 Processing for archiving, research and statistical purposes: safeguards

(1) This section makes provision about—

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

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

(c) processing that is necessary for statistical purposes.

(2) Such processing does not satisfy the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if—

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

(b) it is likely to cause substantial damage or substantial distress to an individual.

CHAPTER 3

OTHER GENERAL PROCESSING

Scope

19 Processing to which this Chapter applies

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

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

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

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

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

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

(4) In this section—

"automated or structured processing of personal data" means—

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

(b) processing of personal data that forms part of a filing system or is intended to form part of a filing system;

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

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

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

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

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

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

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

but such references do not include information held by an intelligence service (as defined in section 80) on behalf of an FOI public authority.

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

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

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

Application of the GDPR

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

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

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

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

(4) Schedule 6 contains provision modifying—
(a) the GDPR as it applies by virtue of subsection (1) (see Part 1);
(b) Chapter 2 of this Part as it applies by virtue of subsection (2) (see Part 2).

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

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

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

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

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

(4) Regulations under subsection (1) may amend or repeal a provision of—
(a) the applied GDPR;
(b) this Chapter;
(c) Parts 5 to 7, in so far as they apply in relation to the applied GDPR.

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

Exemptions etc

22 Manual unstructured data held by FOI public authorities

(1) The provisions of the applied GDPR and this Act listed in subsection (2) do not apply to personal data to which this Chapter applies by virtue of section 19(2) (manual unstructured personal data held by FOI public authorities).

(2) Those provisions are—
(a) in Chapter II of the applied GDPR (principles)—

(i) Articles 5(1)(a) to (c), (e) and (f) (principles relating to processing, other than the accuracy principle),
(ii) Article 6 (lawfulness),
(iii) Article 7 (conditions for consent),
(iv) Article 8(1) and (2) (child's consent),
(v) Article 9 (processing of special categories of personal data),
(vi) Article 10 (data relating to criminal convictions etc), and
(vii) Article 11(2) (processing not requiring identification);

(b) in Chapter III of the applied GDPR (rights of the data subject)—
(i) Article 13(1) to (3) (personal data collected from data subject: information to be provided),
(ii) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),
(iii) Article 20 (right to data portability), and
(iv) Article 21(1) (objections to processing);

(c) in Chapter V of the applied GDPR, Articles 44 to 49 (transfers of personal data to third countries or international organisations);

(d) sections 161 and 162 of this Act;

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

(3) In addition, the provisions of the applied GDPR listed in subsection (4) do not apply to personal data to which this Chapter applies by virtue of section 19(2) where the personal data relates to appointments, removals, pay, discipline, superannuation or other personnel matters in relation to—

(a) service in any of the armed forces of the Crown;

(b) service in any office or employment under the Crown or under any public authority;

(c) service in any office or employment, or under any contract for services, in respect of which power to take action, or to determine or approve the action taken, in such matters is vested in—
(i) Her Majesty,
(ii) a Minister of the Crown,
(iii) the National Assembly for Wales,
(iv) the Welsh Ministers,
(v) a Northern Ireland Minister (within the meaning of the Freedom of Information Act 2000), or
(vi) an FOI public authority.

(4) Those provisions are—

(a) the remaining provisions of Chapters II and III (principles and rights of the data subject);

(b) Chapter IV (controller and processor);

(c) Chapter IX (specific processing situations).

(5) A controller is not obliged to comply with Article 15(1) to (3) of the applied GDPR (right of access by the data subject) in relation to personal data to which this Chapter applies by virtue of section 19(2) if—

(a) the request under that Article does not contain a description of the personal data, or

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

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

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

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

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

23 Manual unstructured data used in longstanding historical research

(1) The provisions of the applied GDPR listed in subsection (2) do not apply to personal data to which this Chapter applies by virtue of section 19(2) (manual unstructured personal data held by FOI public authorities) at any time when—

(a) the personal data—

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

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

(b) the processing is not carried out—

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

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

(2) Those provisions are—

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

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

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

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

(3) The exemptions in this section apply in addition to the exemptions in section 22.

24 National security and defence exemption

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

(a) the purpose of safeguarding national security, or

(b) defence purposes.

(2) The provisions are—

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

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

(ii) Article 6 (lawfulness of processing);
(iii) Article 9 (processing of special categories of personal data);

(b) Chapter III of the applied GDPR (rights of data subjects);

(c) in Chapter IV of the applied GDPR—
(i) Article 33 (notification of personal data breach to the Commissioner);
(ii) Article 34 (communication of personal data breach to the data subject);

(d) Chapter V of the applied GDPR (transfers of personal data to third countries or international organisations);

(e) in Chapter VI of the applied GDPR—
(i) Article 57(1)(a) and (h) (Commissioner's duties to monitor and enforce the applied GDPR and to conduct investigations);
(ii) Article 58 (investigative, corrective, authorisation and advisory powers of Commissioner);

(f) Chapter VIII of the applied GDPR (remedies, liabilities and penalties) except for—
(i) Article 83 (general conditions for imposing administrative fines);
(ii) Article 84 (penalties);

(g) in Part 5 of this Act—
(i) in section 113 (general functions of the Commissioner), subsections (3) and (8);
(ii) in section 113, subsection (9), so far as it relates to Article 58(2)(i) of the applied GDPR;
(iii) section 117 (inspection in accordance with international obligations);

(h) in Part 6 of this Act—
(i) sections 137 to 147 and Schedule 15 (Commissioner's notices and powers of entry and inspection);
(ii) sections 161 to 163 (offences relating to personal data);

(i) in Part 7 of this Act, section 173 (representation of data subjects).

25 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 24(2) is, or at any time was, required in relation to any personal data for the purpose of safeguarding national security is conclusive evidence of that fact.

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

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

(4) If, on an appeal under subsection (3), the Tribunal finds that, applying the principles applied by a court on an application for judicial review, the Minister did not have reasonable grounds for issuing a certificate, the Tribunal may—
(a) allow the appeal, and

(b) quash the certificate.

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

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

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

(8) A document purporting to be a certificate under subsection (1) is to be—
(a) received in evidence, and
(b) deemed to be such a certificate unless the contrary is proved.

(9) A document which purports to be certified by or on behalf of a Minister of the Crown as a true copy of a certificate issued by that Minister under subsection (1) is—
(a) in any legal proceedings, evidence of that certificate;
(b) in any legal proceedings in Scotland, sufficient evidence of that certificate.

(10) The power conferred by subsection (1) on a Minister of the Crown is exercisable only by—
(a) a Minister who is a member of the Cabinet, or
(b) the Attorney General or the Advocate General for Scotland.

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

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

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

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

(4) For the purposes of subsection (3), where the processing of personal data is carried out wholly or partly by automated means, the controller or the processor must, following an evaluation of the risks, implement measures designed to—

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

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

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

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

PART 3

LAW ENFORCEMENT PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

Scope

27 Processing to which this Part applies

(1) This Part applies to—

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

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

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

(3) For the meaning of "competent authority", see section 28.

Definitions

28 Meaning of "competent authority"

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

(a) a person specified in Schedule 7, and

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

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

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

(a) so as to add a person to, or remove a person from, the Schedule;

(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 71(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.

29 "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.

30 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).

31 Other definitions

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

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

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

(4) "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects

relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

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

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

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

(8) Sections 2 and 184 include definitions of other expressions used in this Part.

CHAPTER 2

PRINCIPLES

32 Overview and general duty of controller

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

(a) section 33(1) sets out the first data protection principle (requirement that processing be lawful and fair);

(b) section 34(1) sets out the second data protection principle (requirement that purposes of processing be specified, explicit and legitimate);

(c) section 35 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 36(1) sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

(e) section 37(1) sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 38 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) In addition—

(a) each of sections 33, 34, 36 and 37 makes provision to supplement the principle to which it relates, and

(b) sections 39 and 40 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.

33 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 40).

(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 40).

(6) The Secretary of State may by regulations amend Schedule 8 by adding, varying or omitting conditions.

(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.

34 The second data protection principle

(1) The second data protection principle is that—

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

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

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

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

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

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

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

35 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.

36 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.

37 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.

38 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).

39 Safeguards: archiving

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

(a) for archiving purposes in the public interest,

(b) for scientific or historical research purposes, or

(c) for statistical purposes.

(2) The processing is not permitted if—

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

(b) it is likely to cause substantial damage or substantial distress to an individual.

40 Safeguards: sensitive processing

(1) This section applies for the purposes of section 33(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 32(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 59(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 59(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 33 (lawfulness of processing), and

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

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

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

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

CHAPTER 3

RIGHTS OF THE DATA SUBJECT

Overview and scope

41 Overview and scope

(1) This Chapter—

(a) imposes general duties on the controller to make information available (see section 42);

(b) confers a right of access by the data subject (see section 43);

(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 44 to 46);

(d) regulates automated decision-making (see sections 47 and 48);

(e) makes supplementary provision (see sections 49 to 52).

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

(3) But sections 42 to 46 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

42 Information: controller's general duties

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

(a) the identity and the contact details of the controller;
(b) where applicable, the contact details of the data protection officer (see sections 67 to 69);
(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 43),
(ii) rectification of personal data (see section 44), and
(iii) erasure of personal data or the restriction of its processing (see section 45);
(e) the existence of the right to lodge a complaint with the Commissioner and the contact details of the Commissioner.

(2) The controller must also, in specific cases for the purpose of enabling the exercise of a data subject's rights under this Part, give the data subject the following—
(a) information about the legal basis for the processing;
(b) information about the period for which the personal data will be stored or, where that is not possible, about the criteria used to determine that period;
(c) where applicable, information about the categories of recipients of the personal data (including recipients in third countries or international organisations);
(d) such further information as is necessary to enable the exercise of the data subject's rights under this Part.

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

(4) The controller may restrict, wholly or partly, the provision of information to the data subject under subsection (2) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—
(a) avoid obstructing an official or legal inquiry, investigation or procedure;
(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) protect public security;
(d) protect national security;
(e) protect the rights and freedoms of others.

(5) Where the provision of information to a data subject under subsection (2) is restricted, wholly or partly, the controller must inform the data subject in writing without undue delay—
(a) that the provision of information has been restricted,
(b) of the reasons for the restriction,
(c) of the data subject's right to make a request to the Commissioner under section 49,
(d) of the data subject's right to lodge a complaint with the Commissioner, and
(e) of the data subject's right to apply to a court under section 158.

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

(7) The controller must—

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

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

Data subject's right of access

43 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 44), and

(ii) erasure of personal data or the restriction of its processing (see section 45);

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

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

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

(a) without undue delay, and

(b) in any event, before the end of the applicable time period (as to which see section 52).

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

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

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

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

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

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

(b) of the reasons for the restriction,

(c) of the data subject's right to make a request to the Commissioner under section 49,

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

(e) of the data subject's right to apply to a court under section 158.

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

(7) The controller must—

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

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

Data subject's rights to rectification or erasure etc

44 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.

45 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 33, 34(1) to (3), 35, 36(1), 37(1), 38, 39 or 40, 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 44 or in any other way), but it is not

possible to ascertain whether it is accurate or not, the controller must restrict its processing.

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

46 Rights under section 44 or 45: 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 49,

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

(iv) of the data subject's right to apply to a court under section 158.

(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 52).

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

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

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

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

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

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

(b) of the reasons for the restriction,

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

(d) of the data subject's right to apply to a court under section 158.

(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 (4), and

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

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

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

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

(a) the controller must notify the recipients, and

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

(10) Where processing is restricted in accordance with section 45(3), the controller must inform the data subject before lifting the restriction.

Automated individual decision-making

47 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.

48 Automated decision-making authorised by law: safeguards

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

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

(b) it is required or authorised by law.

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

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

(b) the data subject may, before the end of the period of 21 days beginning with receipt of the notification, request the controller to—

(i) reconsider the decision, or

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

(3) If a request is made to a controller under subsection (2), the controller must, before the end of the period of 21 days 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 47(2).

Supplementary

49 Exercise of rights through the Commissioner

(1) This section applies where a controller—
(a) restricts under section 42(4) the information provided to the data subject under section 42(2) (duty of the data controller to give the data subject additional information),
(b) restricts under section 43(4) the data subject's rights under section 43(1) (right of access), or
(c) refuses a request by the data subject for rectification under section 44 or for erasure or restriction of processing under section 45.

(2) The data subject may—
(a) where subsection (1)(a) or (b) applies, request the Commissioner to check that the processing of personal data relating to the data subject complies with this Part;
(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 137 and 140).

(4) After taking those steps, the Commissioner must inform the data subject—
(a) where subsection (1)(a) or (b) applies, whether the Commissioner is satisfied that the processing by the controller of personal data relating to the data subject complies with this Part;
(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 158.

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

50 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 43, 44, 45 or 48, the controller must provide the information in the same form as the request where it is practicable to do so.

(4) Where the controller has reasonable doubts about the identity of an individual making a request under section 43, 44 or 45, 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 51, 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 43 to 48.

51 Manifestly unfounded or excessive requests by the data subject

(1) Where a request from a data subject under section 43, 44 or 45 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 43, 44 or 45 is manifestly unfounded or excessive, it is for the controller to show that it is.

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

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

52 Meaning of "applicable time period"

(1) This section defines "the applicable time period" for the purposes of sections 43(3)(b) and 46(2)(b).

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

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

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

(b) the day on which the controller receives the information (if any) requested in connection with a request under section 50(4);

(c) the day on which the fee (if any) charged in connection with the request under section 51 is paid.

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

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

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

CHAPTER 4

CONTROLLER AND PROCESSOR

Overview and scope

53 Overview and scope

(1) This Chapter—

(a) sets out the general obligations of controllers and processors (see sections 54 to 63);

(b) sets out specific obligations of controllers and processors with respect to security (see section 64);

(c) sets out specific obligations of controllers and processors with respect to personal data breaches (see sections 65 and 66);

(d) makes provision for the designation, position and tasks of data protection officers (see sections 67 to 69).

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

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

(a) the latest developments in technology,

(b) the cost of implementation,

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

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

General obligations

54 General obligations of the controller

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

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

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

55 Data protection by design and default

(1) Each controller must implement appropriate technical and organisational measures which are designed—
(a) to implement the data protection principles in an effective manner, and
(b) to integrate into the processing itself the safeguards necessary for that purpose.

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

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

(4) The duty under subsection (3) applies to—
(a) the amount of personal data collected,
(b) the extent of its processing,
(c) the period of its storage, and
(d) its accessibility.

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

56 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.

57 Processors

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

(2) The controller may use only a processor who provides guarantees to implement appropriate technical and organisational measures that are sufficient to secure that the processing will—
(a) meet the requirements of this Part, and
(b) ensure the protection of the rights of the data subject.

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

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

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

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

(b) the nature and purpose of the processing;

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

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

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

(a) act only on instructions from the controller,

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

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

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

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

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

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

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

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

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

58 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.

59 Records of processing activities

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

(2) The controller's record must contain the following information—
(a) the name and contact details of the controller;
(b) where applicable, the name and contact details of the joint controller;
(c) where applicable, the name and contact details of the data protection officer;
(d) the purposes of the processing;
(e) the categories of recipients to whom personal data has been or will be disclosed (including recipients in third countries or international organisations);
(f) a description of the categories of—
(i) data subject, and
(ii) personal data;
(g) where applicable, details of the use of profiling;
(h) where applicable, the categories of transfers of personal data to a third country or an international organisation;
(i) an indication of the legal basis for the processing operations, including transfers, for which the personal data is intended;
(j) where possible, the envisaged time limits for erasure of the different categories of personal data;
(k) where possible, a general description of the technical and organisational security measures referred to in section 64.

(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 57(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 64.

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

60 Logging

(1) A controller (or, where personal data is processed on behalf of the controller by a processor, the processor) must keep logs for at least the following processing operations in automated processing systems—
(a) collection;
(b) alteration;
(c) consultation;
(d) disclosure (including transfers);

(e) combination;
(f) erasure.

(2) The logs of consultation must make it possible to establish—
(a) the justification for, and date and time of, the consultation, and
(b) so far as possible, the identity of the person who consulted the data.

(3) The logs of disclosure must make it possible to establish—
(a) the justification for, and date and time of, the disclosure, and
(b) so far as possible—
(i) the identity of the person who disclosed the data, and
(ii) the identity of the recipients of the data.

(4) The logs kept under subsection (1) may be used only for one or more of the following purposes—
(a) to verify the lawfulness of processing;
(b) to assist with self-monitoring by the controller or (as the case may be) the processor, including the conduct of internal disciplinary proceedings;
(c) to ensure the integrity and security of personal data;
(d) the purposes of criminal proceedings.

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

61 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.

62 Data protection impact assessment

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

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

(3) A data protection impact assessment must include the following—
(a) a general description of the envisaged processing operations;
(b) an assessment of the risks to the rights and freedoms of data subjects;
(c) the measures envisaged to address those risks;
(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

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

63 Prior consultation with the Commissioner

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

(2) The controller must consult the Commissioner prior to the processing if a data protection impact assessment prepared under section 62 indicates that the processing of the data would result in a high risk to the rights and freedoms of individuals (in the absence of measures to mitigate the risk).

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

(a) the data protection impact assessment prepared under section 62, and

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

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

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

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

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

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

(b) provide reasons for the delay.

Obligations relating to security

64 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.

65 Notification of a personal data breach to the Commissioner

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

(a) without undue delay, and

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

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

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

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

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

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

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

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

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

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

(a) the facts relating to the breach,

(b) its effects, and

(c) the remedial action taken.

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

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

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

Obligations relating to personal data breaches

66 Communication of a personal data breach to the data subject

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

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

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

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

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

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

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

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

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

(c) it would involve a disproportionate effort.

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

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

(6) Where the controller has not informed the data subject of the breach the Commissioner, on being notified under section 65 and after considering the likelihood of the breach resulting in a high risk, may—

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

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

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

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

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

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

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

(9) The duties in section 50(1) and (2) apply in relation to information that the controller is required to provide to the data subject under this section as they apply in relation to information that the controller is required to provide to the data subject under Chapter 3.

Data protection officers

67 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 69.

(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.

68 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 69, 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 69;

(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 69.

(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.

69 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 62 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 63, and consulting with the Commissioner, where appropriate, in relation to any other matter,

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

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

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

(a) assigning responsibilities under those policies,

(b) raising awareness of those policies,

(c) training staff involved in processing operations, and

(d) conducting audits required under those policies.

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

CHAPTER 5

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES ETC

Overview and interpretation

70 Overview and interpretation

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

(a) sections 71 to 74 set out the general conditions that apply;

(b) section 75 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 76 makes special provision about subsequent transfers of personal data.

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

General principles for transfers

71 General principles for transfers of personal data

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

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

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

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

(3) Condition 2 is that the transfer—

(a) is based on an adequacy decision (see section 72),

(b) if not based on an adequacy decision, is based on there being appropriate safeguards (see section 73), or

(c) if not based on an adequacy decision or on there being appropriate safeguards, is based on special circumstances (see section 74).

(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 4 to 16, 20 to 43, 46 and 48 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 75 are met.

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

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

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

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

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

72 Transfers on the basis of an adequacy decision

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

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

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

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

ensures an adequate level of protection of personal data, and

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

73 Transfers on the basis of appropriate safeguards

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

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

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

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

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

(a) the transfer must be documented,

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

(c) the documentation must include, in particular—

(i) the date and time of the transfer,

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

(iii) the justification for the transfer, and

(iv) a description of the personal data transferred.

74 Transfers on the basis of special circumstances

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

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

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

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

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

(e) in individual cases for a legal purpose.

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

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

(a) the transfer must be documented,

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

(c) the documentation must include, in particular—

(i) the date and time of the transfer,
(ii) the name of and any other pertinent information about the recipient,
(iii) the justification for the transfer, and
(iv) a description of the personal data transferred.

(4) For the purposes of this section, a transfer is necessary for a legal purpose if—
(a) it is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) relating to any of the law enforcement purposes,
(b) it is necessary for the purpose of obtaining legal advice in relation to any of the law enforcement purposes, or
(c) it is otherwise necessary for the purposes of establishing, exercising or defending legal rights in relation to any of the law enforcement purposes.

Transfers to particular recipients

75 Transfers of personal data to persons other than relevant authorities

(1) The additional conditions referred to in section 71(4)(b)(ii) are the following four conditions.

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

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

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

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

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

(7) The transferring controller must—
(a) document any transfer to a recipient in a third country other than a relevant authority, and
(b) inform the Commissioner about the transfer.

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

Subsequent transfers

76 Subsequent transfers

(1) Where personal data is transferred in accordance with section 71, the transferring controller must make it a condition of the transfer that the data is not to be further transferred to a third country or international organisation without the authorisation of the transferring controller or another competent authority.

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

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

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

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

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

(4) In a case where the personal data was originally transmitted or otherwise made available to the transferring controller or another competent authority by a member State other than the United Kingdom, an authorisation may not be given under subsection (1) unless that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State.

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

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

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

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

CHAPTER 6

SUPPLEMENTARY

77 National security: certificates by the Minister

(1) A Minister of the Crown may issue a certificate certifying, for the purposes of section 42(4), 43(4), 46(3) or 66(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 42(4), 43(4), 46(3) or 66(7), or

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

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

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

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

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

(a) allow the appeal, and

(b) quash the certificate.

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

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

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

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

(a) received in evidence, and

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

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

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

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

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

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

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

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

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

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

78 Special processing restrictions

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

(2) In this section—

"EU recipient" means—

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

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

"non-EU recipient" means—

(a) a recipient in a third country, or

(b) an international organisation.

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

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

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

(6) Subsection (7) applies where—

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

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

(7) The controller must comply with the restrictions.

79 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.

PART 4

INTELLIGENCE SERVICES PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

Scope

80 Processing to which this Part applies

(1) This Part applies to—

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

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

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

(a) the Security Service;

(b) the Secret Intelligence Service;

(c) the Government Communications Headquarters.

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

Definitions

81 Meaning of "controller" and "processor"

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

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

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

(2) Where personal data is processed only—

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

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

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

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

82 Other definitions

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

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

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

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

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

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

(7) Sections 2 and 184 include definitions of other expressions used in this Part.

CHAPTER 2

PRINCIPLES

Overview

83 Overview

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

(a) section 84 sets out the first data protection principle (requirement that processing be lawful, fair and transparent);

(b) section 85 sets out the second data protection principle (requirement that the purposes of processing be specified, explicit and legitimate);

(c) section 86 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 87 sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

(e) section 88 sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 89 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) Each of sections 84, 85 and 89 makes provision to supplement the principle to which it relates.

The data protection principles

84 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 by adding, varying or omitting conditions.

(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.

85 The second data protection principle

(1) The second data protection principle is that—

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

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

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

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

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

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

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

(a) consists of—

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

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

(iii) processing for statistical purposes, and

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

86 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.

87 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.

88 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.

89 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

90 Overview

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

(a) section 91 deals with the information to be made available to the data subject;

(b) sections 92 and 93 deal with the right of access by the data subject;

(c) sections 94 to 96 deal with rights in relation to automated processing;

(d) section 97 deals with the right to object to processing;

(e) section 98 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

91 Right to information

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

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

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

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

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

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

(f) how to exercise rights under this Chapter;

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

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

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

(4) Where personal data relating to a data subject is collected by or on behalf of the controller from a person other than the data subject, the requirement in subsection (1) has effect, in relation to the personal data so collected, with the following exceptions—

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

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

92 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 98);
  (f) the right to lodge a complaint with the Commissioner and the contact details of the Commissioner;
  (g) any information about the origin of the personal data concerned.

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

(4) The Secretary of State may by regulations—
  (a) specify cases in which a controller may not charge a fee;
  (b) specify the maximum amount of a fee.

(5) Where a controller—
  (a) reasonably requires further information—
    (i) in order that the controller be satisfied as to the identity of the individual making a request under subsection (1), or
    (ii) to locate the information which that individual seeks, and
  (b) has informed that individual of that requirement,

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

(6) Where a controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, the controller is not obliged to comply with the request unless—
  (a) the other individual has consented to the disclosure of the information to the individual making the request, or
  (b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

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

(8) Subsection (6) is not to be construed as excusing a controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual

concerned, whether by the omission of names or other identifying particulars or otherwise.

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

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

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

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

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

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

(a) promptly, and

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

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

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

(13) In this section—

"the applicable time period" means the period of—

(a) one month, or

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

beginning with the relevant day;

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

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

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

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

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

93 Right of access: supplementary

(1) The controller must comply with the obligation imposed by section 92(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 92(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 92 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 92 are made at reasonable intervals, regard must be had to—

(a) the nature of the data,

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

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

(4) The information to be supplied pursuant to a request under section 92 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 92(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.

94 Right not to be subject to automated decision-making

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

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

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

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

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

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

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

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

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

95 Right to intervene in automated decision-making

(1) This section applies where—

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

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

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

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

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

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

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

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

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

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

(a) to reconsider the decision, or

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

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

96 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.

97 Right to object to processing

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

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

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

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

(2) Where the controller—

(a) reasonably requires further information—

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

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

(b) has informed that individual of that requirement,

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

(3) The controller must, before the end of 21 days beginning with the relevant day, 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) The jurisdiction conferred on a court by this section is exercisable by the High Court or, in Scotland, by the Court of Session.

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

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

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

98 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 84 to 89, 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) 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

99 Overview

This Chapter sets out—

(a) the general obligations of controllers and processors (see sections 100 to 104);

(b) specific obligations of controllers and processors with respect to security (see section 105);

(c) specific obligations of controllers and processors with respect to personal data breaches (see section 106).

General obligations

100 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.

101 Data protection by design

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

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

(a) the data protection principles are implemented, and

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

102 Joint controllers

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

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

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

103 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.

104 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

105 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

106 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

107 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

108 National security

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

(2) The provisions are—

(a) Chapter 2 (the data protection principles), except section 84(1)(a) and (2) and Schedules 9 and 10;
(b) Chapter 3 (rights of data subjects);
(c) in Chapter 4, section 106 (communication of a personal data breach to the Commissioner);
(d) in Part 5—
  (i) section 117 (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 137 to 147 and Schedule 15 (Commissioner's notices and powers of entry and inspection);
  (ii) sections 161 to 163 (offences relating to personal data);
  (iii) sections 164 to 166 (provision relating to the special purposes).

109 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 108(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.

110 Other exemptions

Schedule 11 provides for further exemptions.

111 Power to make further exemptions

(1) Regulations made by the Secretary of State may provide for further exemptions from any provision of this Part.

(2) Regulations under this section may include provision amending or repealing any provision of Schedule 11.

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

PART 5

THE INFORMATION COMMISSIONER

The Commissioner

112 The Information Commissioner

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

(2) Schedule 12 makes provision about the Commissioner.

General functions

113 General functions under the GDPR and safeguards

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

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

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

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

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

(a) a duty to advise Parliament, the government and other institutions and bodies on legislative and administrative measures relating to the

protection of individuals' rights and freedoms with regard to the processing of personal data, and

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

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

(5) The Commissioner's power under Article 58(1)(a) of the GDPR (power to require a controller or processor to provide information that the Commissioner requires for the performance of the Commissioner's tasks under the GDPR) is exercisable only by giving an information notice under section 137.

(6) The Commissioner's power under Article 58(1)(b) of the GDPR (power to carry out data protection audits) is exercisable only in accordance with section 140.

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

(a) in accordance with Schedule 15 (see section 147), or

(b) to the extent that they are exercised in conjunction with the power under Article 58(1)(b) of the GDPR, in accordance with section 140.

(8) The following powers are exercisable only by giving an enforcement notice under section 142—

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

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

(9) The Commissioner's powers under Articles 58(2)(i) and 83 of the GDPR (administrative fines) are exercisable only by giving a penalty notice under section 148.

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

114 Other general functions

(1) The Commissioner—

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

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

(2) Schedule 13 confers general functions on the Commissioner in connection with processing to which the GDPR does not apply.

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

115 Competence in relation to courts etc

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

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

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

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

International role

116 Co-operation and mutual assistance

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

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

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

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

(5) Part 2 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).

117 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 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.

118 Further international role

(1) The Commissioner must, in relation to third countries and international organisations, take appropriate steps to—

(a) develop international co-operation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of legislation and practice for the protection of personal data, including legislation and practice relating to jurisdictional conflicts with third countries.

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

(3) The Commissioner must carry out data protection functions which the Secretary of State directs the Commissioner to carry out for the purpose of enabling Her Majesty's Government in the United Kingdom to give effect to an international obligation of the United Kingdom.

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

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

(6) In this section—

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

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

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

Codes of practice

119 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.

120 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.

121 Approval of data-sharing and direct marketing codes

(1) When a code is prepared under section 119 or 120—
(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) If, within the 40-day period, either House of Parliament resolves not to approve the code, the Commissioner must not issue the code.

(3) 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.

(4) If, as a result of subsection (2), there is no code in force under section 119 or 120, the Commissioner must prepare another version of the code.

(5) Nothing in subsection (2) prevents another version of the code being laid before Parliament.

(6) 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.

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

(8) This section, other than subsection (4), applies in relation to amendments prepared under sections 119 and 120 as it applies in relation to codes prepared under those sections.

122 Publication and review of data-sharing and direct marketing codes

(1) The Commissioner must publish a code issued under section 121(3).

(2) Where an amendment of a code is issued under section 121(3), 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 121(3) 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 119(2) or 120(2) with a view to remedying the situation.

123 Effect of data-sharing and direct marketing codes

(1) A failure by a person to act in accordance with a provision of a code issued under section 121(3) does not of itself make that person liable to legal proceedings in a court or tribunal.

(2) A code issued under section 121(3), 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 121(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.

(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 121(3) 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).

124 Other codes of practice

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

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

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

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

(a) trade associations;

(b) data subjects;

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

(3) Regulations under this section—

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

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

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

(5) In this section—

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

including compliance with the requirements of the data protection legislation;

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

Consensual audits

125 Consensual audits

(1) The Commissioner's functions under Article 58(1) of the 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 124.

Information provided to the Commissioner

126 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 under—

(a) the data protection legislation, or

(b) the information regulations.

(2) The "information regulations" means—

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

(b) the Environmental Information Regulations 2004 (S.I. 2004/3391);

(c) the INSPIRE Regulations 2009 (S.I. 2009/3157);

(d) the Re-use of Public Sector Information Regulations 2015 (S.I. 2015/1415).

127 Confidentiality of information

(1) It is an offence for a person who is or has been the Commissioner, or a member of the Commissioner's staff or an agent of the Commissioner, knowingly or recklessly to disclose information which—

(a) has been obtained by, or provided to, the Commissioner under or for the purposes of the data protection legislation or the information regulations,

(b) relates to an identified or identifiable living 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 provided for the purpose of its being made available to the public (in whatever manner) under a provision of the data protection legislation, the information regulations or the Freedom of Information Act 2000,

(c) the disclosure was made for the purposes of, and is necessary for, the discharge of a function under the data protection legislation, the information regulations or the Freedom of Information Act 2000,

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

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

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

(3) In this section, "the information regulations" has the same meaning as in section 126.

128 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

129 Fees for services

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

130 Manifestly unfounded or excessive requests by data subjects etc

(1) Where a request to the Commissioner from a data subject or a data protection officer is manifestly unfounded or excessive, the Commissioner may—

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

(b) refuse to act on the request.

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

(3) In any proceedings where there is an issue as to whether a request described in subsection (1) is manifestly unfounded or excessive, it is for the Commissioner to show that it is.

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

131 Guidance about fees

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

(a) section 129 or 130, or

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

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

Charges

132 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.

133 Regulations under section 132: supplementary

(1) Before making regulations under section 132(1) or (6), the Secretary of State must consult—

(a) such representatives of persons likely to be affected by the regulations as the Secretary of State thinks appropriate, and

(b) such other persons as the Secretary of State thinks appropriate,

(and see also section 169).

(2) The Commissioner—

(a) must keep under review the working of regulations under section 132(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 132(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 132(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 132(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 132(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 made under section 132(1) or (6) may bind the Crown.

(8) But regulations under section 132(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

134 Reporting to Parliament

(1) The Commissioner must—

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

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

(c) publish it.

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

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

135 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.

136 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

137 Information notices

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

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

(3) An information notice—

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

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

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

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

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

(4) An information notice must provide information about the rights of appeal under section 154.

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

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

(7) If an information notice—

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

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

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

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

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

138 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 164 with respect to the data or the processing has taken effect, or

(b) the Commissioner—

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

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

(2) An information notice does not require a person to give the Commissioner information 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.

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

(a) between a professional legal adviser and the adviser's client 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 information notice does not require a person to provide the Commissioner with information if doing so would, by revealing evidence of the commission of an offence expose the person to proceedings for that offence.

(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) 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 139) 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.

(8) In subsection (5), in relation to an information notice given to a representative of a controller or processor designated under Article 27 of the GDPR, the reference to the person providing the information being exposed to proceedings for an offence includes a reference to the controller or processor being exposed to such proceedings.

139 Failure to comply with an information notice

(1) It is an offence for a person to fail to comply with an information notice.

(2) It is a defence for a person charged with an offence under subsection (1) to prove that the person exercised all due diligence to comply with the notice.

(3) It is an offence for a person, in response to an information notice—
(a) to make a statement which the person knows to be false in a material respect, or
(b) recklessly to make a statement which is false in a material respect.

Assessment notices

140 Assessment notices

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

(2) An assessment notice may require the controller or processor to do any of the following—
(a) permit the Commissioner to enter specified premises;
(b) direct the Commissioner to documents on the premises that are of a specified description;
(c) assist the Commissioner to view information of a specified description that is capable of being viewed using equipment on the premises;
(d) comply with a request from the Commissioner for—
(i) a copy of the documents to which the Commissioner is directed;
(ii) a copy (in such form as may be requested) of the information which the Commissioner is assisted to view;
(e) direct the Commissioner to equipment or other material on the premises which is of a specified description;
(f) permit the Commissioner to inspect or examine the documents, information, equipment or material to which the Commissioner is directed or which the Commissioner is assisted to view;
(g) permit the Commissioner to observe the processing of personal data that takes place on the premises;
(h) make available for interview by the Commissioner a specified number of people of a specified description who process personal data on behalf of the controller, not exceeding the number who are willing to be interviewed.

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

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

(5) An assessment notice must provide information about the rights of appeal under section 154.

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

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

(8) If an assessment notice—

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

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

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

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

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

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

141 Assessment notices: restrictions

(1) 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.

(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 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.

(3) In subsections (1) and (2)—

(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 (1)(b) or in subsection (2)(b) and (c).

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

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

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

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

Enforcement notices

142 Enforcement notices

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

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

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

or both (and see also sections 143 and 144).

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

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

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

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

(d) a requirement to communicate a personal data breach to the Commissioner or a data subject under section 65, 66 or 106 of this Act;

(e) the principles for transfers of personal data to third countries, non-Convention countries and international organisations in Articles 44 to 49 of the GDPR or in sections 71 to 76 or 107 of this Act.

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

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

(a) does not meet the requirements for accreditation,

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

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

(5) The fourth type of failure is where a controller has failed, or is failing, to comply with regulations under section 132.

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

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

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

(9) Before making regulations under this section, the Secretary of State must consult such persons as the Secretary of State considers appropriate.

(10) Regulations under this section—
- (a) may make provision about the giving of enforcement notices in respect of the failure,
- (b) may amend this section and sections 143 to 146, and
- (c) are subject to the affirmative resolution procedure.

143 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 142(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 142(2), the Commissioner's power under section 142(1)(b) to require a person to refrain from taking specified steps includes power—
- (a) to impose a ban relating to all processing of personal data, or
- (b) to impose a ban relating only to a specified description of processing of personal data, including by specifying one or more of the following—
  - (i) a description of personal data;
  - (ii) the purpose or manner of the processing;
  - (iii) the time when the processing takes place.

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

(5) An enforcement notice must provide information about the rights of appeal under section 154.

(6) An enforcement notice must not specify a time for compliance with a requirement in the notice which falls before the end of the period within which an appeal can be brought against the notice.

(7) If an appeal is brought against an enforcement notice, a requirement in the notice need not be complied with pending the determination or withdrawal of the appeal.

(8) If an enforcement notice—
- (a) states that, in the Commissioner's opinion, it is necessary for a requirement to be complied with urgently, and
- (b) gives the Commissioner's reasons for reaching that opinion,

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

(9) In this section, "specified" means specified in an enforcement notice.

144 Enforcement notices: rectification and erasure of personal data etc

(1) Subsections (2) and (3) apply where an enforcement notice is given in respect of a failure by a controller or processor—

(a) to comply with a data protection principle relating to accuracy, or

(b) to comply with a data subject's request to exercise rights under Article 16, 17 or 18 of the GDPR (right to rectification, erasure or restriction on processing) or section 44, 45 or 98 of this Act.

(2) If the enforcement notice requires the controller or processor to rectify or erase inaccurate personal data, it may also require the controller or processor to rectify or erase any other data which—

(a) is held by the controller or processor, and

(b) contains an expression of opinion which appears to the Commissioner to be based on the inaccurate personal data.

(3) Where a controller or processor has accurately recorded personal data provided by the data subject or a third party but the data is inaccurate, the enforcement notice may require the controller or processor—

(a) to take steps specified in the notice to ensure the accuracy of the data,

(b) if relevant, to secure that the data indicates the data subject's view that the data is inaccurate, and

(c) to supplement the data with a statement of the true facts relating to the matters dealt with by the data that is approved by the Commissioner,

(as well as imposing requirements under subsection (2)).

(4) When deciding what steps it is reasonable to specify under subsection (3)(a), the Commissioner must have regard to the purpose for which the data was obtained and further processed.

(5) Subsections (6) and (7) apply where—

(a) an enforcement notice requires a controller or processor to rectify or erase personal data, or

(b) the Commissioner is satisfied that the processing of personal data which has been rectified or erased by the controller or processor involved a failure described in subsection (1).

(6) An enforcement notice may, if reasonably practicable, require the controller or processor to notify third parties to whom the data has been disclosed of the rectification or erasure.

(7) In determining whether it is reasonably practicable to require such notification, the Commissioner must have regard, in particular, to the number of people who would have to be notified.

(8) In this section, "data protection principle relating to accuracy" means the principle in—

(a) Article 5(1)(d) of the GDPR,

(b) section 36(1) of this Act, or

(c) section 87 of this Act.

145 Enforcement notices: restrictions

(1) The Commissioner may not give a controller or processor an enforcement notice in reliance on section 142(2) with respect to the processing of personal data for the special purposes unless—

(a) a determination under section 164 with respect to the data or the processing has taken effect, and

(b) the 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 142(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) 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 56 or 102, the Commissioner may only give the controller an enforcement notice in reliance on section 142(2) if the controller is responsible for compliance with the provision, requirement or principle in question.

146 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

147 Powers of entry and inspection

Schedule 15 makes provision about powers of entry and inspection.

Penalties

148 Penalty notices

(1) If the Commissioner is satisfied that a person—

(a) has failed or is failing as described in section 142(2), (3), (4) or (5),

(b) has failed to comply with an assessment notice given in exercise of the Commissioner's powers under Article 58(1) of the GDPR, or

(c) has failed to comply with an enforcement notice,

the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.

(2) In the case of a failure described in section 142(2), (3) or (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant—

(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR;

(b) to the extent that the notice concerns another matter, the matters listed in subsection (3).

(3) Those matters are—

(a) the nature, gravity and duration of the failure;

(b) the intentional or negligent character of the failure;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor in accordance with section 55, 64, 101 or 105;

(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) 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.

(5) The Secretary of State may by regulations—

(a) confer power on the Commissioner to give a penalty notice in respect of other failures, and

(b) make provision about the amount of the penalty that may be imposed.

(6) Before making regulations under this section, the Secretary of State must consult such persons as the Secretary of State considers appropriate.

(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 149 to 151, and

(c) are subject to the affirmative resolution procedure.

149 Penalty notices: restrictions

(1) The Commissioner may not give a controller or processor a penalty notice in reliance on section 142(2) with respect to the processing of personal data for the special purposes unless—

(a) a determination under section 164 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 142(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 penalty notice to—

(a) the Crown Estate Commissioners, or

(b) a person who is a controller under section 188(3) (controller for the Royal Household etc).

(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 56 or 102, the Commissioner may only give the controller a penalty notice in reliance on section 142(2) if the controller is responsible for compliance with the provision, requirement or principle in question.

150 Maximum amount of penalty

(1) In relation to an infringement of a provision of the GDPR, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) the amount specified in Article 83 of the GDPR, or

(b) if an amount is not specified there, the standard maximum amount.

(2) In relation to an infringement of a provision of Part 3 of this Act, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) in relation to a failure to comply with section 33, 34, 35, 36(1), 37(1), 38, 42, 43, 44, 45, 46, 47, 50, 51, 71, 72, 73, 74, 75 or 76, the higher maximum amount, and

(b) otherwise, the standard maximum amount.

(3) In relation to an infringement of a provision of Part 4 of this Act, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) in relation to a failure to comply with section 84, 85, 86, 87, 88, 89, 91, 92, 98 or 107, the higher maximum amount, and

(b) otherwise, the standard maximum amount.

(4) In relation to a failure to comply with an enforcement notice, the maximum amount of the penalty that may be imposed by a penalty notice is the higher maximum amount.

(5) The "higher maximum amount" is—

(a) in the case of an undertaking, 20 million Euros or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or

(b) in any other case, 20 million Euros.

(6) The "standard maximum amount" is—

(a) in the case of an undertaking, 10 million Euros or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or

(b) in any other case, 10 million Euros.

(7) The maximum amount of a penalty in sterling must be determined by applying the spot rate of exchange set by the Bank of England on the day on which the penalty notice is given.

151 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 132.

(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,

(b) such other persons as the Secretary of State considers appropriate.

(6) The Commissioner must arrange for a document published under this section (including any altered or replacement document) to be laid before Parliament.

152 Amount of penalties: supplementary

(1) For the purposes of Article 83 of the GDPR and section 150, the Secretary of State may by regulations—

(a) provide that a person of a description specified in the regulations is or is not an undertaking, and

(b) make provision about how an undertaking's turnover is to be determined.

(2) For the purposes of Article 83 of the GDPR, section 150 and section 151, the Secretary of State may by regulations provide that a period is or is not a financial year.

(3) Before making regulations under this section, the Secretary of State must consult such persons as the Secretary of State considers appropriate.

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

Guidance

153 Guidance about regulatory action

(1) The Commissioner must produce and publish guidance about how the Commissioner proposes to exercise the Commissioner's functions in connection with—

(a) assessment notices,

(b) enforcement notices, and

(c) penalty notices.

(2) The Commissioner may produce and publish guidance about how the Commissioner proposes to exercise the Commissioner's other functions under this Part.

(3) In relation to assessment notices, the guidance must include—

(a) provision specifying factors to be considered in determining whether to give an assessment notice to a person;

(b) provision specifying descriptions of documents or information that—

(i) are not to be examined or inspected in accordance with an assessment notice, or

(ii) are to be so examined or inspected only by a person of a description specified in the guidance;

(c) provision about the nature of inspections and examinations carried out in accordance with an assessment notice;

(d) provision about the nature of interviews carried out in accordance with an assessment notice;

(e) provision about the preparation, issuing and publication by the Commissioner of assessment reports in respect of controllers and processors that have been given assessment notices.

(4) The guidance prepared in accordance with subsection (3)(b) must include provisions that relate to—

(a) documents and information concerning an individual's physical or mental health;

(b) documents and information concerning the provision of social care for an individual.

(5) In relation to penalty notices, the guidance must include—

(a) provision about the circumstances in which the Commissioner would consider it appropriate to issue a penalty notice;

(b) provision about the circumstances in which the Commissioner would consider it appropriate to allow a controller or processor make oral representations about a notice of intent;

(c) provision explaining how the Commissioner will determine the amount of penalties.

(6) The Commissioner—

(a) may alter or replace the guidance, and

(b) must publish any altered or replacement guidance.

(7) Before publishing guidance under this section (including any altered or replacement guidance), the Commissioner must consult—

(a) the Secretary of State, and

(b) such other persons as the Secretary of State considers appropriate.

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

(9) 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).

Appeals

154 Rights of appeal

(1) A person who is given any of the following notices may appeal to the Tribunal—

(a) an information notice;
(b) an assessment notice;
(c) an enforcement notice;
(d) a penalty notice;
(e) a penalty variation notice.

(2) Where a notice listed in subsection (1) contains a statement under section 137(7)(a), 140(8)(a) or 143(8) (urgency), the person given the notice may appeal against—

(a) the Commissioner's decision to include the statement in the notice, or
(b) the effect of its inclusion as respects any part of the notice,

whether or not the person appeals against the notice.

(3) A person who is given an enforcement notice may appeal to the Tribunal against the refusal of an application under section 146 for the cancellation or variation of the notice.

(4) A person who is given a penalty notice or a penalty variation notice may appeal against the amount of the penalty specified in the notice, whether or not the person appeals against the notice.

(5) Where a determination is made under section 164 in respect of the processing of personal data, the controller or processor may appeal to the Tribunal against the determination.

155 Determination of appeals

(1) Subsections (2) to (4) apply where a person appeals to the Tribunal under section 154(1) or (4).

(2) The Tribunal may review any determination of fact on which the notice or decision against which the appeal is brought was based.

(3) If the Tribunal considers—

(a) that the notice or decision against which the appeal is brought is not in accordance with the law, or
(b) to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently,

the Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.

(4) Otherwise, the Tribunal must dismiss the appeal.

(5) On an appeal under section 154(2), the Tribunal may direct—

(a) that the notice against which the appeal is brought is to have effect as if it did not contain the statement under section 137(7)(a), 140(8)(a) or 143(8) (urgency), or

(b) that the inclusion of that statement is not to have effect in relation to any part of the notice,

and may make such modifications to the notice as are required to give effect to the direction.

(6) On an appeal under section 154(3), if the Tribunal considers that the enforcement notice ought to be cancelled or varied by reason of a change in circumstances, the Tribunal must cancel or vary the notice.

(7) On an appeal under section 154(5), the Tribunal may cancel the Commissioner's determination.

Complaints

156 Complaints by data subjects

(1) Articles 57(1)(f) and (2) and 77 of the GDPR (data subject's right to lodge a complaint) confer rights on data subjects to complain to the Commissioner if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of the GDPR.

(2) A data subject may make a complaint to the Commissioner if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of Part 3 or 4 of this Act.

(3) The Commissioner must facilitate the making of complaints under subsection (2) by taking steps such as providing a complaint form which can be completed electronically and by other means.

(4) If the Commissioner receives a complaint under subsection (2), the Commissioner must—

(a) take appropriate steps to respond to the complaint,

(b) inform the complainant of the outcome of the complaint,

(c) inform the complainant of the rights under section 157, and

(d) if asked to do so by the complainant, provide the complainant with further information about how to pursue the complaint.

(5) The reference in subsection (4)(a) to taking appropriate steps in response to a complaint includes—

(a) investigating the subject matter of the complaint, to the extent appropriate, and

(b) informing the complainant about progress on the complaint, including about whether further investigation or co-ordination with another supervisory authority or foreign designated authority is necessary.

(6) If the Commissioner receives a complaint relating to the infringement of a data subject's rights under provisions adopted by a member State other than the United Kingdom pursuant to the Law Enforcement Directive, the Commissioner must—

(a) send the complaint to the relevant supervisory authority for the purposes of that Directive,
(b) inform the complainant that the Commissioner has done so, and
(c) if asked to do so by the complainant, provide the complainant with further information about how to pursue the complaint.

(7) In this section—
"foreign designated authority" means an authority designated for the purposes of Article 13 of the Data Protection Convention by a party, other than the United Kingdom, which is bound by that Convention;
"supervisory authority" means a supervisory authority for the purposes of Article 51 of the GDPR or Article 41 of the Law Enforcement Directive in a member State other than the United Kingdom.

157 Orders to progress complaints

(1) This section applies where, after a data subject makes a complaint under section 156 or Article 77 of the GDPR, the Commissioner—
(a) fails to take appropriate steps to respond to the complaint,
(b) fails to provide the complainant with information about progress on the complaint, or of the outcome of the complaint, before the end of the period of 3 months beginning with the day on which the Commissioner received the complaint, or
(c) if the Commissioner's consideration of the complaint is not concluded during that period, fails to provide the complainant with such information during a subsequent period of 3 months.

(2) The Tribunal may, on an application by the data subject, make an order requiring the Commissioner—
(a) to take appropriate steps to respond to the complaint, or
(b) to inform the complainant of progress on the complaint, or of the outcome of the complaint, within a period specified in the order.

(3) An order under subsection (2)(a) may require the Commissioner—
(a) to take steps specified in the order;
(b) to conclude the investigation, or take a specified step, within a period specified in the order.

(4) Section 156(5) applies for the purposes of subsections (1)(a) and (2)(a) as it applies for the purposes of section 156(4)(a).

Remedies in the court

158 Compliance orders

(1) This section applies if, on an application by a data subject, a court is satisfied that there has been an infringement of the data subject's rights under the data protection legislation in contravention of that legislation.

(2) A court may make an order for the purposes of securing compliance with the data protection legislation which requires the controller in respect of the processing, or a processor acting on behalf of that controller—
(a) to take steps specified in the order, or
(b) to refrain from taking steps specified in the order.

(3) The order may, in relation to each step, specify the time at which, or the period within which, it must be taken.

(4) In subsection (1)—

(a) the reference to an application by a data subject includes an application made in exercise of the right under Article 79(1) of the GDPR (right to an effective remedy against a controller or processor);

(b) the reference to the data protection legislation does not include Part 4 of this Act or regulations made under that Part.

(5) In relation to a joint controller in respect of the processing of personal data to which Part 3 applies whose responsibilities are determined in an arrangement under section 56, 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.

159 Compensation for contravention of the GDPR

(1) In Article 82 of the GDPR (right to compensation) "damage" includes financial loss, distress and other adverse effects.

(2) Subsection (3) applies where—

(a) in accordance with rules of court, proceedings under Article 82 of the GDPR are brought by a representative body on behalf of a person, and

(b) a court orders the payment of compensation.

(3) The court may make an order providing for the compensation to be paid on behalf of the person to—

(a) the representative body, or

(b) such other person as the court thinks fit.

160 Compensation for contravention of other data protection legislation

(1) A person who suffers damage by reason of a contravention of a requirement of the data protection legislation, other than the GDPR, is entitled to compensation for that damage from the controller or the processor, subject to subsections (2) and (3).

(2) Under subsection (1)—

(a) a controller involved in processing of personal data is liable for any damage caused by the processing, and

(b) a processor involved in processing of personal data is liable for damage caused by the processing only if the processor—

(i) has not complied with an obligation under the data protection legislation specifically directed at processors, or

(ii) has acted outside, or contrary to, the controller's lawful instructions.

(3) A controller or processor is not liable as described in subsection (2) if the controller or processor proves that the controller or processor is not in any way responsible for the event giving rise to the damage.

(4) A joint controller in respect of the processing of personal data to which Part 3 or 4 applies whose responsibilities are determined in an arrangement under section 56 or 102 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, distress and other adverse effects, whether or not material.

Offences relating to personal data

161 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
  (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, or
  (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.

(4) It is an offence for a person to sell personal data if the person obtained the data in circumstances in which an offence under subsection (1) was committed.

(5) It is an offence for a person to offer to sell personal data if the person—
  (a) has obtained the data in circumstances in which an offence under subsection (1) was committed, or
  (b) subsequently obtains the data in such circumstances.

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale is an offer to sell the data.

(7) In this section—
  (a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 57(8) or 103(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.

162 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—
  (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
  (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 the person acted in the reasonable belief that —
  (a) 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, or
  (b) 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.

(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
  (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 the person acted in the reasonable belief that—
  (a) the processing was lawful, or

(b) 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.

(8) In this section—

(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 57(8) or 103(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.

163 Alteration etc of personal data to prevent disclosure

(1) Subsection (3) applies where—

(a) a request has been made in exercise of a data subject access right, and

(b) the person making the request would have been entitled to receive information in response to that request.

(2) In this section, "data subject access right" means a right under—

(a) Article 15 of the GDPR (right of access by the data subject);

(b) Article 20 of the GDPR (right to data portability);

(c) section 43 of this Act (law enforcement processing: right of access by the data subject);

(d) section 92 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

164 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 under section 158 (including proceedings on an application under Article 79 of the GDPR) which relate, wholly or partly, to personal data processed for the special purposes.

(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;
(c) carrying out the processing in compliance with a provision of the data protection legislation specified in the determination, is not incompatible with the special purposes.

(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 154.

(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.

165 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 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.

166 Staying special purposes proceedings

(1) In any special purposes proceedings before a court or tribunal, if the controller or processor claims, or it appears to the court or tribunal, 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, literary or artistic material, and

(c) has not previously been published by the controller,

the court or tribunal must stay 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 or tribunal must stay the proceedings until either of the following conditions is met—

(a) a determination of the Commissioner under section 164 with respect to the personal data or the processing takes effect;

(b) where the proceedings were stayed on the making of a claim, the claim is withdrawn.

Jurisdiction of courts

167 Jurisdiction

(1) The jurisdiction conferred on a court by the provisions listed in subsection (2) is exercisable—

(a) in England and Wales, by the High Court or the county court,

(b) in Northern Ireland, by the High Court or a county court, and

(c) in Scotland, by the Court of Session or the sheriff,

subject to subsection (3).

(2) Those provisions are—

(a) section 145 (enforcement notices and processing for the special purposes);

(b) section 149 (penalty notices and processing for the special purposes);

(c) section 158 and Article 79 of the GDPR (compliance orders);

(d) sections 159 and 160 and Article 82 of the GDPR (compensation).

(3) In relation to the processing of personal data to which Part 4 applies, the jurisdiction is exercisable only by the High Court or, in Scotland, the Court of Session.

Definitions

168 Interpretation of Part 6

In this Part—

"assessment notice" has the meaning given in section 140;

"certification provider" has the meaning given in section 16;

"the data protection principles" means the principles listed in—

(a) Article 5(1) of the GDPR,

(b) section 32(1) of this Act, and

(c) section 83(1) of this Act;

"enforcement notice" has the meaning given in section 142;

"information notice" has the meaning given in section 137;

"penalty notice" has the meaning given in section 148;

"penalty variation notice" has the meaning given in Schedule 16;

"representative", in relation to a controller or processor, means a person designated by the controller or processor under Article 27 of the GDPR to represent the controller or processor with regard to the controller's or processor's obligations under the GDPR.

PART 7

SUPPLEMENTARY AND FINAL PROVISION

Regulations under this Act

169 Regulations and consultation

(1) Regulations under this Act are to be made by statutory instrument.

(2) The Secretary of State must consult the Commissioner before making regulations under this Act, other than regulations made under—
  (a) section 21;
  (b) section 28;
  (c) section 190;
  (d) section 191;
  (e) section 192;
  (f) paragraph 13 or 24 of Schedule 2.

(3) Regulations under this Act may—
  (a) make different provision for different purposes;
  (b) include consequential, supplementary, incidental, transitional, transitory or saving provision.

(4) 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.

(5) 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.

(6) Any provision that may be included in regulations under this Act subject to the negative resolution procedure may be made by regulations subject to the affirmative resolution procedure.

(7) 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.

Changes to the Data Protection Convention

170 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 add to or otherwise amend the Commissioner's functions, and
  (b) to amend this Act.

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

Rights of the data subject

171 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
(b) in the particular circumstances, was justified as being in the public interest.

(4) The imposition of the requirement referred to in subsection (1) or (2) is not to be regarded as justified as being in the public interest on the ground that it would assist in the prevention or detection of crime, given Part 5 of the Police Act 1997 (certificates of criminal records etc).

(5) In subsections (1) and (2), the references to a person who requires another person to provide or give access to a relevant record include a person who asks another person to do so—
(a) knowing that, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request, or
(b) being reckless as to whether, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request,

and the references to a "requirement" in subsections (3) and (4) are to be interpreted accordingly.

(6) In this section—

"employment" means any employment, including—
(a) work under a contract for services or as an office-holder,
(b) work under an apprenticeship,
(c) work experience as part of a training course or in the course of training for employment, and
(d) voluntary work,

and "employee" is to be interpreted accordingly;

"relevant record" has the meaning given in Schedule 17 and references to a relevant record include—
(a) a part of such a record, and
(b) a copy of, or of part of, such a record.

172 Avoidance of certain contractual terms relating to health records

(1) A term or condition of a contract is void in so far as it purports to require an individual to supply another person with a record which—
(a) consists of the information contained in a health record, and
(b) has been or is to be obtained by a data subject in the exercise of a data subject access right.

(2) A term or condition of a contract is also void in so far as it purports to require an individual to produce such a record to another person.

(3) The references in subsections (1) and (2) to a record include a part of a record and a copy of all or part of a record.

(4) In this section, "data subject access right" means a right under—
(a) Article 15 of the GDPR (right of access by the data subject);
(b) Article 20 of the GDPR (right to data portability);
(c) section 43 of this Act (law enforcement processing: right of access by the data subject);
(d) section 92 of this Act (intelligence services processing: right of access by the data subject).

173 Representation of data subjects

(1) In relation to the processing of personal data to which the GDPR applies—
(a) Article 80 of the GDPR (representation of data subjects) enables a data subject to authorise a body or other organisation which meets the conditions set out in that Article to exercise certain rights on the data subject's behalf, and
(b) a data subject may also authorise such a body or organisation to exercise the data subject's rights under Article 82 (right to compensation).

(2) In relation to the processing of personal data to which the GDPR does not apply, a body or other organisation which meets the conditions in subsections (3) and (4), if authorised to do so by a data subject, may exercise some or all of the following rights under the following provisions on the data subject's behalf—
(a) section 156(2), (4)(d) and (6)(c) (complaints to the Commissioner);
(b) section 157(2) (orders for the Commissioner to progress complaints);
(c) section 158(1) (compliance orders);
(d) the right to bring judicial review proceedings against the Commissioner.

(3) The first condition is that the body or organisation, by virtue of its constitution or an enactment—
(a) is required (after payment of outgoings) to apply the whole of its income and any capital it expends for charitable or public purposes,
(b) is prohibited from directly or indirectly distributing amongst its members any part of its assets (otherwise than for charitable or public purposes), and
(c) has objectives which are in the public interest.

(4) The second condition is that the body or organisation is active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data.

(5) In this Act, references to a "representative body", in relation to a right of a data subject, are to a body or other organisation authorised to exercise the right on the data subject's behalf under Article 80 of the GDPR or this section.

174 Data subject's rights and other prohibitions and restrictions

(1) An enactment or rule of law prohibiting or restricting the disclosure of information, or authorising the withholding of information, does not remove or restrict the obligations and rights provided for in the provisions listed in subsection (2), except as provided by or under the provisions listed in subsection (3).

(2) The provisions providing obligations and rights are—

(a) Chapter III of the GDPR (rights of the data subject),

(b) Chapter 3 of Part 3 of this Act (law enforcement processing: rights of the data subject), and

(c) Chapter 3 of Part 4 of this Act (intelligence services processing: rights of the data subject).

(3) The provisions providing exceptions are—

(a) in Chapter 2 of Part 2 of this Act (including as applied by Chapter 3 of that Part), sections 14 and 15 and Schedules 2, 3 and 4,

(b) in Chapter 3 of Part 2 of this Act, sections 21, 22, 23 and 24,

(c) in Part 3 of this Act, sections 42(4), 43(4) and 46(3), and

(d) in Part 4 of this Act, Chapter 6.

Offences

175 Penalties for offences

(1) A person who commits an offence under section 117 or 163 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 127, 139, 161, 162 or 171 is liable—

(a) on summary conviction in England and Wales, to a fine;

(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding the statutory maximum;

(c) on conviction on indictment, to a fine.

(3) Subsections (4) and (5) apply where a person is convicted of an offence under section 161 or 171.

(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.

176 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 163 (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.

177 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.

178 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 117;
(b) section 127;
(c) section 139;
(d) section 161;
(e) section 162;
(f) section 163;
(g) section 171;
(h) 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).

179 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

180 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 its functions under—

(a) the data protection legislation, or
(b) the information regulations.

(2) In this section, "the information regulations" has the same meaning as in section 126.

181 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 25, 77, 109 or 154, or

(ii) for an order under section 157, 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.

182 Tribunal Procedure Rules

(1) Tribunal Procedure Rules may make provision for regulating—

(a) the exercise of the rights of appeal conferred by section 25, 77, 109 or 154, and

(b) the exercise of the rights of data subjects under section 157, including their exercise by a representative body.

(2) In relation to proceedings involving the exercise of those rights, Tribunal Procedure Rules may make provision about—

(a) securing the production of material used for the processing of personal data, and

(b) the inspection, examination, operation and testing of equipment or material used in connection with the processing of personal data.

Definitions

183 Meaning of "health professional" and "social work professional"

(1) In this Act, "health professional" means any of the following—

(a) a registered medical practitioner;

(b) a registered nurse or midwife;

(c) a registered dentist within the meaning of the Dentists Act 1984 (see section 53 of that Act);

(d) a registered dispensing optician or a registered optometrist within the meaning of the Opticians Act 1989 (see section 36 of that Act);

(e) a registered osteopath with the meaning of the Osteopaths Act 1993 (see section 41 of that Act);

(f) a registered chiropractor within the meaning of the Chiropractors Act 1994 (see section 43 of that Act);

(g) a person registered as a member of a profession to which the Health and Social Work Professions Order 2001 (S.I. 2002/254) for the time being extends, other than the social work profession in England;

(h) a registered pharmacist or a registered pharmacy technician within the meaning of the Pharmacy Order 2010 (S.I. 2010/231) (see Article 3 of that Order);

(i) a registered person within the meaning of the Pharmacy (Northern Ireland) Order 1976 (S.I. 1976/1213 (N.I. 22)) (see Article 2 of that Order);

(j) a child psychotherapist;

(k) a scientist employed by a health service body as head of a department.

(2) In this Act, "social work professional" means any of the following—

(a) a person registered as a social worker in England in the register maintained under the Health and Social Work Professions Order 2001 (S.I. 2002/254);

(b) a person registered as a social worker in the register maintained by Social Care Wales under section 80 of the Regulation and Inspection of Social Care (Wales) Act 2016 (anaw 2);

(c) a person registered as a social worker in the register maintained by the Scottish Social Services Council under section 44 of the Regulation of Care (Scotland) Act 2001 (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)).

184 Other definitions

In this Act—

"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data;

"data concerning health" means personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveals information about his or her health status;

"enactment" includes—

(a) an enactment passed or made after this Act,

(b) an enactment comprised in subordinate legislation,

(c) an enactment comprised in, or in an instrument made under, a Measure or Act of the National Assembly for Wales,

(d) an enactment comprised in, or in an instrument made under, an Act of the Scottish Parliament, and

(e) an enactment comprised in, or in an instrument made under, Northern Ireland legislation;

"genetic data" means personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about the physiology or the health of that individual and which results, in particular, from an analysis of a biological sample from the individual in question;

"government department" includes—

(a) a part of the Scottish Administration;

(b) a Northern Ireland department;
(c) the Welsh Government;
(d) a body or authority exercising statutory functions on behalf of the Crown;

"health record" means a record which—
(a) consists of data concerning health, and
(b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates;

"inaccurate", in relation to personal data, means incorrect or misleading as to any matter of fact;

"international obligation of the United Kingdom" includes—
(a) an EU obligation, and
(b) an obligation that arises under an international agreement or arrangement to which the United Kingdom is a party;

"international organisation" means an organisation and its subordinate bodies governed by international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

"Minister of the Crown" has the same meaning as in the Ministers of the Crown Act 1975;

"publish" means make available to the public or a section of the public;

"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.

185 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 169
the applied Chapter 2 (in Chapter 3 of Part 2)	section 20
the applied GDPR	section 2
assessment notice (in Part 6)	section 168
biometric data	section 184
certification provider (in Part 6)	section 168

the Commissioner	section 2
competent authority (in Part 3)	section 28
consent (in Part 4)	section 82
controller	section 2
data concerning health	section 184
the Data Protection Convention	section 2
the data protection legislation	section 2
the data protection principles (in Part 6)	section 168
data subject	section 2
employee (in Parts 3 and 4)	sections 31 and 82
enactment	section 184
enforcement notice (in Part 6)	section 168
filing system	section 2
FOI public authority (in Chapter 3 of Part 2)	section 19
the GDPR	section 2
genetic data	section 184
government department	section 184
health professional	section 183
health record	section 184
identifiable living individual	section 2
inaccurate	section 184
information notice (in Part 6)	section 168
intelligence service (in Part 4)	section 80
international obligation of the United Kingdom	section 184
international organisation	section 184
the Law Enforcement Directive	section 2
the law enforcement purposes (in Part 3)	section 29
Minister of the Crown	section 184

the negative resolution procedure	section 169
penalty notice (in Part 6)	section 168
penalty variation notice (in Part 6)	section 168
personal data	section 2
personal data breach (in Parts 3 and 4)	sections 31 and 82
processing	section 2
processor	section 2
profiling (in Part 3)	section 31
public authority (in the GDPR and Part 2)	section 6
public body (in the GDPR and Part 2)	section 6
publish	section 184
recipient (in Parts 3 and 4)	sections 31 and 82
representative (in Part 6)	section 168
representative body (in relation to a right of a data subject)	section 173
restriction of processing (in Parts 3 and 4)	sections 31 and 82
social work professional	section 183
the special purposes (in Part 6)	section 164
special purposes proceedings (in Part 6)	section 164
subordinate legislation	section 184
third country (in Part 3)	section 31
tribunal	section 184
the Tribunal	section 184

Territorial application

186 Territorial application of this Act

(1) This Act applies to a controller in respect of the processing of personal data only if the controller is established in the United Kingdom and the personal

data is processed in the context of the activities of that establishment, subject to subsection (3).

(2) This Act applies to a processor in respect of the processing of personal data only if—

(a) the controller on whose behalf the processor acts is established in the United Kingdom and the personal data is processed in the context of the activities of that establishment, or

(b) the processor is established in the United Kingdom and the personal data is processed in the context of the activities of that establishment,

subject to subsection (4).

(3) This Act also applies to a controller in respect of the processing of personal data to which Chapter 2 of Part 2 (the GDPR) applies where—

(a) the controller is established in a country or territory other than the United Kingdom and the personal data is processed in the context of the activities of that establishment,

(b) the personal data relates to an individual who is in the United Kingdom when the processing takes place, and

(c) the purpose of the processing is—

(i) to offer goods or services to individuals in the United Kingdom, whether or not for payment, or

(ii) to monitor individuals' behaviour in the United Kingdom.

(4) This Act also applies to a processor in respect of the processing of personal data to which Chapter 2 of Part 2 (the GDPR) applies where—

(a) the controller on whose behalf the processor acts is established in a country or territory other than the United Kingdom and the personal data is processed in the context of the activities of that establishment, or

(b) the processor is established in a country or territory other than the United Kingdom and the personal data is processed in the context of the activities of that establishment,

and the conditions in subsection (3)(b) and (c) are satisfied.

(5) Subsections (1) to (4) have effect subject to any provision made under section 118 providing for the Commissioner to carry out functions in relation to other controllers or processors.

(6) In this section, references to a person established 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 carried on activities through, an office, branch or agency or other stable arrangements in the United Kingdom,

and references to establishment in another country or territory have a corresponding meaning.

(7) For the purposes of this section—

(a) a person who is treated as a controller by virtue of Article 28(10) of the GDPR or section 57(8) or 103(3) of this Act (processor to be treated as controller in certain circumstances) is to be treated as a processor;

(b) where there is more than one controller, the references in subsections (2)(a) and (4)(a) to the controller are to one or more of them.

General

187 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.

188 Application to the Crown

(1) This Act binds the Crown.

(2) For the purposes of this Act, each government department is to be treated as a person separate from the other government departments.

(3) Where the purposes for which and the manner in which personal data is, or is to be, processed are determined by a person acting on behalf of the Royal Household, the Duchy of Lancaster or the Duchy of Cornwall, the controller in respect of that data for the purposes of the GDPR and this Act is—

(a) in relation to the Royal Household, the Keeper of the Privy Purse,

(b) in relation to the Duchy of Lancaster, such person as the Chancellor of the Duchy appoints, and

(c) in relation to the Duchy of Cornwall, such person as the Duke of Cornwall, or the possessor for the time being of the Duchy of Cornwall, appoints.

(4) Different persons may be appointed under subsection (3)(b) or (c) for different purposes.

(5) The following provisions apply to a person in the service of the Crown as they apply to any other person—

(a) section 117;

(b) section 161;

(c) section 162;

(d) section 163;

(e) paragraph 15 of Schedule 15.

(6) Subject to subsection (5), neither a government department nor a person who is a controller under subsection (3) is liable to prosecution under the GDPR or this Act.

189 Application to Parliament

(1) Parts 1, 2 and 5 to 7 of this Act apply to the processing of personal data by or on behalf of either House of Parliament.

(2) Where the purposes for which and the manner in which personal data is, or is to be, processed are determined by or on behalf of the House of Commons, the controller in respect of that data for the purposes of the GDPR and this Act is the Corporate Officer of that House.

(3) Where the purposes for which and the manner in which personal data is, or is to be, processed are determined by or on behalf of the House of Lords, the controller in respect of that data for the purposes of the GDPR and this Act is the Corporate Officer of that House.

(4) Subsections (2) and (3) do not apply where the purposes for which and the manner in which the personal data is, or is to be, processed are determined by or on behalf of the Intelligence and Security Committee of Parliament.

(5) The following provisions apply to a person acting on behalf of either House as they apply to any other person—

(a) section 161;
(b) section 162;
(c) section 163;
(d) paragraph 15 of Schedule 15.

(6) Subject to subsection (5), 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 the GDPR or this Act.

190 Minor and consequential amendments

(1) Schedule 18 contains minor and consequential amendments.

(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

191 Commencement

(1) Except as provided by subsection (2), this Act comes into force on such day as the Secretary of State may by regulations appoint.

(2) This section and the following provisions come into force on the day on which this Act is passed—

(a) sections 1 and 2;
(b) section 169;
(c) sections 183, 184 and 185;
(d) sections 188 and 189;
(e) this section and sections 192, 193 and 194;
(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.

192 Transitional provision

The Secretary of State may by regulations make transitional, transitory or saving provision in connection with the coming into force of any provision of this Act.

193 Extent

(1) This Act extends to England and Wales, Scotland and Northern Ireland, subject to—

(a) subsections (2) and (3), and
(b) paragraph 12 of Schedule 12.

(2) Section 178 extends to England and Wales only.

(3) An amendment, repeal or revocation made by this Act has the same extent as the enactment amended, repealed or revoked.

194 Short title

This Act may be cited as the Data Protection Act 2017.

SCHEDULES

SCHEDULE 1

Section 9

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 of the controller or the data subject under employment law, social security law or the law relating to social protection, and

(b) when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 30 in Part 4 of this Schedule).

(2) See also the additional safeguards in Part 4 of this Schedule.

(3) In this paragraph—

"social security law" includes the law relating to 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 amended from time to time).

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 GDPR (obligations of secrecy) and section 10(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 supervision 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 89(1) of the GDPR (as supplemented by section 18), and

(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) 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 30 in Part 4 of this Schedule).

(2) See also the additional safeguards in Part 4 of this Schedule.

Parliamentary, statutory 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 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;

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

Equality of opportunity or treatment

7 (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—

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

(b) it is carried out without that data subject's consent.

(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.

Preventing or detecting unlawful acts

8 (1) This condition is met if the processing—

(a) is necessary for the purposes of the prevention or detection of an unlawful act,

(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 this paragraph, "act" includes a failure to act.

Protecting the public against dishonesty etc

9 (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.

Journalism etc in connection with unlawful acts and dishonesty etc

10 (1) This condition is met if—
(a) the processing consists of the disclosure of personal data for the special purposes,
(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) 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

11 (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, or

(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

12 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).

Counselling etc

13 (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 a reason 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).

Insurance

14 (1) This condition is met if the processing—

(a) is necessary for the purpose of carrying on insurance business,

(b) is of data concerning health which relates to a data subject who is the parent, grandparent, great-grandparent or sibling of an insured person,

(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—

"insurance business" means business which consists of effecting or carrying out contracts for the following types of insurance—

(a) life and annuity;

(b) linked long term;

(c) permanent health;

(d) accident;

(e) sickness;

"insured person" includes an individual who is seeking to become an insured person.

(4) Terms used in the definition of "insurance business" in sub-paragraph (3) and also in an order made under section 22 of the Financial Services and Markets Act 2000 (regulated markets) have the same meaning in that sub-paragraph as they have in that order.

Third party data processing for group insurance policies and insurance on the life of another

15 (1) This condition is met if the processing—

(a) is necessary for the purpose of carrying on business which consists of effecting or carrying out a contract described in sub-paragraph (2),

(b) is of personal data which relates to a data subject who is not a party to the contract or seeking to become a party to the contract, and

(c) can reasonably be carried out without the consent of the data subject.

(2) The contracts mentioned in sub-paragraph (1)(a) are—

(a) a contract which satisfies section 7(1)(a) to (c) of the Consumer Insurance (Disclosure and Representations) Act 2012 (group insurance contracts);

(b) a contract to which section 8 of that Act applies (consumer insurance contract for life insurance on the life of another).

(3) For the purposes of sub-paragraph (1)(c), 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.

Occupational pensions

16 (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 not carried out for the purposes of measures or decisions with respect to the data subject, and

(c) can reasonably be carried out without the consent of the data subject.

(2) For the purposes of sub-paragraph (1)(c), 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.

Political parties

17 (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

18 (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) a member of the European Parliament elected in the United Kingdom;

(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) the Mayor of London or an elected member of the London Assembly;

(i) an elected member of—

(i) the Common Council of the City of London, or

(ii) the Council of the Isles of Scilly;

(j) an elected member of a council constituted under section 2 of the Local Government etc (Scotland) Act 1994;

(k) an elected member of a district council within the meaning of the Local Government Act (Northern Ireland) 1972.

(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 Scottish Parliament immediately before that Parliament is dissolved,

(c) a Member of the Northern Ireland Assembly immediately before that Assembly is dissolved, or

(d) a Member of the National Assembly for Wales 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

19 (1) This condition is met if—

(a) the processing consists of the disclosure of personal data—

(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 18.

Informing elected representatives about prisoners

20 (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 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.

Anti-doping in sport

21 (1) This condition is met if the processing is carried out—

(a) in connection with measures designed to eliminate doping which are undertaken by or under the supervision of a body with responsibility 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.

(2) The reference in sub-paragraph (1)(a) to measures designed to eliminate doping include measures designed to identify or prevent doping.

PART 3

ADDITIONAL CONDITIONS RELATING TO CRIMINAL CONVICTIONS ETC

Consent

22 This condition is met if the data subject has given consent to the processing.

Protecting individual's vital interests

23 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

24 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

25 This condition is met if the processing relates to personal data which is manifestly made public by the data subject.

Legal claims and judicial acts

26 This condition is met if the processing is necessary for the establishment, exercise or defence of a legal claim or whenever a court is acting in its judicial capacity.

Administration of accounts used in commission of indecency offences involving children

27 (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 30 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 certain conditions under Part 2 of this Schedule

28 (1) This condition is met if—

(a) 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, and

(b) when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 30 in Part 4 of this Schedule).

(2) See also the additional safeguards in Part 4 of this Schedule.

PART 4

APPROPRIATE POLICY DOCUMENT AND ADDITIONAL SAFEGUARDS

Application of this Part

29 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

30 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 29 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 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

31 (1) Where personal data is processed in reliance on a condition described in paragraph 29, 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 29, 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 on the day the controller ceases to carry out such processing.

Additional safeguard: record of processing

32 A record maintained by the controller, or the controller's representative, under Article 30 of the GDPR in respect of the processing of personal data in reliance on a condition described in paragraph 29 must include the following information—

(a) which condition is relied on,

(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing), and

(c) whether the personal data is retained and erased in accordance with the policies described in paragraph 30(b) and, if it is not, the reasons for not following those policies.

SCHEDULE 2

Section 14

EXEMPTIONS ETC FROM THE GDPR

PART 1

ADAPTATIONS AND RESTRICTIONS BASED ON ARTICLES 6(3) AND 23(1)

GDPR provisions to be adapted or restricted: "the listed GDPR provisions"

1 In this Part "the listed GDPR provisions" means—

(a) the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the 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 20(1) and (2) (right to data portability);

(viii) Article 21(1) (objections to processing);

(ix) 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 (viii); and

(b) the following provisions of the GDPR (the application of which may be adapted by virtue of Article 6(3) of the 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).

Crime and taxation: general

2 (1) The listed GDPR provisions do not apply to personal data processed for any of the following purposes—

(a) the prevention or detection of crime,

(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 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 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 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.

(3) The GDPR provisions referred to in sub-paragraph (1) are the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the 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 listed GDPR provisions do not apply to personal data processed 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).

(2) Sub-paragraph (3) applies where—
(a) personal data is processed by a person ("Controller 1"), and
(b) another person ("Controller 2") obtains the data from Controller 1 for any of the purposes mentioned in sub-paragraph (1)(a) and (b) and processes it for any of those purposes.

(3) Controller 1 is exempt from the obligations in the following provisions of the 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 2 is exempt from those obligations by virtue of sub-paragraph (1).

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, 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 is necessary—
(a) for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), or
(b) for the purpose of obtaining legal advice or otherwise 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 BASED ON ARTICLE 23(1): RESTRICTIONS OF RULES IN ARTICLES 13 TO 21

GDPR provisions to be restricted: "the listed GDPR provisions"

6 In this Part "the listed GDPR provisions" means the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the 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 20(1) and (2) (right to data portability);
(h) Article 21(1) (objections to processing);
(i) 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 (h).

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, (b) financial loss due to the conduct of discharged or undischarged bankrupts, or (c) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity.	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.

Description of function design	*Condition*
2. 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.
3. 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.
4. 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, or (f) the Scottish Public Services Ombudsman.

Description of function design	*Condition*
5. 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.

Regulatory functions relating to legal services, the health service and children's services

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—

(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;

(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).

Functions of certain other regulatory bodies

9 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 body described in column 1 of the Table, and

(b) is conferred on that body 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

Body on which function is conferred	*How function is conferred*
1. The Financial Ombudsman.	By or under Part 16 of the Financial Services and Markets Act 2000.
2. The investigator of complaints against the financial regulators.	By or under Part 6 of the Financial Services Act 2012.
3. A consumer protection enforcer, other than the Competition and Markets Authority.	By or under the CPC Regulation.
4. The monitoring officer of a relevant authority.	By or under the Local Government and Housing Act 1989.
5. The monitoring officer of a relevant Welsh authority.	By or under the Local Government Act 2000.
6. The Public Services Ombudsman for Wales.	By or under the Local Government Act 2000.

10 In the Table in paragraph 9—

"consumer protection enforcer" has the same meaning as "CPC enforcer" in section 213(5A) of the Enterprise Act 2002;

the "CPC Regulation" has the meaning given in section 235A of the Enterprise Act 2002;

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

11 The listed GDPR 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 appointments, judicial independence and judicial proceedings

12 (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

13 (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 3

RESTRICTION BASED ON ARTICLE 23(1): PROTECTION OF RIGHTS OF OTHERS

Protection of the rights of others: general

14 (1) Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers), and Article 5 of the 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

15 (1) For the purposes of paragraph 14(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) or (b) 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 BASED ON ARTICLE 23(1): RESTRICTIONS OF RULES IN ARTICLES 13 TO 15

GDPR provisions to be restricted: "the listed GDPR provisions"

16 In this Part "the listed GDPR provisions" means the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the 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

17 The listed GDPR provisions do not apply to personal data that consists of information in respect of which a claim to legal professional privilege or, in Scotland, confidentiality of communications, could be maintained in legal proceedings.

Self incrimination

18 (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 GDPR is not admissible against the person in proceedings for an offence under this Act.

Corporate finance

19 (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—

(d) 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;

(e) 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;

(f) 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);

(g) a person, not falling within paragraph (a), (b) or (c), who may lawfully carry on a corporate finance service without contravening the general prohibition;

(h) 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";

(i) 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

20 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

21 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

22 The listed GDPR 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 exam marks

23 (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 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 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 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 five months beginning with the date on which the question arises, or

(b) if earlier, before the end of the period of 40 days beginning with the date of 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 5

EXEMPTIONS ETC BASED ON ARTICLE 85(2) FOR REASONS OF FREEDOM OF EXPRESSION AND INFORMATION

Journalistic, academic, artistic and literary purposes

24 (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) The listed GDPR provisions do not apply to personal data that is being processed only for the special purposes to the extent that—

(a) the personal data is being processed with a view to the publication by a person of journalistic, academic, artistic or literary material,

(b) the controller reasonably believes that the publication of the material would be in the public interest, and

(c) the controller reasonably believes that the application of any one or more of the listed GDPR provisions would be incompatible with the special purposes.

(3) 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.

(4) 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 (5) that is relevant to the publication in question.

(5) The codes of practice and guidelines are—

(a) BBC Editorial Guidelines;

(b) Ofcom Broadcasting Code;

(c) IPSO Editors' Code of Practice.

(6) The Secretary of State may by regulations amend the list in sub-paragraph (5).

(7) Regulations under sub-paragraph (6) are subject to the affirmative resolution procedure.

(8) For the purposes of this paragraph, the listed GDPR provisions are the following provisions of the GDPR (which may be exempted or derogated from by virtue of Article 85(2) of the GDPR)—

(a) in Chapter II of the 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 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 20(1) and (2) (right to data portability);

(viii) Article 21(1) (objections to processing);

(c) in Chapter VII of the GDPR (co-operation and consistency)—

(i) Articles 60 to 62 (co-operation);

(ii) Articles 63 to 67 (consistency).

(9) For the purposes of this paragraph "publish", in relation to journalistic, academic, artistic or literary material, means make available to the public or a section of the public.

PART 6

DEROGATIONS ETC BASED ON ARTICLE 89 FOR RESEARCH, STATISTICS AND ARCHIVING

Research and statistics

25 (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-paragraph (3).

(2) The listed GDPR provisions are the following provisions of the GDPR (the rights in which may be derogated from by virtue of Article 89(2) of the 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 89(1) of the GDPR (as supplemented by section 18), and

(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.

Archiving in the public interest

26 (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-paragraph (3).

(2) The listed GDPR provisions are the following provisions of the GDPR (the rights in which may be derogated from by virtue of Article 89(3) of the 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 obligations);

(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 89(1) of the GDPR (as supplemented by section 18).

SCHEDULE 3

Section 14

EXEMPTIONS ETC FROM THE GDPR: HEALTH, SOCIAL WORK, EDUCATION AND CHILD ABUSE DATA

PART 1

GDPR PROVISIONS TO BE RESTRICTED: "THE LISTED GDPR PROVISIONS"

1 In this Schedule "the listed GDPR provisions" means the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the 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 20(1) and (2) (right to data portability);

(h) Article 21(1) (objections to processing);

(i) 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 (h).

PART 2

HEALTH DATA

Definitions

2 (1) In this Part of this Schedule—

"the appropriate health professional", in relation to a question as to whether the serious harm test is met with respect to data concerning health, means—

(a) the health professional who is currently or was most recently responsible for the diagnosis, care or treatment of the data subject in connection with the matters to which the data relates,

(b) where there is more than one such health professional, the health professional who is the most suitable to provide an opinion on the question, or

(c) a health professional who has the necessary experience and qualifications to provide an opinion on the question, where—

(i) there is no health professional available falling within paragraph (a) or (b), or

(ii) the controller is the Secretary of State and data is processed in connection with the exercise of the functions conferred on the Secretary of State by or under the Child Support Act 1991 and the Child

Support Act 1995, or the Secretary of State's functions in relation to social security or war pensions, or

(iii) the controller is the Department for Communities in Northern Ireland and data is processed in connection with the exercise of the functions conferred on the Department by or under the Child Support (Northern Ireland) Order 1991 (S.I. 1991/2628) and the Child Support (Northern Ireland) Order 1995 (S.I. 1995/2702);

"war pension" has the same meaning as in section 25 of the Social Security Act 1989 (establishment and functions of war pensions committees).

(2) For the purposes of this Part of this Schedule, the "serious harm test" is met with respect to data concerning health if the application of Article 15 of the GDPR to the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

Exemption from the listed GDPR provisions: data processed by a court

3 (1) The listed GDPR provisions do not apply to data concerning health if—

(a) it is processed by a court,

(b) it consists of information supplied in a report or other evidence given to the court in the course of proceedings to which rules listed in sub-paragraph (2) apply, and

(c) in accordance with those rules, the data may be withheld by the court in whole or in part from the data subject.

(2) Those rules are—

(a) the Magistrates' Courts (Children and Young Persons) Rules (Northern Ireland) 1969 (S.R. 1969 No. 221);

(b) the Magistrates' Courts (Children and Young Persons) Rules 1992 (S.I. 1992/2071 (L. 17));

(c) the Family Proceedings Rules (Northern Ireland) 1996 (S.R. 1996 No. 322);

(d) the Magistrates' Courts (Children (Northern Ireland) Order 1995) Rules (Northern Ireland) 1996 (S.R. 1996 No.323);

(e) the Act of Sederunt (Child Care and Maintenance Rules) 1997 (S.I. 1997/291 (S. 19));

(f) the Family Procedure Rules 2010 (S.I. 2010/2955 (L. 17));

(g) the Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013 (S.S.I. 2013/194).

Exemption from the listed GDPR provisions: data subject's expectations and wishes

4 (1) This paragraph applies where a request for data concerning health is made in exercise of a power conferred by an enactment or rule of law and—

(a) in relation to England and Wales or Northern Ireland, the data subject is an individual aged under 18 and the person making the request has parental responsibility for the data subject,

(b) in relation to Scotland, the data subject is an individual aged under 16 and the person making the request has parental responsibilities for the data subject, or

(c) the data subject is incapable of managing his or her own affairs and the person making the request has been appointed by a court to manage those affairs.

(2) The listed GDPR provisions do not apply to data concerning health to the extent that complying with the request would disclose information—

(a) which was provided by the data subject in the expectation that it would not be disclosed to the person making the request,

(b) which was obtained as a result of any examination or investigation to which the data subject consented in the expectation that the information would not be so disclosed, or

(c) which the data subject has expressly indicated should not be so disclosed.

(3) The exemptions under sub-paragraph (2)(a) and (b) do not apply if the data subject has expressly indicated that he or she no longer has the expectation mentioned there.

Exemption from Article 15 of the GDPR: serious harm

5 (1) Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) does not apply to data concerning health to the extent that the serious harm test is met with respect to the data.

(2) A controller who is not a health professional may not rely on sub-paragraph (1) to withhold data concerning health unless the controller has obtained an opinion from the person who appears to the controller to be the appropriate health professional to the effect that the serious harm test is met with respect to the data.

(3) An opinion does not count for the purposes of sub-paragraph (2) if—

(a) it was obtained before the beginning of the relevant period, or

(b) it was obtained during that period but it is reasonable in all the circumstances to re-consult the appropriate health professional.

(4) In this paragraph, "the relevant period" means the period of 6 months ending with the day on which the opinion would be relied on.

Restriction of Article 15 of the GDPR: prior opinion of appropriate health professional

6 (1) Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) does not permit the disclosure of data concerning health by a controller who is not a health professional unless the controller has obtained an opinion from the person who appears to the controller to be the appropriate health professional to the effect that the serious harm test is not met with respect to the data.

(2) Sub-paragraph (1) does not apply to the extent that the controller is satisfied that the data concerning health has already been seen by, or is within the knowledge of, the data subject.

(3) An opinion does not count for the purposes of sub-paragraph (1) if—

(a) it was obtained before the beginning of the relevant period, or

(b) it was obtained during that period but it is reasonable in all the circumstances to re-consult the appropriate health professional.

(4) In this paragraph, "the relevant period" means the period of 6 months ending with the day on which the opinion would be relied on.

PART 3

SOCIAL WORK DATA

Definitions

7 (1) In this Part of this Schedule—

"education data" has the meaning given by paragraph 17 of this Schedule;

"Health and Social Care trust" means a Health and Social Care trust established under the Health and Personal Social Services (Northern Ireland) Order 1991;

"Principal Reporter" means the Principal Reporter appointed under the Children's Hearings (Scotland) Act 2011, or an officer of the Scottish Children's Reporter Administration to whom there is delegated under paragraph 10(1) of Schedule 3 to that Act any function of the Principal Reporter;

"social work data" means personal data which—

(a) is data to which paragraph 8 applies, but

(b) is not education data or data concerning health.

(2) For the purposes of this Part of this Schedule, the "serious harm test" is met with respect to social work data if the application of Article 15 of the GDPR to the data would be likely to prejudice the carrying out of social work, because it would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

(3) In sub-paragraph (2), "the carrying out of social work" is to be taken to include doing any of the following—

(a) the exercise of any functions mentioned in paragraph 8(1)(a), (d), (f) to (j), (m), (p), (s), (t), (u), (v) or (w);

(b) the provision of any service mentioned in paragraph 8(1)(b), (c) or (k);

(c) the exercise of the functions of a body mentioned in paragraph 8(1)(e) or a person mentioned in paragraph 8(1)(q) or (r).

(4) In this Part of this Schedule, a reference to a local authority, in relation to data processed or formerly processed by it, includes a reference to the Council of the Isles of Scilly, in relation to data processed or formerly processed by the Council in connection with any functions mentioned in paragraph 8(1)(a)(ii) which are or have been conferred on the Council by an enactment.

8 (1) This paragraph applies to personal data falling within any of the following descriptions—

(a) data processed by a local authority—

(i) in connection with its social services functions within the meaning of the Local Authority Social Services Act 1970 or any functions exercised by local authorities under the Social Work (Scotland) Act 1968 or referred to in section 5(1B) of that Act, or

(ii) in the exercise of other functions but obtained or consisting of information obtained in connection with any of the functions mentioned in sub-paragraph (i);

(b) data processed by the Regional Health and Social Care Board—

(i) in connection with the provision of social care within the meaning of the Health and Personal Social Services (Northern Ireland) Order 1972, or

(ii) in the exercise of other functions but obtained or consisting of information obtained in connection with the provision of that care;

(c) data processed by a Health and Social Care trust—

(i) in connection with the provision of social care within the meaning of the Health and Personal Social Services (Northern Ireland) Order 1972 on behalf of the Regional Health and Social Care Board by virtue of an authorisation made under Article 3(1) of the Health and Personal Social Services (Northern Ireland) Order 1994, or

(ii) in the exercise of other functions but obtained or consisting of information obtained in connection with the provision of that care;

(d) data processed by a council in the exercise of its functions under Part 2 of Schedule 9 to the Health and Social Services and Social Security Adjudications Act 1983;

(e) data processed by—

(i) a probation trust established under section 5 of the Offender Management Act 2007, or

(ii) the Probation Board for Northern Ireland established by the Probation Board (Northern Ireland) Order 1982;

(f) data processed by a local authority in the exercise of its functions under section 36 of the Children Act 1989 or Chapter 2 of Part 6 of the Education Act 1996, so far as those functions relate to ensuring that children of compulsory school age (within the meaning of section 8 of the Education Act 1996) receive suitable education whether by attendance at school or otherwise;

(g) data processed by the Education Authority in the exercise of its functions under Article 55 of the Children (Northern Ireland) Order 1995 or Article 45 of, and Schedule 13 to, the Education and Libraries (Northern Ireland) Order 1986, so far as those functions relate to ensuring that children of compulsory school age (within the meaning of Article 46 of the Education and Libraries (Northern Ireland) Order 1986) receive efficient full-time education suitable to their age, ability and aptitude and to any special educational needs they may have, either by regular attendance at school or otherwise;

(h) data processed by an education authority in the exercise of its functions under sections 35 to 42 of the Education (Scotland) Act 1980 so far as those functions relate to ensuring that children of school age (within the meaning of section 31 of the Education (Scotland) Act 1980) receive efficient education suitable to their age, ability and aptitude, whether by attendance at school or otherwise;

(i) data relating to persons detained in a hospital at which high security psychiatric services are provided under section 4 of the National Health Service Act 2006 and processed by a Special Health Authority

established under section 28 of that Act in the exercise of any functions similar to any social services functions of a local authority;

(j) data relating to persons detained in special accommodation provided under Article 110 of the Mental Health (Northern Ireland) Order 1986 and processed by a Health and Social Care trust in the exercise of any functions similar to any social services functions of a local authority;

(k) data which—

(i) is processed by the National Society for the Prevention of Cruelty to Children, or by any other voluntary organisation or other body designated under this paragraph by the Secretary of State or the Department of Health in Northern Ireland, and

(ii) appears to the Secretary of State or the Department, as the case may be, to be processed for the purposes of the provision of any service similar to a service provided in the exercise of any functions specified in paragraph (a), (b), (c) or (d);

(l) data processed by a body mentioned in sub-paragraph (2)—

(i) which was obtained, or consists of information which was obtained, from an authority or body mentioned in any of paragraphs (a) to (k) or from a government department, and

(ii) in the case of data obtained, or consisting of information obtained, from an authority or body mentioned in any of paragraphs (a) to (k), fell within any of those paragraphs while processed by the authority or body;

(m) data processed by a National Health Service trust first established under section 25 of the National Health Service Act 2006, section 18 of the National Health Service (Wales) Act 2006 or section 5 of the National Health Service and Community Care Act 1990 in the exercise of any functions similar to any social services functions of a local authority;

(n) data processed by an NHS foundation trust in the exercise of any functions similar to any social services functions of a local authority;

(o) data processed by a government department—

(i) which was obtained, or consists of information which was obtained, from an authority or body mentioned in any of paragraphs (a) to (n), and

(ii) which fell within any of those paragraphs while processed by that authority or body;

(p) data processed for the purposes of the functions of the Secretary of State pursuant to section 82(5) of the Children Act 1989;

(q) data processed by—

(i) a children's guardian appointed under Part 16 of the Family Procedure Rules 2010 (S.I. 2010/2955),

(ii) a guardian ad litem appointed under Article 60 of the Children (Northern Ireland) Order 1995 (S.I. 1995/755) or Article 66 of the Adoption (Northern Ireland) Order 1987 (S.I. 1997/2203), or

(iii) a safeguarder appointed under section 30(2) or 31(3) of the Children's Hearings (Scotland) Act 2011 (asp 1);

(r) data processed by the Principal Reporter;

(s) data processed by an officer of the Children and Family Court Advisory and Support Service for the purpose of the officer's functions under section 7 of the Children Act 1989 or Part 16 of the Family Procedure Rules 2010;

(t) data processed by the Welsh family proceedings officer for the purposes of the functions under section 7 of the Children Act 1989 or Part 16 of the Family Procedure Rules 2010;

(u) data processed by an officer of the service appointed as guardian ad litem under Part 16 of the Family Procedure Rules 2010;

(v) data processed by the Children and Family Court Advisory and Support Service for the purpose of its functions under section 12(1) and (2) and section 13(1), (2) and (4) of the Criminal Justice and Court Services Act 2000;

(w) data processed by the Welsh Ministers for the purposes of their functions under section 35(1) and (2) and section 36(1), (2), (4), (5) and (6) of the Children Act 2004;

(x) data processed for the purposes of the functions of the appropriate Minister pursuant to section 12 of the Adoption and Children Act 2002 (independent review of determinations).

(2) The bodies referred to in sub-paragraph (1)(l) are—

(a) a National Health Service trust first established under section 25 of the National Health Service Act 2006 or section 18 of the National Health Service (Wales) Act 2006;

(b) a National Health Service trust first established under section 5 of the National Health Service and Community Care Act 1990;

(c) an NHS foundation trust;

(d) a clinical commissioning group established under section 14D of the National Health Service Act 2006;

(e) the National Health Service Commissioning Board;

(f) a Local Health Board established under section 11 of the National Health Service (Wales) Act 2006;

(g) a Health Board established under section 2 of the National Health Service (Scotland) Act 1978.

Exemption from the listed GDPR provisions: data processed by a court

9 (1) The listed GDPR provisions do not apply to data that is not education data or data concerning health if—

(a) it is processed by a court,

(b) it consists of information supplied in a report or other evidence given to the court in the course of proceedings to which rules listed in sub-paragraph (2) apply, and

(c) in accordance with any of those rules, the data may be withheld by the court in whole or in part from the data subject.

(2) Those rules are—

(a) the Magistrates' Courts (Children and Young Persons) Rules (Northern Ireland) 1969 (S.R. 1969 No. 221);

(b) the Magistrates' Courts (Children and Young Persons) Rules 1992 (S.I. 1992/2071 (L. 17));

(c) the Family Proceedings Rules (Northern Ireland) 1996 (S.R. 1996 No. 322);

(d) the Magistrates' Courts (Children (Northern Ireland) Order 1995) Rules (Northern Ireland) 1996 (S.R. 1996 No.323);
(e) the Act of Sederunt (Child Care and Maintenance Rules) 1997 (S.I. 1997/291 (S. 19));
(f) the Family Procedure Rules 2010 (S.I. 2010/2955 (L. 17));
(g) the Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013 (S.S.I. 2013/194).

Exemption from the listed GDPR provisions: data subject's expectations and wishes

10 (1) This paragraph applies where a request for social work data is made in exercise of a power conferred by an enactment or rule of law and—
(a) in relation to England and Wales or Northern Ireland, the data subject is an individual aged under 18 and the person making the request has parental responsibility for the data subject,
(b) in relation to Scotland, the data subject is an individual aged under 16 and the person making the request has parental responsibilities for the data subject, or
(c) the data subject is incapable of managing his or her own affairs and the person making the request has been appointed by a court to manage those affairs.

(2) The listed GDPR provisions do not apply to social work data to the extent that complying with the request would disclose information—
(a) which was provided by the data subject in the expectation that it would not be disclosed to the person making the request,
(b) which was obtained as a result of any examination or investigation to which the data subject consented in the expectation that the information would not be so disclosed, or
(c) which the data subject has expressly indicated should not be so disclosed.

(3) The exemptions under sub-paragraph (2)(a) and (b) do not apply if the data subject has expressly indicated that he or she no longer has the expectation mentioned there.

Exemption from Article 15 of the GDPR: serious harm

11 Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) does not apply to social work data to the extent that the serious harm test is met with respect to the data.

Restriction of Article 15 of the GDPR: prior opinion of Principal Reporter

12 (1) This paragraph applies where—
(a) a question arises as to whether a controller who is a social work authority is obliged Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) to disclose social work data, and
(b) the data—
(i) originated from or was supplied by the Principal Reporter acting in pursuance of the Principal Reporter's statutory duties, and

(ii) is not data which the data subject is entitled to receive from the Principal Reporter.

(2) The controller must inform the Principal Reporter of the fact that the question has arisen before the end of the period of 14 days beginning with the day on which the question arises.

(3) Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) does not permit the controller to disclose the data to the data subject unless the Principal Reporter has informed the controller that, in the opinion of the Principal Reporter, the serious harm test is not met with respect to the data.

(4) In this paragraph "social work authority" means a local authority for the purposes of the Social Work (Scotland) Act 1968.

PART 4

EDUCATION DATA

Educational records

13 In this Part of this Schedule "educational record" means a record to which paragraph 14, 15 or 16 applies.

14 (1) This paragraph applies to a record of information which—

(a) is processed by or on behalf of the governing body of, or a teacher at, a school in England and Wales specified in sub-paragraph (3),

(b) relates to an individual who is or has been a pupil at the school, and

(c) originated from, or was supplied by or on behalf of, any of the persons specified in sub-paragraph (4).

(2) But this paragraph does not apply to information which is processed by a teacher solely for the teacher's own use.

(3) The schools referred to in sub-paragraph (1)(a) are—

(a) a school maintained by a local authority;

(b) a special school (as defined in section 337 of the Education Act 1996) that is not maintained by a local authority.

(4) The persons referred to in sub-paragraph (1)(c) are—

(a) an employee of the local authority which maintains the school;

(b) in the case of—

(i) a voluntary aided, foundation or foundation special school (within the meaning of the School Standards and Framework Act 1998), or

(ii) a special school that is not maintained by a local authority,

a teacher or other employee at the school (including an educational psychologist engaged by the governing body under a contract for services);

(c) the pupil to whom the record relates;

(d) a parent, as defined by section 576(1) of the Education Act 1996, of that pupil.

(5) In this paragraph "local authority" has the meaning given by section 579(1) of the Education Act 1996.

15 (1) This paragraph applies to a record of information which is processed—
(a) by an education authority in Scotland, and
(b) for the purpose of the relevant function of the authority.

(2) But this paragraph does not apply to information which is processed by a teacher solely for the teacher's own use.

(3) For the purposes of this paragraph, information processed by an education authority is processed for the purpose of the relevant function of the authority if the processing relates to the discharge of that function in respect of a person—
(a) who is or has been a pupil in a school provided by the authority, or
(b) who receives, or has received, further education provided by the authority.

(4) In this paragraph "the relevant function" means, in relation to each education authority, its function under section 1 of the Education (Scotland) Act 1980 and section 7(1) of the Self-Governing Schools etc. (Scotland) Act 1989.

16 (1) This paragraph applies to a record of information which—
(a) is processed by or on behalf of the Board of Governors of, or a teacher at, a grant-aided school in Northern Ireland,
(b) relates to an individual who is or has been a pupil at the school, and
(c) originated from, or was supplied by or on behalf of, any of the persons specified in sub-paragraph (4).

(2) But this paragraph does not apply to information which is processed by a teacher solely for the teacher's own use.

(3) In this paragraph "grant-aided school" has the same meaning as in the Education and Libraries (Northern Ireland) Order 1986 (S.I. 1986/594 (N.I. 3).

(4) The persons referred to in sub-paragraph (1)(c) are—
(a) a teacher at the school;
(b) an employee of the Education Authority, other than a teacher at the school;
(c) the pupil to whom the record relates;
(d) a parent, as defined by Article 2(2) of the Education and Libraries (Northern Ireland) Order 1986.

Other definitions

17 (1) In this Part of this Schedule—
"education authority" and "further education" have the same meaning as in the Education (Scotland) Act 1980;
"education data" means personal data consisting of information which—
(a) constitutes an educational record, but
(b) is not data concerning health;
"Principal Reporter" means the Principal Reporter appointed under the Children's Hearings (Scotland) Act 2011, or an officer of the Scottish Children's Reporter Administration to whom there is delegated

under paragraph 10(1) of Schedule 3 to that Act any function of the Principal Reporter;

"pupil" means—

(a) in relation to a school in England and Wales, a registered pupil within the meaning of the Education Act 1996,

(b) in relation to a school in Scotland, a pupil within the meaning of the Education (Scotland) Act 1980, and

(c) in relation to a school in Northern Ireland, a registered pupil within the meaning of the Education and Libraries (Northern Ireland) Order 1986;

"school"—

(a) in relation to England and Wales, has the same meaning as in the Education Act 1996,

(b) in relation to Scotland, has the same meaning as in the Education (Scotland) Act 1980, and

(c) in relation to Northern Ireland, has the same meaning as in the Education and Libraries (Northern Ireland) Order 1986;

"teacher" includes—

(a) in Great Britain, head teacher, and

(b) in Northern Ireland, the principal of a school.

(2) For the purposes of this Part of this Schedule, the "serious harm test" is met with respect to education data if the application of Article 15 of the GDPR to the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

Exemption from the listed GDPR provisions: data processed by a court

18 (1) The listed GDPR provisions do not apply to education data if—

(a) it is processed by a court,

(b) it consists of information supplied in a report or other evidence given to the court in the course of proceedings to which rules listed in sub-paragraph (2) apply, and

(c) in accordance with those rules, the data may be withheld by the court in whole or in part from the data subject.

(2) Those rules are—

(a) the Magistrates' Courts (Children and Young Persons) Rules (Northern Ireland) 1969 (S.R. 1969 No. 221);

(b) the Magistrates' Courts (Children and Young Persons) Rules 1992 (S.I. 1992/2071 (L. 17));

(c) the Family Proceedings Rules (Northern Ireland) 1996 (S.R. 1996 No. 322);

(d) the Magistrates' Courts (Children (Northern Ireland) Order 1995) Rules (Northern Ireland) 1996 (S.R. 1996 No.323);

(e) the Act of Sederunt (Child Care and Maintenance Rules) 1997 (S.I. 1997/291 (S. 19));

(f) the Family Procedure Rules 2010 (S.I. 2010/2955 (L. 17));

(g) the Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013 (S.S.I. 2013/194).

Exemption from Article 15 of the GDPR: serious harm

19 Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) does not apply to education data to the extent that the serious harm test is met with respect to the data.

Restriction of Article 15 of the GDPR: prior opinion of Principal Reporter

20 (1) This paragraph applies where—

(a) a question arises as to whether a controller who is an education authority is obliged by Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) to disclose education data, and

(b) the controller believes that the data—

(i) originated from or was supplied by or on behalf of the Principal Reporter acting in pursuance of the Principal Reporter's statutory duties, and

(ii) is not data which the data subject is entitled to receive from the Principal Reporter.

(2) The controller must inform the Principal Reporter of the fact that the question has arisen before the end of the period of 14 days beginning with the day on which the question arises.

(3) Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) does not permit the controller to disclose the data to the data subject unless the Principal Reporter has informed the controller that, in the opinion of the Principal Reporter, the serious harm test is not met with respect to the data.

PART 5

CHILD ABUSE DATA

Exemption from Article 15 of the GDPR: child abuse data

21 (1) This paragraph applies where a request for child abuse data is made in exercise of a power conferred by an enactment or rule of law and—

(a) the data subject is an individual aged under 18 and the person making the request has parental responsibility for the data subject, or

(b) the data subject is incapable of managing his or her own affairs and the person making the request has been appointed by a court to manage those affairs.

(2) Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) does not apply to child abuse data to the extent that the application of that provision would not be in the best interests of the data subject.

(3) "Child abuse data" is personal data consisting of information as to whether the data subject is or has been the subject of, or may be at risk of, child abuse.

(4) For this purpose, "child abuse" includes physical injury (other than accidental injury) to, and physical and emotional neglect, ill-treatment and sexual abuse of, an individual aged under 18.

(5) This paragraph does not apply in relation to Scotland.

SCHEDULE 4

Section 14

EXEMPTIONS ETC FROM THE GDPR: DISCLOSURE PROHIBITED OR RESTRICTED BY AN ENACTMENT

GDPR provisions to be restricted: "the listed GDPR provisions"

1 In this Schedule "the listed GDPR provisions" means the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the GDPR)—

(a) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(b) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in Article 15(1) to (3).

Human fertilisation and embryology information

2 The listed GDPR provisions do not apply to personal data consisting of information the disclosure of which is prohibited or restricted by any of sections 31, 31ZA to 31ZE and 33A to 33D of the Human Fertilisation and Embryology Act 1990.

Adoption records and reports

3 (1) The listed GDPR provisions do not apply to personal data consisting of information the disclosure of which is prohibited or restricted by an enactment listed in sub-paragraph (2), (3) or (4).

(2) The enactments extending to England and Wales are—

(a) regulation 14 of the Adoption Agencies Regulations 1983 (S.I. 1983/1964);

(b) regulation 41 of the Adoption Agencies Regulations 2005 (S.I. 2005/389);

(c) regulation 42 of the Adoption Agencies (Wales) Regulations 2005 (S.I. 2005/1313) (W.95);

(d) rules 5, 6, 9, 17, 18, 21, 22 and 53 of the Adoption Rules 1984 (S.I. 1984/265);

(e) rules 24, 29, 30, 65, 72, 73, 77, 78 and 83 of the Family Procedure (Adoption) Rules 2005 (S.I. 2005/2795) (L.22);

(f) in the Family Procedure Rules 2010 (S.I. 2010/2955) (L.17): rules 14.6, 14.11, 14.12, 14.13, 14.14, 14.24, 16.20 (so far as it applies to a children's guardian appointed in proceedings to which Part 14 of those Rules applies), 16.32 and 16.33 (so far as it applies to a children and family reporter in proceedings to which Part 14 of those Rules applies).

(3) The enactments extending to Scotland are—

(a) regulation 23 of the Adoption Agencies (Scotland) Regulations 1996 (S.I. 1996/3266) (S.254);

(b) rule 67.3 of the Act of Sederunt (Rules of the Court of Session 1994) 1994 (S.I. 1994/1443) (S.69);

(c) rules 10.3, 17.2, 21, 25, 39, 43.3, 46.2, 47 of the Act of Sederunt (Sheriff Court Rules Amendment) (Adoption and Children (Scotland) Act 2007) 2009 (S.S.I. 2009/284).

(d) regulation 28(1) of Adoption Support Services and Allowances (Scotland) Regulations 2009 (S.S.I. 2009/152);

(e) sections 53 and 55 of the Adoption and Children (Scotland) Act 2007 (asp 4);

(f) regulation 28 of the Adoption Agencies (Scotland) Regulations 2009 (S.S.I. 2009/154);

(g) regulation 3 of the Adoption (Disclosure of Information and Medical Information about Natural Parents) (Scotland) Regulations 2009 (S.S.I. 2009/268).

(4) The enactments extending to Northern Ireland are—

(a) Articles 50 and 54 of the Adoption (Northern Ireland) Order 1987 (S.I. 1987/2203) (N.I.22);

(b) rule 53 of Order 84 of the Rules of the Court of Judicature (Northern Ireland) 1980 (S.R. 1980/346);

(c) rules 4A.4(5), 4A.5(1), 4A.6(6) and 4A.22(5), 4C.7 of Part IVA of the Family Proceedings Rules (Northern Ireland) 1996 (S.R. 1996/322).

Statements of special educational needs

4 (1) The listed GDPR provisions do not apply to personal data consisting of information the disclosure of which is prohibited or restricted by an enactment listed in sub-paragraph (2).

(2) The enactments are—

(a) regulation 17 of the Special Educational Needs and Disability Regulations 2014 (S.I. 2014/1530);

(b) regulation 10 of the Additional Support for Learning (Co-ordinated Support Plan) (Scotland) Amendment Regulations 2005 (S.I. 2005/518);

(c) regulation 22 of the Education (Special Educational Needs) Regulations (Northern Ireland) 2005 (S.I. 2005/384).

Parental order records and reports

5 (1) The listed GDPR provisions do not apply to personal data consisting of information the disclosure of which is prohibited or restricted by an enactment listed in sub-paragraph (2), (3) or (4).

(2) The enactments extending to England and Wales are—

(a) sections 60, 77, 78 and 79 of the Adoption and Children Act 2002, as applied with modifications by regulation 2 of and Schedule 1 to the Human Fertilisation and Embryology (Parental Orders) Regulations 2010 (S.I. 2010/985) in relation to parental orders made under—

(i) section 30 of the Human Fertilisation and Embryology Act 1990, or

(ii) section 54 of the Human Fertilisation and Embryology Act 2008;

(b) rules made under section 144 of the Magistrates' Courts Act 1980 by virtue of section 141(1) of the Adoption and Children Act 2002, as applied with modifications by regulation 2 of and Schedule 1 to the Human Fertilisation and Embryology (Parental Orders) Regulations 2010, so far as the rules relate to—

(i) the appointment and duties of the parental order reporter, and

(ii) the keeping of registers and the custody, inspection and disclosure of documents and information relating to parental order proceedings or related proceedings;

(c) rules made under section 75 of the Courts Act 2003 by virtue of section 141(1) of the Adoption and Children Act 2002, as applied with modifications by regulation 2 of Schedule 1 to the Human Fertilisation and Embryology (Parental Orders) Regulations 2010, so far as the rules relate to—

(i) the appointment and duties of the parental order reporter, and

(ii) the keeping of registers and the custody, inspection and disclosure of documents and information relating to parental order proceedings or related proceedings.

(3) The enactments extending to Scotland are—

(a) sections 53 and 55 of the Adoption and Children (Scotland) Act 2007, as applied with modifications by regulation 4 of and Schedule 3 to the Human Fertilisation and Embryology (Parental Orders) Regulations 2010 in relation to parental orders made under—

(i) section 30 of the Human Fertilisation and Embryology Act 1990, or

(ii) section 54 of the Human Fertilisation and Embryology Act 2008;

(b) rules 2.47 and 2.59 of the Act of Sederunt (Child Care and Maintenance Rules) 1997 (S.I. 1997/291), or rules with equivalent effect replacing those rules;

(c) rules 21 and 25 of the Sheriff Court Adoption Rules 2009.

(4) The enactments extending to Northern Ireland are—

(a) Articles 50 and 54 of the Adoption (Northern Ireland) Order 1987, as applied with modifications by regulation 3 of and Schedule 2 to the Human Fertilisation and Embryology (Parental Orders) Regulations 2010 in respect of parental orders made under—

(i) section 30 of the Human Fertilisation and Embryology Act 1990, or

(ii) section 54 of the Human Fertilisation and Embryology Act 2008;

(b) rules 4, 5 and 16 of Order 84A of the Rules of the Court of Judicature (Northern Ireland) 1980, or rules with equivalent effect replacing those rules;

(c) rules 3, 4 and 15 of Order 50A of the County Court Rules (Northern Ireland) 1981 (S.I. 1981/225), or rules with equivalent effect replacing those rules.

Information provided by Principal Reporter for children's hearing

6 The listed GDPR provisions do not apply to personal data consisting of information the disclosure of which is prohibited or restricted by any of the following enactments—

(a) section 178 of the Children's Hearings (Scotland) Act 2011 (asp 1);

(b) the Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013 (S.S.I. 2013/194).

SCHEDULE 5

Section 16

ACCREDITATION OF CERTIFICATION PROVIDERS: REVIEWS AND APPEALS

Introduction

1 (1) This Schedule applies where—

(a) a person ("the applicant") applies to an accreditation authority for accreditation as a certification provider, and

(b) is dissatisfied with the decision on that application.

(2) In this Schedule—

"accreditation authority" means—

(a) the Commissioner, or

(b) the national accreditation body;

"certification provider" and "national accreditation body" have the same meaning as in section 16.

Review

2 (1) The applicant may ask the accreditation authority to review the decision.

(2) The request must be made in writing before the end of the period of 28 days beginning with the day on which the person receives written notice of the accreditation authority's decision.

(3) The request must specify—

(a) the decision to be reviewed, and

(b) the reasons for asking for the review.

(4) The request may be accompanied by additional documents which the applicant wants the accreditation authority to take into account for the purposes of the review.

(5) If the applicant makes a request in accordance with sub-paragraphs (1) to (4), the accreditation authority must—

(a) review the decision, and

(b) inform the applicant of the outcome of the review in writing before the end of the period of 28 days beginning with the day on which the request for a review is received.

Right to appeal

3 (1) If the applicant is dissatisfied with the decision on the review under paragraph 2, the applicant may ask the accreditation authority to refer the decision to an appeal panel constituted in accordance with paragraph 4.

(2) The request must be made in writing before the end of the period of 3 months beginning with the day on which the person receives written notice of the decision on the review.

(3) A request must specify—

(a) the decision to be referred to the appeal panel, and

(b) the reasons for asking for it to be referred.

(4) The request may be accompanied by additional documents which the applicant wants the appeal panel to take into account.

(5) The applicant may discontinue an appeal at any time by giving notice in writing to the accreditation authority.

Appeal panel

4 (1) If the applicant makes a request in accordance with paragraph 3, an appeal panel must be established in accordance with this paragraph.

(2) An appeal panel must consist of a chair and at least two other members.

(3) Where the request relates to a decision of the Commissioner—

(a) the Secretary of State may appoint one person to be a member of the appeal panel other than the chair, and

(b) subject to paragraph (a), the Commissioner must appoint the members of the appeal panel.

(4) Where the request relates to a decision of the national accreditation body—

(a) the Secretary of State—

(i) may appoint one person to be a member of the appeal panel other than the chair, or

(ii) may direct the Commissioner to appoint one person to be a member of the appeal panel other than the chair, and

(b) subject to paragraph (a), the chair of the national accreditation body must appoint the members of the appeal panel.

(5) A person may not be a member of an appeal panel if the person—

(a) has a commercial interest in the decision referred to the panel,

(b) has had any prior involvement in any matters relating to the decision, or

(c) is an employee or officer of the accreditation authority.

(6) The Commissioner may not be a member of an appeal panel to which a decision of the Commissioner is referred.

(7) The applicant may object to all or any of the members of the appeal panel.

(8) If the applicant objects to a member of the appeal panel under sub-paragraph (7), the person who appointed that member must appoint a replacement.

(9) The applicant may not object to a member of the appeal panel appointed under sub-paragraph (7).

Hearing

5 (1) If the appeal panel considers it necessary, a hearing must be held at which both the applicant and the accreditation authority may be represented.

(2) Any additional documents which the applicant or the accreditation authority want the appeal panel to take into account must be submitted to the chair of the appeal panel at least 5 working days before the hearing.

(3) The appeal panel may allow experts and witnesses to give evidence at a hearing.

Decision following referral to appeal panel

6 (1) The appeal panel must, before the end of the period of 28 days beginning with the day on which the appeal panel is established in accordance with paragraph 4—

(a) make a reasoned recommendation in writing to the accreditation authority, and

(b) give a copy of the recommendation to the applicant.

(2) For the purposes of sub-paragraph (1), where there is an objection under paragraph 4(7), an appeal panel is not to be taken to be established in accordance with paragraph 4 until the replacement member is appointed (or, if there is more than one objection, until the last replacement member is appointed).

(3) The accreditation authority must, before the end of the period of 3 working days beginning with the day on which the authority receives the recommendation—

(a) make a reasoned final decision in writing, and

(b) give a copy of the decision to the applicant.

(4) Where the accreditation authority is the national accreditation body, the recommendation must be given to, and the final decision must be made by, the chief executive of that body.

(5) In this paragraph, "working day" means any day other than—

(a) Saturday or Sunday,

(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.

SCHEDULE 6

Section 20

THE APPLIED GDPR AND THE APPLIED CHAPTER 2

PART 1

MODIFICATIONS TO THE GDPR

Introductory

1 In its application by virtue of section 20(1), the GDPR has effect as if it were modified as follows.

References to the GDPR and its provisions

2 References to "this Regulation" and to provisions of the GDPR have effect as references to the applied GDPR and to the provisions of the applied GDPR, except—

(a) in the provisions modified by paragraphs 9(f), 15(b), 16(a)(ii), 35, 36(a) and (e)(ii), 38(a), 46 and 47;

(b) in Article 61(2) inserted by paragraph 49.

References to Union law and Member State law

3 (1) References to "Union law", "Member State law", "the law of a Member State" and "Union or Member State law" have effect as references to domestic law.

(2) Sub-paragraph (1) is subject to the specific modifications made in this Part of this Schedule.

(3) For the purposes of this Part of this Schedule, "domestic law" means the law of the United Kingdom, or of a part of the United Kingdom, and includes law in the form of an enactment, an instrument made under Her Majesty's prerogative or a rule of law.

References to the Union and to Member States

4 (1) References to "the Union", "a Member State" and "Member States" have effect as references to the United Kingdom.

(2) Sub-paragraph (1) is subject to the specific modifications made in this Part of this Schedule.

References to supervisory authorities

5 (1) References to a "supervisory authority", a "competent supervisory authority" or "supervisory authorities", however expressed, have effect as references to the Commissioner.

(2) Sub-paragraph (1) does not apply to the references in—

(a) Article 4(21) as modified by paragraph 9(f);

(b) Article 57(1)(h);

(c) Article 61(1) inserted by paragraph 49.

(3) Sub-paragraph (1) is also subject to the specific modifications made in this Part of this Schedule.

References to the national parliament

6 References to "the national Parliament" have effect as references to both Houses of Parliament.

Chapter I of the GDPR (general provisions)

7 For Article 2 (material scope) substitute—

"2 This Regulation applies to the processing of personal data to which Chapter 3 of Part 2 of the 2017 Act applies (see section 19 of that Act)."

8 For Article 3 substitute—

"*Article 3*

Territorial application

Section 186 of the 2017 Act has effect for the purposes of this Regulation as it has effect for the purposes of that Act but as if it were modified as follows—

(a) references to "this Act" have effect as references to this Regulation;
(b) in subsection (1), omit ", subject to subsection (3)";
(c) in subsection (2), omit ", subject to subsection (4)";
(d) omit subsections (3) to (5);
(e) in subsection (7), omit "or section 57(8) or 103(3) of this Act (processor to be treated as controller in certain circumstances)."

9 In Article 4 (definitions)—

(a) in paragraph (7) (meaning of "controller"), for "; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" substitute ", subject to section 5 of the 2017 Act (meaning of "controller")";
(b) after paragraph (7), insert—

"(7A) "the 2017 Act" means the Data Protection Act 2017 as applied by section 20 of that Act and further modified by section 2 of that Act."

(c) omit paragraph (16) (meaning of "main establishment");
(d) omit paragraph (17) (meaning of "representative");
(e) in paragraph (20) (meaning of "binding corporate rules"), for "on the territory of a Member State" substitute "in the United Kingdom";
(f) in paragraph (21) (meaning of "supervisory authority"), after "a Member State" insert "(other than the United Kingdom);
(g) after paragraph (21) insert—

"(21A) "the Commissioner" means the Information Commissioner (see section 112 of the 2017 Act);";

(h) omit paragraph (22) (meaning of "supervisory authority concerned";
(i) omit paragraph (23) (meaning of "cross-border processing");
(j) omit paragraph (24) (meaning of "relevant and reasoned objection");

(k) after paragraph (26), insert—

"(27) "the GDPR" has the meaning given in section 2(10) of the 2017 Act."

Chapter II of the GDPR (principles)

10 In Article 6 (lawfulness of processing)—

(a) omit paragraph 2;

(b) in paragraph 3, for the first subparagraph, substitute—

"In addition to the provision made in section 14 of and Part 1 of Schedule 2 to the 2017 Act, a legal basis for the processing referred to in point (c) and (e) of paragraph 1 may be laid down by the Secretary of State in regulations (see section 15 of the 2017 Act)."

(c) in paragraph 3, in the second subparagraph, for "The Union or Member State law shall" substitute "The regulations must"

11 In Article 8 (conditions applicable to child's consent in relation to information society services)—

(a) in paragraph 1, for the second subparagraph, substitute—

"This paragraph is subject to section 8 of the 2017 Act.";

(b) in paragraph 3, for "general contract law of Member States" substitute "the general law of contract as it operates in domestic law".

12 In Article 9 (processing of special categories of personal data)—

(a) in paragraph 2(a), omit ", except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject";

(b) in paragraph 2(b), for "Union or Member State law" substitute "domestic law (see section 9 of the 2017 Act)";

(c) in paragraph 2, for point (g), substitute—

"(g) processing is necessary for reasons of substantial public interest and is authorised by domestic law (see section 9 of the 2017 Act);";

(d) in paragraph 2(h), for "Union or Member State law" substitute "domestic law (see section 9)";

(e) in paragraph 2(i), for "Union or Member State law" insert "domestic law (see section 9 of the 2017 Act);";

(f) in paragraph 2, for point (j) substitute—

"(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 18 of the 2017 Act) and is authorised by domestic law (see section 9 of that Act).";

(g) in paragraph 3, for "national competent bodies", in both places, substitute "a national competent body of the United Kingdom";

(h) omit paragraph 4.

13 In Article 10 (processing of personal data relating to criminal convictions and offences), in the first sentence, for "Union or Member State law

providing for appropriate safeguards for the rights and freedoms of data subjects", substitute "domestic law (see section 9 of the 2017 Act)".

Section 1 of Chapter III of the GDPR (rights of the data subject: transparency and modalities)

14 In Article 12 (transparent information etc for the exercise of the rights of the data subject), omit paragraph 8.

Section 2 of Chapter III of the GDPR (rights of the data subject: information and access to personal data)

15 In Article 13 (personal data collected from data subject: information to be provided), in paragraph 1—

(a) in point (a), omit "and, where applicable, of the controller's representative";

(b) in point (f), after "the Commission" insert "pursuant to Article 45(3) of the GDPR".

16 In Article 14 (personal data collected other than from data subject: information to be provided)—

(a) in paragraph 1—

(i) in point (a), omit "and, where applicable, of the controller's representative";

(ii) in point (f), after "the Commission" insert "pursuant to Article 45(3) of the GDPR";

(b) in paragraph 5(c), for "Union or Member State law to which the controller is subject" substitute "a rule of domestic law".

Section 3 of Chapter IV of the GDPR (rights of the data subject: rectification and erasure)

17 In Article 17 (right to erasure ('right to be forgotten'))—

(a) in paragraph 1(e), for "in Union or Member State law to which the controller is subject" substitute "under domestic law";

(b) in paragraph 3(b), for "by Union or Member State law to which the controller is subject" substitute "under domestic law".

18 In Article 18 (right to restriction of processing), in paragraph 2, for "of the Union or of a Member State" substitute "of the United Kingdom".

Section 4 of Chapter IV of the GDPR (rights of the data subject: right to object and automated individual decision-making)

19 In Article 21 (right to object), in paragraph 5, omit ", and notwithstanding Directive 2002/58/EC,".

20 In Article 22 (automated individual decision-making, including profiling), for paragraph 2(b) substitute—

"(b) is a "qualifying significant decision" for the purposes of section 13 of the 2017 Act; or".

Section 5 of Chapter III of the GDPR (rights of data the subject: restrictions)

21 In Article 23 (restrictions), in paragraph 1—

(a) for "Union or Member State law to which the data controller or processor is subject" substitute "In addition to the provision made by section 14 of and Schedules 2, 3 and 4 to the 2017 Act, the Secretary of State";

(b) in point (e), for "of the Union or of a Member State", in both places, substitute "of the United Kingdom";

(c) after point (j), insert—

"See section 15 of the 2017 Act."

Section 1 of Chapter IV of the GDPR (controller and processor: general obligations)

22 In Article 26 (joint controllers), in paragraph 1, for "Union or Member State law to which the controllers are subject" substituted "domestic law".

23 Omit Article 27 (representatives of controllers or processors not established in the Union).

24 In Article 28 (processor)—

(a) in paragraph 3, in point (a), for "Union or Member State law to which the processor is subject" substitute "domestic law";

(b) in paragraph 3, in the second subparagraph, for "other Union or Member State data protection provisions" substitute "any other rule of domestic law relating to data protection";

(c) in paragraph 6, for "paragraphs 7 and 8" substitute "paragraph 8";

(d) omit paragraph 7;

(e) in paragraph 8, omit "and in accordance with the consistency mechanism referred to in Article 63".

25 In Article 30 (records of processing activities)—

(a) in paragraph 1, in the first sentence, omit ", and where applicable, the controller's representative";

(b) in paragraph 1, in point (a), omit ", the controller's representative";

(c) in paragraph 1, in point (g), after "32(1)" insert "or section 26(3) of the 2017 Act";

(d) in paragraph 2, in the first sentence, omit "and where applicable, the processor's representative";

(e) in paragraph 2, in point (a), omit "the controller's or the processor's representative, and";

(f) in paragraph 2, in point (d), after "32(1)" insert "or section 26(3) of the 2017 Act;

(g) in paragraph 4 omit "and, where applicable, the controller's or processor's representative".

26 In Article 31 (co-operation with the supervisory authority), omit "and, where applicable, their representatives".

Section 3 of Chapter IV of the GDPR (controller and processor: data protection impact assessment and prior consultation)

27 In Article 35 (data protection impact assessment), omit paragraphs 4, 5, 6 and 10.

28 In Article 36 (prior consultation)—

(a) for paragraph 4, substitute—

"4 The Secretary of State must consult the Commissioner during the preparation of any proposal for a legislative measure which relates to processing.";

(b) omit paragraph 5.

Section 4 of Chapter IV of the GDPR (controller and processor: data protection officer)

29 In Article 37 (designation of data protection officers), omit paragraph 4.

30 In Article 39 (tasks of the data protection officer), in paragraph 1(a) and (b), for "other Union or Member State data protection provisions" substitute "other rules of domestic law relating to data protection".

Section 5 of Chapter IV of the GDPR (controller and processor: codes of conduct and certification)

31 In Article 40 (codes of conduct)—

(a) in paragraph 1, for "The Member States, the supervisory authorities, the Board and the Commission shall" substitute "The Commissioner must";

(b) omit paragraph 3;

(c) in paragraph 6, omit ", and where the code of conduct concerned does not relate to processing activities in several Member States";

(d) omit paragraphs 7 to 11.

32 In Article 41 (monitoring of approved codes of conduct), omit paragraph 3.

33 In Article 42 (certification)—

(a) in paragraph 1—

(i) for "The Member States, the supervisory authorities, the Board and the Commission" substitute "The Commissioner";

(ii) omit ", in particular at Union level,";

(b) omit paragraph 2;

(c) in paragraph 5, omit "or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal";

(d) omit paragraph 8.

34 In Article 43 (certification bodies)—

(a) in paragraph 1, in the second sentence, for "Member States shall ensure that those certification bodies are" substitute "Those certification bodies must be";

(b) in paragraph 2, in point (b), omit "or by the Board pursuant to Article 63;

(c) in paragraph 3, omit "or by the Board pursuant to Article 63";

(d) in paragraph 6, omit the second and third sentences;

(e) omit paragraphs 8 and 9.

Chapter V of the GDPR (transfers of data to third countries or international organisations)

35 In Article 45 (transfers on the basis of an adequacy decision)—

(a) in for paragraph 1, after "decided" insert "in accordance with Article 45 of the GDPR";]

(b) after paragraph 1, insert—

"1A But a transfer of personal data to a third country or international organisation must not take place under paragraph 1, if the Commission's decision in relation to the third country (including a territory or sector within it) or the international organisation—

(a) is suspended,

(b) has been amended, or

(c) has been repealed,

by the Commission under Article 45(5) of the GDPR.";

(c) omit paragraphs 2 to 8.

36 In Article 46 (transfers subject to appropriate safeguards)—

(a) in paragraph 1, for "Article 45(3)" substitute "Article 45(3) of the GDPR";

(b) in paragraph 2, omit point (c);

(c) in paragraph 2, in point (d), omit "and approved by the Commission pursuant to the examination procedure referred to in Article 93(2)";

(d) omit paragraph 4;

(e) in paragraph 5—

(i) in the first sentence, for "a Member State or supervisory authority" substitute "the Commissioner";

(ii) in the second sentence, for "this Article" substitute "Article 46 of the GDPR".

37 In Article 47 (binding corporate rules)—

(a) in paragraph 1, in the first sentence, omit "in accordance with the consistency mechanism set out in Article 63";

(b) in paragraph 2, in point (e), for "the competent courts of the Member States" substitute "a court";

(c) in paragraph 2, in point (f), for "on the territory of a Member State" substitute "in the United Kingdom";

(d) omit paragraph 3.

38 In Article 49 (derogations for specific situations)—

(a) in paragraph 1, in the first sentence,—

(i) for "Article 45(3)" substitute "Article 45(3) of the GDPR";

(ii) for "Article 46" substitute "Article 46 of this Regulation";

(b) in paragraph 4, for "in Union law or in the law of the Member State to which the controller is subject" substitute "domestic law (see section 17 of the 2017 Act)";

(c) for paragraph 5, substitute—

"5 Paragraph 1 is subject to any regulations made under section 17(2) of the 2017 Act."

39 In Article 50 (international co-operation for the protection of personal data) omit "the Commission and".

Section 1 of Chapter VI of the GDPR (independent supervisory authorities)

40 In Article 51 (supervisory authority)—

(a) in paragraph 1—

(i) for "Each Member State shall provide for one or more independent public authorities to be" substitute "The Commissioner is";

(ii) omit "and to facilitate the free flow of personal data within the Union ('supervisory authority')";

(b) omit paragraphs 2 to 4.

41 In Article 52 (independence)

(a) in paragraph 2—

(i) for "The member or members of each supervisory authority" substitute "The Commissioner";

(ii) for "their", in both places, substitute "the Commissioner's";

(b) in paragraph 3—

(i) for "Member or members of each supervisory authority" substitute "The Commissioner";

(ii) for "their", in both places, substitute "the Commissioner's";

(c) omit paragraphs 4 to 6.

42 Omit Article 53 (general conditions for the members of the supervisory authority).

43 Omit Article 54 (rules on the establishment of the supervisory authority).

Section 2 of Chapter VI of the GDPR (independent supervisory authorities: competence, tasks and powers)

44 In Article 55 (competence)—

(a) in paragraph 1, omit "on the territory of its own Member State";

(b) omit paragraph 2.

45 Omit Article 56 (competence of the lead supervisory authority).

46 In Article 57 (tasks)—

(a) in paragraph 1, in the first sentence, for "each supervisory authority on its territory shall" substitute "the Commissioner is to",

(b) in paragraph 1, in point (e), omit "and, if appropriate, cooperate with the supervisory authorities in other Member States to that end";

(c) in paragraph 1, in point (f), omit "or coordination with another supervisory authority";

(d) in paragraph 1, omit points (g), (k) and (t);

(e) after paragraph 1, insert—

"1A In this Article and Article 58, references to "this Regulation" have effect as references to this Regulation and section 26(3) of the 2017 Act."

47 In Article 58 (powers)—

(a) in paragraph 1, in point (a), omit ", and, where applicable, the controller's or the processor's representative";

(b) in paragraph 1, in point (f), for "Union or Member State procedural law" substitute "domestic law";
(c) in paragraph 3, omit point (c);
(d) omit paragraphs 4 to 6.

48 In Article 59 (activity reports)—
(a) for ", the government and other authorities as designated by Member State law" substitute "and the Secretary of State";
(b) omit ", to the Commission or to the Board".

Chapter VII of the GDPR (co-operation and consistency)

49 For Articles 60 to 76 substitute—

"Article 61

Co-operation with other supervisory authorities etc

1 The Commissioner may, in connection with carrying out the Commissioner's functions under this Regulation—
(a) co-operate with, provide assistance to and seek assistance from other supervisory authorities;
(b) conduct joint operations with other supervisory authorities, including joint investigations and joint enforcement measures.

2 The Commissioner must, in carrying out the Commissioner's functions under this Regulation, have regard to—
(a) decisions, advice, guidelines, recommendations and best practices issued by the European Data Protection Board established under Article 68 of the GDPR;
(b) any implementing acts adopted by the Commission under Article 67 of the GDPR (exchange of information)."

Chapter VIII of the GDPR (remedies, liability and penalties)

50 In Article 77 (right to lodge a complaint with a supervisory authority)—
(a) in paragraph 1, omit "in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement";
(b) in paragraph 2, for "The supervisory authority with which the complaint has been lodged" substitute "The Commissioner".

51 In Article 78 (right to an effective judicial remedy against a supervisory authority)—
(a) omit paragraph 2;
(b) for paragraph 3 substitute—

"3 Proceedings against the Commissioner are to be brought before a court in the United Kingdom.";

(c) omit paragraph 4.

52 In Article 79 (right to an effective judicial remedy against a controller or

processor), for paragraph 2, substitute—

"2 Proceedings against a controller or a processor are to be brought before a court (see section 167 of the 2017 Act)."

53 In Article 80 (representation of data subjects)—

(a) in paragraph 1, omit "where provided for by Member State law";

(b) omit paragraph 2.

54 Omit Article 81 (suspension of proceedings).

55 In Article 82 (right to compensation and liability), for paragraph 6, substitute—

"6 Proceeding for exercising the right to receive compensation are to be brought before a court (see section 167 of the 2017 Act)."

56 In Article 83 (general conditions for imposing administrative fines)—

(a) in paragraph 7, for "each Member State" substitute "the Secretary of State";

(b) for paragraph 8, substitute—

"8 Section 113(9) of the 2017 Act makes provision about the exercise of the Commissioner's powers under this Article. Part 6 of the 2017 Act (enforcement) makes further provision in connection with administrative penalties (including provision about appeals)."

(c) omit paragraph 9.

57 In Article 84 (penalties)—

(a) for paragraph 1, substitute—

"1 The rules on other penalties applicable to infringements of this Regulation are set out in the 2017 Act (see in particular Part 6 (enforcement))."";

(b) omit paragraph 2.

Chapter IX of the GDPR (provisions relating to specific processing situations)

58 In Article 85 (processing and freedom of expression and information)—

(a) omit paragraph 1;

(b) in paragraph 2, for "Member States shall" substitute "the Secretary of State, in addition to the relevant provisions, may by way of regulations (see section 15 of the 2017 Act),";

(c) after paragraph 2, insert—

"In this paragraph, "the relevant provisions" means section 14 of and Part 5 of Schedule 2 to the 2017 Act.";

(d) omit paragraph 3.

59 In Article 86 (processing and public access to official documents) for "Union or Member State law to which the public authority or body is subject" substitute "domestic law".

60 Omit Article 87 (processing of national identification number).

61 Omit Article 88 (processing in the context of employment).

62 In Article 89 (safeguards and derogations relating to processing for archiving purposes etc)—

(a) in paragraph 2, for "Union or Member State law may" substitute "the Secretary of State, in addition to the relevant provisions, may in regulations (see section 15 of the 2017 Act)";

(b) in paragraph 3, for "Union or Member State law" substitute "the Secretary of State, in addition to the relevant provisions, may in regulations (see section 15 of the 2017 Act)";

(c) after paragraph 3, insert—

"3A In this Article "the relevant provisions" means section 14 of and Part 6 of Schedule 2 to the 2017 Act."

63 Omit Article 90 (obligations of secrecy).

64 Omit Article 91 (existing data protection rules of churches and religious associations).

Chapter X of the GDPR (delegated acts and implementing acts)

65 Omit Article 92 (exercise of the delegation).

66 Omit Article 93 (committee procedure).

Chapter XI of the GDPR (final provisions)

67 Omit Article 94 (repeal of Directive 95/46/EC).

68 Omit Article 95 (relationship with Directive 2002/58/EC).

69 In Article 96 (relationship with previously concluded Agreements), for "by Member States" substitute "the United Kingdom or the Commissioner".

70 Omit Article 97 (Commission reports)

71 Omit Article 98 (Commission reviews).

72 Omit Article 99 (entry into force and application).

PART 2

MODIFICATIONS TO CHAPTER 2 OF PART 2

Introductory

73 In its application by virtue of section 20(2), Chapter 2 of the Part has effect as if it were modified as follows.

General modifications

74 (1) References to Chapter 2 of this Part and the provisions of that Chapter have effect as references to the applied Chapter 2 and the provisions of the applied Chapter 2.

(2) References to the GDPR and to the provisions of the GDPR have effect as references to the applied GDPR and to the provisions of the applied GDPR, except in section 17(2)(a).

(3) References to the processing of personal data to which Chapter 2 applies have effect as references to the processing of personal data to which Chapter 3 applies.

Exemptions

75 In section 15 (power to make further exemptions etc by regulations), in subsection (1)(a) and (d), for "Member State law" substitute "the Secretary of State".

SCHEDULE 7

Section 28

COMPETENT AUTHORITIES

1 Any United Kingdom government department other than a non-ministerial government department.

2 The Scottish Ministers.

3 The Department of Justice in Northern Ireland.

Chief officers of police and other policing bodies

4 The chief constable of a police force maintained under section 2 of the Police Act 1996.

5 The Commissioner of Police of the Metropolis.

6 The Commissioner of Police for the City of London.

7 The Chief Constable of the Police Service of Northern Ireland.

8 The chief constable of the Police Service of Scotland.

9 The chief constable of the British Transport Police.

10 The chief constable of the Civil Nuclear Constabulary.

11 The chief constable of the Ministry of Defence Police.

12 The Provost Marshal of the Royal Navy Police.

13 The Provost Marshal of the Royal Military Police.

14 The Provost Marshal of the Royal Air Force Police.

15 The chief officer of—

(a) a body of constables appointed under provision incorporating section 79 of the Harbours, Docks, and Piers Clauses Act 1847;

(b) a body of constables appointed under an order made under section 14 of the Harbours Act 1964;

(c) the body of constables appointed under section 154 of the Port of London Act 1968 (c.xxxii).

16 A body established in accordance with a collaboration agreement under section 22A of the Police Act 1996.

17 The Independent Office for Police Conduct.

18 The Police Investigations and Review Commissioner.

19 The Police Ombudsman for Northern Ireland.

Other authorities with investigatory functions

20 The Commissioners for Her Majesty's Revenue and Customs.

21 The Director General of the National Crime Agency.

22 The Director of the Serious Fraud Office.

23 The Director of Border Revenue.

24 The Financial Conduct Authority.

25 The Health and Safety Executive.

26 The Criminal Cases Review Commission.

27 The Scottish Criminal Cases Review Commission.

Authorities with functions relating to offender management

28 A provider of probation services (other than the Secretary of State), acting in pursuance of arrangements made under section 3(2) of the Offender Management Act 2007.

29 The Youth Justice Board for England and Wales.

30 The Parole Board for England and Wales.

31 The Parole Board for Scotland.

32 The Parole Commissioners for Northern Ireland.

33 The Probation Board for Northern Ireland.

34 The Prisoner Ombudsman for Northern Ireland.

35 A person who has entered into a contract for the running of, or part of—

(a) a prison or young offender institution under section 84 of the Criminal Justice Act 1991, or

(b) a secure training centre under section 7 of the Criminal Justice and Public Order Act 1994.

36 A person who has entered into a contract with the Secretary of State—

(a) under section 80 of the Criminal Justice Act 1991 for the purposes of prisoner escort arrangements, or

(b) under paragraph 1 of Schedule 1 to the Criminal Justice and Public Order Act 1994 for the purposes of escort arrangements.

37 A person who is, under or by virtue of any enactment, responsible for securing the electronic monitoring of an individual.

38 A youth offending team established under section 39 of the Crime and Disorder Act 1998.

Other authorities

39 The Director of Public Prosecutions.

40 The Director of Public Prosecutions for Northern Ireland.

41 The Lord Advocate.

42 A Procurator Fiscal.

43 The Director of Service Prosecutions.

44 The Information Commissioner.

45 The Scottish Information Commissioner.

46 The Scottish Courts and Tribunal Service.

47 The Crown agent.

48 A court or tribunal.

SCHEDULE 8

Section 33(3)

CONDITIONS FOR SENSITIVE PROCESSING UNDER PART 3

Judicial and statutory purposes

1 (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 administration of justice;
(b) the exercise of a function conferred on a person by an enactment.

Protecting individual's vital interests

2 This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual.

Personal data already in the public domain

3 This condition is met if the processing relates to personal data which is manifestly made public by the data subject.

Legal claims and judicial acts

4 This condition is met if the processing is necessary for the establishment, exercise or defence of a legal claim or whenever a court is acting in its judicial capacity.

Preventing fraud

5 (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, or

(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

6 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 purposes.

SCHEDULE 9

Section 84

CONDITIONS FOR PROCESSING UNDER PART 4

1 The data subject has given consent to the processing.

2 The processing is necessary—

(a) for the performance of a contract to which the data subject is a party, or

(b) in order to take steps at the request of the data subject prior to entering into a contract.

3 The processing is necessary for compliance with a legal obligation to which the controller is subject, other than an obligation imposed by contract.

4 The processing is necessary in order to protect the vital interests of the data subject or of another individual.

5 The processing is necessary—

(a) for the administration of justice,

(b) for the exercise of any functions of either House of Parliament,

(c) for the exercise of any functions conferred on a person by an enactment,

(d) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(e) for the exercise of any other functions of a public nature exercised in the public interest by a person.

6 (1) The processing is necessary for the purposes of legitimate interests pursued by—

(a) the controller, or
(b) the third party or parties to whom the data is disclosed.

(2) Sub-paragraph (1) does not apply where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.

(3) In this paragraph, "third party", in relation to personal data, means a person other than the data subject, the controller or a processor or other person authorised to process personal data for the controller or processor.

SCHEDULE 10

Section 84

CONDITIONS FOR SENSITIVE PROCESSING UNDER PART 4

Consent to particular processing

1 The data subject has given consent to the processing.

Right or obligation relating to employment

2 The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by an enactment or rule of law on the controller in connection with employment.

Vital interests of a person

3 The processing is necessary—
(a) in order to protect the vital interests of the data subject or of another person, in a case where—
(i) consent cannot be given by or on behalf of the data subject, or
(ii) the controller cannot reasonably be expected to obtain the consent of the data subject, or
(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

Data already published by data subject

4 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

Legal proceedings etc

5 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.

State functions

6 The processing is necessary—

(a) for the administration of justice,

(b) for the exercise of any functions of either House of Parliament,

(c) for the exercise of any functions conferred on any person by an enactment, or

(d) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

Medical purposes

7 (1) The processing is necessary for medical purposes and is undertaken by—

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph, "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

Equality

8 (1) The processing—

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) In this paragraph, "sensitive personal data" means personal data the processing of which constitutes sensitive processing (see section 84(7)).

SCHEDULE 11

Section 110

OTHER EXEMPTIONS UNDER PART 4

Preliminary

1 In this Schedule, "the listed provisions" means—

(a) Chapter 2 (the data protection principles), except section 84(1)(a) and (2) and Schedules 9 and 10;

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

(c) in Chapter 4, section 106 (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 and detection of crime, or

(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 is necessary—

(a) for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), or

(b) for the purpose of obtaining legal advice or otherwise 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 information in respect of which a claim to legal professional privilege or, in Scotland, confidentiality of communications, could be maintained in legal proceedings.

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 92 has effect subject to sub-paragraph (3).

(3) Where the relevant day falls before the day on which the results of the exam are announced, the period mentioned in section 92(10)(b) is extended until the earlier of—

(a) the end of the period of five months beginning with the relevant day, and

(b) the end of the period of 40 days beginning with the date of 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;

"relevant day" has the same meaning as in section 92.

(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 12

Section 112

THE 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

7 The 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

8 A 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

9 The Secretary of State may make payments to the Commissioner out of money provided by Parliament.

Fees and other sums

10 (1) All fees 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

12 Paragraphs 1(1), 7 and 8 do not extend to Scotland.

SCHEDULE 13

Section 114

OTHER GENERAL FUNCTIONS OF THE COMMISSIONER

General tasks

1 The Commissioner must—

(a) monitor and enforce Parts 3 and 4 of this Act;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing of personal data to which those Parts apply;

(c) 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 processing of personal data to which those Parts apply;

(d) promote the awareness of controllers and processors of their obligations under Parts 3 and 4 of this Act;

(e) on request, provide information to a data subject concerning the exercise of the data subject's rights under Parts 3 and 4 of this Act and, if appropriate, co-operate with LED supervisory authorities and foreign designated authorities to provide such information;

(f) co-operate with LED supervisory authorities and foreign designated authorities with a view to ensuring the consistency of application and enforcement of the Law Enforcement Directive and the Data Protection Convention, including by sharing information and providing mutual assistance;

(g) conduct investigations on the application of Parts 3 and 4 of this Act, including on the basis of information received from an LED supervisory authority, a foreign designated authority or another public authority;

(h) monitor relevant developments to the extent that they have an impact on the protection of personal data, including the development of information and communication technologies;

(i) contribute to the activities of the European Data Protection Board established by the GDPR in connection with the processing of personal data to which the Law Enforcement Directive applies.

General powers

2 The Commissioner has the following investigative, corrective, authorisation and advisory powers in relation to processing of personal data to which Part 3 or 4 of this Act applies—

(a) to notify the controller or the processor of an alleged infringement of Part 3 or 4 of this Act;

(b) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of Part 3 or 4 of this Act;

(c) to issue reprimands to a controller or processor where processing operations have infringed provisions of Part 3 or 4 of this Act;

(d) 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.

Definitions

3 In this Schedule—

"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;

"LED supervisory authority" means a supervisory authority for the purposes of Article 41 of the Law Enforcement Directive in a member State other than the United Kingdom.

SCHEDULE 14

Section 116

CO-OPERATION AND MUTUAL ASSISTANCE

PART 1

LAW ENFORCEMENT DIRECTIVE

Co-operation

1 (1) The Commissioner may provide information or assistance to an LED supervisory authority to the extent that, in the opinion of the Commissioner, providing that information or assistance is necessary for the performance of the recipient's data protection functions.

(2) The Commissioner may ask an LED supervisory authority to provide information or assistance which the Commissioner requires for the performance of the Commissioner's data protection functions.

(3) In this paragraph, "data protection functions" means functions relating to the protection of individuals with respect to the processing of personal data.

Requests for information and assistance from LED supervisory authorities

2 (1) This paragraph applies where the Commissioner receives a request from an LED supervisory authority for information or assistance referred to in Article 41 of the Law Enforcement Directive and the request—

(a) explains the purpose of and reasons for the request, and

(b) contains all other information necessary to enable the Commissioner to respond.

(2) The Commissioner must—

(a) take all appropriate measures required to reply to the request without undue delay and, in any event, before the end of the period of 1 month beginning with receipt of the request, and

(b) inform the LED supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request.

(3) The Commissioner must not refuse to comply with the request unless—

(a) the Commissioner does not have power to do what is requested, or

(b) complying with the request would infringe the Law Enforcement Directive, EU legislation or the law of the United Kingdom or a part of the United Kingdom.

(4) If the Commissioner refuses to comply with a request from an LED supervisory authority, the Commissioner must inform the authority of the reasons for the refusal.

(5) As a general rule, the Commissioner must provide information requested by LED supervisory authorities by electronic means using a standardised format.

Fees

3 (1) Subject to sub-paragraph (2), any information or assistance that is required to be provided by this Part of this Schedule must be provided free of charge.

(2) The Commissioner may enter into agreements with other LED supervisory authorities for the Commissioner and other authorities to indemnify each other for expenditure arising from the provision of assistance in exceptional circumstances.

Restrictions on use of information

4 Where the Commissioner receives information from an LED supervisory authority as a result of a request under paragraph 1(2), the Commissioner may use the information only for the purposes specified in the request.

LED supervisory authority

5 In this Part of this Schedule, "LED supervisory authority" means a supervisory authority for the purposes of Article 41 of the Law Enforcement Directive in a member State other than the United Kingdom.

PART 2

DATA PROTECTION CONVENTION

Co-operation between the Commissioner and foreign designated authorities

6 (1) The Commissioner must, at the request of a foreign designated authority—

(a) provide that authority with such information referred to in Article 13(3)(a) of the Data Protection Convention (information on law and administrative practice in the field of data protection) as is the subject of the request, and

(b) take appropriate measures in accordance with Article 13(3)(b) of the Data Protection Convention for providing that authority with information relating to the processing of personal data in the United Kingdom.

(2) The Commissioner may ask a foreign designated authority—

(a) to provide the Commissioner with information referred to in Article 13(3) of the Data Protection Convention, or

(b) to take appropriate measures to provide such information.

Assisting persons resident outside the UK with requests under Article 14 of the Convention

7 (1) This paragraph applies where a request for assistance in exercising any of the rights referred to in Article 8 of the Data Protection Convention in the United Kingdom is made by a person resident outside the United Kingdom, including where the request is forwarded to the Commissioner through the Secretary of State or a foreign designated authority.

(2) The Commissioner must take appropriate measures to assist the person to exercise those rights.

Assisting UK residents with requests under Article 8 of the Convention

8 (1) This paragraph applies where a request for assistance in exercising any of the rights referred to in Article 8 of the Data Protection Convention in a country or territory (other than the United Kingdom) specified in the request is—

(a) made by a person resident in the United Kingdom, and

(b) submitted through the Commissioner under Article 14(2) of the Convention.

(2) If the Commissioner is satisfied that the request contains all necessary particulars referred to in Article 14(3) of the Data Protection Convention, the Commissioner must send the request to the foreign designated authority in the specified country or territory.

(3) Otherwise, the Commissioner must, where practicable, notify the person making the request of the reasons why the Commissioner is not required to assist.

Restrictions on use of information

9 Where the Commissioner receives information from a foreign designated authority as a result of—

(a) a request made by the Commissioner under paragraph 6(2), or

(b) a request received by the Commissioner under paragraph 6(1) or 7,

the Commissioner may use the information only for the purposes specified in the request.

Foreign designated authority

10 In this Part of this Schedule, "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 Data Protection Convention.

SCHEDULE 15

Section 147

POWERS OF ENTRY AND INSPECTION

Issue of warrants in connection with non-compliance and offences

1 (1) This paragraph applies if a circuit judge or a District Judge (Magistrates' Courts) is satisfied by information on oath supplied by the Commissioner that—

(a) there are reasonable grounds for suspecting that—

(i) a controller or processor has failed or is failing as described in section 142(2), or

(ii) an offence under this Act has been or is being committed, and

(b) there are reasonable grounds for suspecting that evidence of the failure or of the commission of the offence is to be found on premises specified in the information.

(2) The judge may grant a warrant to the Commissioner.

Issue of warrants in connection with assessment notices

2 (1) This paragraph applies if a circuit judge or a District Judge (Magistrates' Courts) is satisfied by information on oath supplied by the Commissioner that a controller or processor has failed to comply with a requirement imposed by an assessment notice.

(2) The judge may, for the purpose of enabling the Commissioner to determine whether the controller or processor has complied or is complying with the data protection legislation, grant a warrant to the Commissioner in relation to premises that were specified in the assessment notice.

Restrictions on issuing warrants: processing for the special purposes

3 A judge must not issue a warrant under this Schedule in respect of personal data processed for the special purposes unless a determination under section 164 with respect to the data or the processing has taken effect.

Restrictions on issuing warrants: procedural requirements

4 (1) A judge must not issue a warrant under this Schedule unless satisfied that—

(a) the conditions in sub-paragraphs (2) to (4) are met,

(b) compliance with those conditions would defeat the object of entry to the premises in question, or

(c) the Commissioner requires access to the premises in question urgently.

(2) The first condition is that the Commissioner has given 7 days' notice in writing to the occupier of the premises in question demanding access to the premises.

(3) The second condition is that—

(a) access to the premises was demanded at a reasonable hour and was unreasonably refused, or

(b) entry to the premises was granted but the occupier unreasonably refused to comply with a request by the Commissioner or the Commissioner's officers or staff to be allowed to do any of the things referred to in paragraph 5.

(4) The third condition is that, since the refusal, the occupier of the premises—

(a) has been notified by the Commissioner of the application for the warrant, and

(b) has had an opportunity to be heard by the judge on the question of whether or not the warrant should be issued.

(5) In determining whether the first condition is met, an assessment notice given to the occupier is to be disregarded.

Content of warrants

5 (1) A warrant issued under this Schedule must authorise the Commissioner or any of the Commissioner's officers or staff—

(a) to enter the premises,

(b) to search the premises, and

(c) to inspect, examine, operate and test any equipment found on the premises which is used or intended to be used for the processing of personal data.

(2) A warrant issued under paragraph 1 must authorise the Commissioner or any of the Commissioner's officers or staff—

(a) to inspect and seize any documents or other material found on the premises which may be evidence of the failure or offence mentioned in that paragraph,

(b) to require any person on the premises to provide an explanation of any document or other material found on the premises, and

(c) to require any person on the premises to provide such other information as may reasonably be required for the purpose of determining whether the controller or processor has failed or is failing as described in section 142(2).

(3) A warrant issued under paragraph 2 must authorise the Commissioner or any of the Commissioner's officers or staff—

(a) to inspect and seize any documents or other material found on the premises which may enable the Commissioner to determine whether the controller or processor has complied or is complying with the data protection legislation,

(b) to require any person on the premises to provide an explanation of any document or other material found on the premises, and

(c) to require any person on the premises to provide such other information as may reasonably be required for the purpose of determining whether the controller or processor has complied or is complying with the data protection legislation.

(4) A warrant issued under this Schedule must authorise the Commissioner or any of the Commissioner's officers or staff to do the things described in sub-paragraphs (1) to (3) at any time in the period of 7 days beginning with the day on which the warrant is issued.

Copies of warrants

6 A judge who issues a warrant under this Schedule must—

(a) issue two copies of it, and

(b) certify them clearly as copies.

Execution of warrants: reasonable force

7 A person executing a warrant issued under this Schedule may use such reasonable force as may be necessary.

Execution of warrants: time when executed

8 A warrant issued under this Schedule may be executed only at a reasonable, hour, unless it appears to the person executing it that there are grounds for suspecting that exercising it at a reasonable hour would defeat the object of the warrant.

Execution of warrants: occupier of premises

9 (1) If an occupier of the premises in respect of which a warrant is issued under this Schedule is present when the warrant is executed, the person executing the warrant must—

(a) show the occupier the warrant, and

(b) give the occupier a copy of it.

(2) Otherwise, a copy of the warrant must be left in a prominent place on the premises.

Execution of warrants: seizure of documents etc

10 (1) This paragraph applies where a person executing a warrant under this Schedule seizes something.

(2) The person must, on request—

(a) give a receipt for it, and

(b) give an occupier of the premises a copy of it.

(3) Sub-paragraph (2)(b) does not apply if the person executing the warrant considers that providing a copy would result in undue delay.

(4) Anything seized may be retained for so long as is necessary in all the circumstances.

Matters exempt from inspection and seizure: privileged communications

11 (1) The powers of inspection and seizure conferred by a warrant issued under this Schedule are not exercisable 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.

(2) The powers of inspection and seizure conferred by a warrant issued under this Schedule are not exercisable 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.

(3) Sub-paragraphs (1) and (2) do not prevent the exercise of powers conferred by a warrant issued under this Schedule in respect of—

(a) anything in the possession of a person other than the professional legal adviser or the adviser's client, or

(b) anything held with the intention of furthering a criminal purpose.

(4) The references to a communication in sub-paragraphs (1) and (2) include—

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

(b) anything enclosed with or referred to in the communication if made as described in sub-paragraph (1)(b) or in sub-paragraph (2)(b) and (c).

(5) In sub-paragraphs (1) to (3), the references to the client of a professional legal adviser include a person acting on behalf of such a client.

Matters exempt from inspection and seizure: Parliamentary privilege

12 The powers of inspection and seizure conferred by a warrant issued under this Schedule are not exercisable where their exercise would involve an infringement of the privileges of either House of Parliament.

Partially exempt material

13 (1) This paragraph applies if a person in occupation of premises in respect of which a warrant is issued under this Schedule objects to the inspection or seizure of any material under the warrant on the grounds that it consists partly of matters in respect of which those powers are not exercisable.

(2) The person must, if the person executing the warrant so requests, provide that person with a copy of so much of the material as is not exempt from those powers.

Return of warrants

14 (1) Where a warrant issued under this Schedule is executed—

(a) it must be returned to the court from which it was issued after being executed, and

(b) the person by whom it is executed must write on the warrant a statement of the powers that have been exercised under the warrant.

(2) Where a warrant issued under this Schedule is not executed, it must be returned to the court from which it was issued within the time authorised for its execution.

Offences

15 (1) It is an offence for a person—

(a) intentionally to obstruct a person in the execution of a warrant issued under this Schedule, or

(b) to fail without reasonable excuse to give a person executing such a warrant such assistance as the person may reasonably require for the execution of the warrant.

(2) It is an offence for a person—

(a) to make a statement in response to a requirement under paragraph 5(2)(b) or (c) or (3)(b) or (c) which the person knows to be false in a material respect, or

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

Self-incrimination

16 (1) An explanation given, or information provided, by a person in response to a requirement under paragraph 5(2)(b) or (c) or (3)(b) or (c) may only be used in evidence against that person—

(a) on a prosecution for an offence under a provision listed in sub-paragraph (2), or

(b) on a prosecution for any other offence where—

(i) in giving evidence that person makes a statement inconsistent with that explanation or information, and

(ii) evidence relating to that explanation or information is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(2) Those provisions are—

(a) paragraph 15,

(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 (false statutory declarations and other false unsworn statements).

Vessels, vehicles etc

17 In this Schedule—

(a) "premises" includes a vehicle, vessel or other means of transport, and

(b) references to the occupier of premises include the person in charge of a vehicle, vessel or other means of transport.

Scotland

18 In the application of this Schedule to Scotland—

(a) references to a circuit judge have effect as if they were references to the sheriff or the summary sheriff,

(b) references to information on oath have effect as if they were references to evidence on oath, and

(c) references to the court from which the warrant was issued have effect as if they were references to the sheriff clerk.

Northern Ireland

19 In the application of this Schedule to Northern Ireland—

(a) references to a circuit judge have effect as if they were references to a county court judge, and

(b) references to information on oath have effect as if they were references to a complaint on oath.

SCHEDULE 16

Section 148

PENALTIES

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 in reliance on a notice of intent after the end of the period of 6 months beginning with the day after the notice of intent is given.

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;

(d) the date on which the Commissioner proposes to give the penalty notice.

(2) The information required under sub-paragraph (1)(b) includes—

(a) a description of the circumstances of the failure, and

(b) where the notice if given in respect of a failure described in section 142(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 with the day on which 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 (1) The Commissioner may not give a penalty notice 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 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.

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 154;

(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 if given in respect of a failure described in section 142(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 with the day after the day on which 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 148 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 controller or processor 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.

SCHEDULE 17

Section 171

RELEVANT RECORDS

Relevant records

1 (1) In section 171, "relevant record" means—

(a) a health record,

(b) a relevant record relating to a conviction or caution (see paragraph 2), or

(c) a relevant record relating to statutory functions (see paragraph 3).

(2) A record is not a "relevant record" to the extent that it relates, or is to relate, only to personal data which falls within section 19(2) (manual unstructured personal data held by FOI public authorities).

Relevant records relating to a conviction or caution

2 (1) "Relevant record relating to a conviction or caution" means a record which—

(a) has been or is to be obtained by a data subject in the exercise of a data subject access right from a person listed in sub-paragraph (2), and

(b) contains information relating to a conviction or caution.

(2) Those persons are—

(a) the chief constable of a police force maintained under section 2 of the Police Act 1996;

(b) the Commissioner of Police of the Metropolis;

(c) the Commissioner of Police for the City of London;

(d) the Chief Constable of the Police Service of Northern Ireland;

(e) the chief constable of the Police Service of Scotland;

(f) the Director General of the National Crime Agency;

(g) the Secretary of State.

(3) 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)).

Relevant records relating to statutory functions

3 (1) "Relevant record relating to statutory functions" means a record which—

(a) has been or is to be obtained by a data subject in the exercise of a data subject access right from a person listed in sub-paragraph (2), and

(b) contains information relating to a relevant function in relation to that person.

(2) Those persons are—

(a) the Secretary of State;

(b) the Department for Communities in Northern Ireland;

(c) the Scottish Ministers;

(d) the Disclosure and Barring Service.

(3) In relation to the Secretary of State, the "relevant functions" are—

(a) the Secretary of State's functions in relation to a person sentenced to detention under—

(i) section 92 of the Powers of Criminal Courts (Sentencing Act 2000,

(ii) section 205(2) or 208 of the Criminal Procedure (Scotland) Act 1995, or

(iii) section 73 of the Children and Young Persons Act (Northern Ireland) 1968 (c. 34 (N.I.));

(b) the Secretary of State's functions in relation to a person imprisoned or detained under—

(i) the Prison Act 1952,

(ii) the Prisons (Scotland) Act 1989, or

(iii) the Prison Act (Northern Ireland) 1953 (c. 18 (N.I.));

(c) the Secretary of State's functions under—

(i) the Social Security Contributions and Benefits Act 1992,

(ii) the Social Security Administration Act 1992,

(iii) the Jobseekers Act 1995,

(iv) Part 1 of the Welfare Reform Act 2007, or

(v) Part 1 of the Welfare Reform Act 2012.

(4) In relation to the Department for Communities in Northern Ireland, the "relevant functions" are its functions under—

(a) the Social Security Contributions and Benefits (Northern Ireland) Act 1992,

(b) the Social Security Administration (Northern Ireland) Act 1992,

(c) the Jobseekers (Northern Ireland) Order 1995 (S.I. 1995/2705 (N.I. 15)), or

(d) Part 1 of the Welfare Reform Act (Northern Ireland) 2007 (c. 2 (N.I.)).

(5) In relation to the Scottish Ministers, the "relevant functions" are their functions under Parts 1 and 2 of the Protection of Vulnerable Groups (Scotland) Act 2007 (asp 14).

(6) In relation to the Disclosure and Barring Service, the "relevant functions" are its functions under—

(a) the Safeguarding Vulnerable Groups Act 2006, or

(b) the Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 (S.I. 2007/1351 (N.I. 11)).

Data subject access right

4 In this Schedule, "data subject access right" means a right under—

(a) Article 15 of the GDPR (right of access by the data subject);

(b) Article 20 of the GDPR (right to data portability);

(c) section 43 of this Act (law enforcement processing: right of access by the data subject);

(d) section 92 of this Act (intelligence services processing: right of access by the data subject).

Records stating that personal data is not processed

5 For the purposes of this Schedule, a record which states that a controller is not processing personal data relating to a particular matter is to be taken to be a record containing information relating to that matter.

Power to amend

6 (1) The Secretary of State may by regulations amend this Schedule.

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

SCHEDULE 18

Section 190

MINOR AND CONSEQUENTIAL AMENDMENTS

Consumer Credit Act 1974 (c. 39)

1 (1) The Consumer Credit Act 1974 is amended as follows.

(2) In section 157 (duty to disclose name etc of agency)—

(a) in subsection (2A)(a), for "the Data Protection Act 1998" substitute "the GDPR";

(b) in subsection (2A)(b), after "any" insert "other";

(c) after subsection (4) insert—

"(5) In this section "the GDPR" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2017 (see section 2(14) of that Act)."

(3) In section 159 (correction of wrong information)—

(a) in subsection (1)(a), for "section 7 of the Data Protection Act 1998" substitute "Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers)";

(b) after subsection (8) insert—

"(9) In this section "the GDPR" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2017 (see section 2(14) of that Act)."

Data Protection Act 1998 (c. 29)

2 The Data Protection Act 1998 is repealed.

Immigration and Asylum Act 1999 (c. 33)

3 (1) Section 13 of the Immigration and Asylum Act 1999 (proof of identity of persons to be removed or deported) is amended as follows.

(2) For subsection (4) substitute—

"(4) For the purposes of Article 49(1)(d) of the GDPR, the provision under this section of identification data is a transfer of personal data which is necessary for important reasons of public interest."

(3) After subsection (4) insert—

"(4A) "The GDPR" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2017 (see section 2(14) of that Act)."

Freedom of Information Act 2000 (c. 36)

4 The Freedom of Information Act 2000 is amended as follows.

5 In section 2(3) (absolute exemptions), for paragraph (f) substitute—

"(f) section 40(1),

(fa) section 40(2) so far as relating to cases where the first condition referred to in that subsection is satisfied,".

6 (1) Section 40 (personal information) is amended as follows.

(2) In subsection (2)—

(a) in paragraph (a), for "do" substitute "does", and

(b) in paragraph (b), for "either the first or the second" substitute "the first, second or third".

(3) For subsection (3) substitute—

"(3A) The first condition is that the disclosure of the information to a member of the public otherwise than under this Act—

(a) would contravene any of the data protection principles, or

(b) would do so if the exemption in section 22(1) of the Data Protection Act 2017 (manual unstructured data held by public authorities) were disregarded.

(3B) The second condition is that the disclosure of the information to a member of the public otherwise than under this Act would contravene Article 21 of the GDPR (general processing: right to object to processing)."

(4) For subsection (4) substitute—

"(4A) The third condition is that—

(a) on a request under Article 15(1) of the GDPR (general processing: right of access by the data subject) for access to personal data, the information would be withheld in reliance on provision made by or under section 14, 15 or 24 of, or Schedule 2, 3 or 4 to, the Data Protection Act 2017, or

(b) on a request under section 43(1)(b) of that Act (law enforcement processing: right of access by the data subject), the information would be withheld in reliance on subsection (4) of that section."

(5) For subsection (5) substitute—

"(5A) The duty to confirm or deny does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1).

(5B) The duty to confirm or deny does not arise in relation to other information if or to the extent that any of the following applies—

(a) giving a member of the public the confirmation or denial that would have to be given to comply with section 1(1)(a)—

(i) would (apart from this Act) contravene any of the data protection principles, or

(ii) would do so if the exemptions in section 22(1) of the Data Protection Act 2017 (manual unstructured data held by public authorities) were disregarded;

(b) giving a member of the public the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) contravene Article 21 of the GDPR (general processing: right to object to processing);

(c) on a request under Article 15(1) of the GDPR (general processing: right of access by the data subject) for confirmation of whether personal data is being processed, the information would be withheld in reliance on a provision listed in subsection (4A)(a);

(d) on a request under section 43(1)(a) of the Data Protection Act 2017 (law enforcement processing: right of access by the data subject), the information would be withheld in reliance on subsection (4) of that section."

(6) Omit subsection (6).

(7) For subsection (7) substitute—

"(7) In this section—

"the data protection principles" means the principles set out in—

(a) Article 5(1) of the GDPR, and

(b) section 32(1) of the Data Protection Act 2017;

"data subject" has the same meaning as in the Data Protection Act 2017 (see section 2(5) of that Act);

"the GDPR", "personal data" and "processing" have the same meaning as in Parts 5 to 7 of the Data Protection Act 2017 (see section 2(14) of that Act).

(8) In determining for the purposes of this section whether the lawfulness principle in Article 5(1)(a) of the GDPR would be contravened by the disclosure of information, Article 6(1) of the GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted."

7 Omit section 49 (reports to be laid before Parliament).

8 For section 61 (appeal proceedings) substitute—

"61 Appeal proceedings

(1) Tribunal Procedure Rules may make provision for regulating the exercise of rights of appeal conferred by sections 57(1) and (2) and 60(1) and (4).

(2) In relation to appeals under those provisions, 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.

(3) Subsection (4) applies where—

(a) a person does something, or fails to do something, in relation to proceedings before the First-tier Tribunal on an appeal under those provisions, 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.

(4) The First-tier Tribunal may certify the offence to the Upper Tribunal.

(5) Where an offence is certified under subsection (4), the Upper Tribuna 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.

(6) Before exercising the power under subsection (5)(b), the court 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."

9 After section 76A insert—

"76B Disclosure of information to Commissioner or Tribunal

No enactment or rule of law prohibiting or restricting the disclosure of information precludes a person from providing the Commissioner, the First-tier Tribunal or the Upper Tribunal with information necessary for the discharge of their functions under this Act.

76C Confidentiality of information provided to Commissioner

(1) It is an offence for a person who is or has been the Commissioner, or a member of the Commissioner's staff or an agent of the Commissioner, knowingly or recklessly to disclose information which—

(a) has been obtained by, or provided to, the Commissioner under or for the purposes of this Act,

(b) relates to an identified or identifiable living 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 provided for the purpose of its being made available to the public (in whatever manner) under a provision of this Act or the data protection legislation,

(c) the disclosure was made for the purposes of, and is necessary for, the discharge of a function under this Act or the data protection legislation,

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

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

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

(3) In this section, "the data protection legislation" and "identifiable living individual" have the same meaning as in the Data Protection Act 2017 (see section 2 of that Act)."

10 In section 77(1)(b) (offence of altering etc records with intent to prevent disclosure), omit "or section 7 of the Data Protection Act 1998,".

Freedom of Information (Scotland) Act 2002 (asp 13)

11 The Freedom of Information (Scotland) Act 2002 is amended as follows.

12 In section 2(2)(e)(ii) (absolute exemptions), omit "by virtue of subsection (2)(a)(i) or (b) of that section".

13 (1) Section 38 (personal information) is amended as follows.

(2) In subsection (1), for paragraph (b) substitute—

"(b) personal data and the first, second or third condition is satisfied (see subsections (2A) to (3A));".

(3) For subsection (2) substitute—

"(2A) The first condition is that the disclosure of the information to a member of the public otherwise than under this Act—

(a) would contravene any of the data protection principles, or

(b) would do so if the exemptions in section 22(1) of the Data Protection Act 2017 (manual unstructured data held by public authorities) were disregarded.

(2B) The second condition is that the disclosure of the information to a member of the public otherwise than under this Act would contravene Article 21 of the GDPR (general processing: right to object to processing)."

(4) For subsection (3) substitute—

"(3A) The third condition is that—

(a) on a request under Article 15(1) of the GDPR (general processing: right of access by the data subject) for access to personal data, the information would be withheld in reliance on provision made by or under section 14, 15 or 24 of, or Schedule 2, 3 or 4 to, the Data Protection Act 2017, or

(b) on a request under section 43(1)(b) of that Act (law enforcement processing: right of access by the data subject), the information would be withheld in reliance on subsection (4) of that section."

(5) Omit subsection (4).

(6) In subsection (5), for the definitions of "the data protection principles" and of "data subject" and "personal data" substitute—

""the data protection principles" means the principles set out in—

(a) Article 5(1) of the GDPR, and

(b) 32(1) of the Data Protection Act 2017;

"data subject" has the same meaning as in the Data Protection Act 2017 (see section 2(5) of that Act);

"the GDPR", "personal data" and "processing" have the same meaning as in Parts 5 to 7 of the Data Protection Act 2017 (see section 2(14) of that Act);".

(7) After that subsection insert—

"(5A) In determining for the purposes of this section whether the lawfulness principle in Article 5(1)(a) of the GDPR would be contravened by the disclosure of information, Article 6(1) of the GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted."

Environmental Information Regulations 2004 (S.I. 2004/3391)

14 The Environmental Information Regulations 2004 (S.I. 2004/3391) are amended as follows.

15 (1) Regulation 2 (interpretation) is amended as follows.

(2) In paragraph (1), at the appropriate places, insert—

""the data protection principles" means the principles set out in—

(a) Article 5(1) of the GDPR,

(b) section 32(1) of the Data Protection Act 2017, and

(c) section 83(1) of that Act;";

""data subject" has the same meaning as in the Data Protection Act 2017 (see section 2(5) of that Act);";

""the GDPR" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2017 (see section 2(14) of that Act);";

""personal data" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2017 (see section 2(14) of that Act);".

(3) For paragraph (4) substitute—

"(4A) In these Regulations, references to the Data Protection Act 2017 have effect as if in Chapter 3 of Part 2 of that Act (other general processing)—

(a) the references to an FOI public authority were references to a public authority as defined in these Regulations, and

(b) the references to personal data held by such an authority were to be interpreted in accordance with regulation 3(2)."

16 (1) Regulation 13 (personal data) is amended as follows.

(2) For paragraph (1) substitute—

"(1) To the extent that the information requested includes personal data of which the applicant is not the data subject, a public authority must not disclose the personal data if—

(a) the first condition is satisfied, or

(b) the second or third condition is satisfied and, in all the circumstances of the case, the public interest in not disclosing the information outweighs the public interest in disclosing it."

(3) For paragraph (2) substitute—

"(2A) The first condition is that the disclosure of the information to a member of the public otherwise than under these Regulations—

(a) would contravene any of the data protection principles, or

(b) would do so if the exemption in section 22(1) of the Data Protection Act 2017 (manual unstructured data held by public authorities) were disregarded.

(2B) The second condition is that the disclosure of the information to a member of the public otherwise than under these Regulations would contravene—

(a) Article 21 of the GDPR (general processing: right to object to processing), or

(b) section 97 of the Data Protection Act 2017 (intelligence services processing: right to object to processing)."

(4) For paragraph (3) substitute—

"(3A) The third condition is that—

(a) on a request under Article 15(1) of the GDPR (general processing: right of access by the data subject) for access to personal data, the information would be withheld in reliance on provision made by or under section 14, 15 or 24 of, or Schedule 2, 3 or 4 to, the Data Protection Act 2017,

(b) on a request under section 43(1)(b) of that Act (law enforcement processing: right of access by the data subject), the information would be withheld in reliance on subsection (4) of that section, or

(c) on a request under section 92(1)(b) of that Act (intelligence services processing: rights of access by the data subject), the information would be withheld in reliance on a provision of Chapter 6 of Part 4 of that Act."

(5) Omit paragraph (4).

(6) For paragraph (5) substitute—

"(5A) For the purposes of this regulation a public authority may respond to a request by neither confirming nor denying whether such information exists and is held by the public authority, whether or not it holds such information, to the extent that—

(a) the condition in paragraph (5B)(a) is satisfied, or

(b) a condition in paragraphs (5B)(b) to (e) is satisfied and in all the circumstances of the case, the public interest in not

confirming or denying whether the information exists outweighs the public interest in doing so.

(5B) The conditions mentioned in paragraph (5A) are—

(a) giving a member of the public the confirmation or denial—

(i) would (apart from these Regulations) contravene any of the data protection principles, or

(ii) would do so if the exemptions in section 22(1) of the Data Protection Act 2017 (manual unstructured data held by public authorities) were disregarded;

(b) giving a member of the public the confirmation or denial would (apart from these Regulations) contravene Article 21 of the GDPR or section 97 of the Data Protection Act 2017 (right to object to processing);

(c) on a request under Article 15(1) of the GDPR (general processing: right of access by the data subject) for confirmation of whether personal data is being processed, the information would be withheld in reliance on a provision listed in paragraph (3A)(a);

(d) on a request under section 43(1)(a) of the Data Protection Act 2017 (law enforcement processing: right of access by the data subject), the information would be withheld in reliance on subsection (4) of that section;

(e) on a request under section 92(1)(a) of that Act (intelligence services processing: rights of access by the data subject), the information would be withheld in reliance on a provision of Chapter 6 of Part 4 of that Act."

(7) After that paragraph insert—

"(6) In determining for the purposes of this regulation whether the lawfulness principle in Article 5(1)(a) of the GDPR would be contravened by the disclosure of information, Article 6(1) of the GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted."

17 In regulation 14 (refusal to disclose information), in paragraph (3)(b), for "regulations 13(2)(a)(ii) or 13(3)" substitute "regulation 13(1)(b) or (5A)".

18 In regulation 18 (enforcement and appeal provisions), in paragraph (5), for "regulation 13(5)" substitute "regulation 13(5A)".

Environmental Information (Scotland) Regulations 2004 (S.S.I. 2004/520)

19 The Environmental Information (Scotland) Regulations 2004 (S.I. 2004/520) are amended as follows.

20 (1) Regulation 2 (interpretation) is amended as follows.

(2) In paragraph (1), at the appropriate places, insert—

""the data protection principles" means the principles set out in—

(a) Article 5(1) of the GDPR, and

(b) section 32(1) of the Data Protection Act 2017;";

""data subject" has the same meaning as in the Data Protection Act 2017 (see section 2(5) of that Act);";

""the GDPR" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2017 (see section 2(14) of that Act);";

""personal data" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2017 (see section 2(14) of that Act);".

(3) For paragraph (3) substitute—

"(3A) In these Regulations, references to the Data Protection Act 2017 have effect as if in Chapter 3 of Part 2 of that Act (other general processing)—

(a) the references to an FOI public authority were references to a Scottish public authority as defined in these Regulations, and

(b) the references to personal data held by such an authority were to be interpreted in accordance with paragraph (2) of this regulation."

21 (1) Regulation 11 (personal data) is amended as follows.

(2) For paragraph (2) substitute—

"(2) To the extent that environmental information requested includes personal data of which the applicant is not the data subject, a Scottish public authority must not make the personal data available if—

(a) the first condition set out in paragraph (3A) is satisfied, or

(b) the second or third condition set out in paragraph (3B) or (4A) is satisfied and, in all the circumstances of the case, the public interest in making the information available is outweighed by that in not doing so."

(3) For paragraph (3) substitute—

"(3A) The first condition is that the disclosure of the information to a member of the public otherwise than under these Regulations—

(a) would contravene any of the data protection principles, or

(b) would do so if the exemption in section 22(1) of the Data Protection Act 2017 (manual unstructured data held by public authorities) were disregarded.

(3B) The second condition is that the disclosure of the information to a member of the public otherwise than under these Regulations would contravene Article 21 of the GDPR (general processing: right to object to processing)."

(4) For paragraph (4) substitute—

"(4A) The third condition is that any of the following applies to the information—

(a) it is exempt from the obligation under Article 15(1) of the GDPR (general processing: right of access by the data subject) to provide access to, and information about, personal data by virtue of provision made by or under section 14, 15 or 24 of, or Schedule 2, 3 or 4 to, the Data Protection Act 2017, or

(b) on a request under section 43(1)(b) of that Act (law enforcement processing: right of access by the data subject),

the information would be withheld in reliance on subsection (4) of that section.

(5) Omit paragraph (5).

(6) After paragraph (6) insert—

"(7) In determining, for the purposes of this regulation, whether the lawfulness principle in Article 5(1)(a) of the GDPR would be contravened by the disclosure of information, Article 6(1) of the GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted."

Criminal Justice and Immigration Act 2008 (c. 4)

22 In the Criminal Justice and Immigration Act 2008, omit—

(a) section 77 (power to alter penalty for unlawfully obtaining etc personal data);

(b) section 78 (new defence for obtaining etc for journalism and other special purposes).

Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 (S.I. 2014/3141)

23 In the Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014, omit Part 4 (data protection in relation to police and judicial co-operation in criminal matters).

Small Business, Enterprise and Employment Act 2015 (c. 26)

24 (1) Section 6 of the Small Business, Enterprise and Employment Act 2015 (application of listed provisions to designated credit reference agencies) is amended as follows.

(2) In subsection (7)—

(a) for paragraph (b) substitute—

"(b) Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers);";

(b) omit paragraph (c).

(3) After subsection (7) insert—

"(7A) In subsection (7) "the GDPR" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2017 (see section 2(14) of that Act)."

Digital Economy Act 2017 (c. 30)

25 In the Digital Economy Act 2017, omit sections 108 to 110 (charges payable to the Information Commissioner).

Provision inserted in subordinate legislation by this Schedule

26 Provision inserted into subordinate legislation by this Schedule may be amended or revoked as if it had been inserted using the power under which the subordinate legislation was originally made.

Data Protection Bill [HL]

A

B I L L

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 conduct; and for connected purposes.

Lord Ashton of Hyde

Ordered to be Printed, 13th September 2017

© Parliamentary copyright House of Lords 2017
This publication may be reproduced under the terms of the Open Parliament Licence, which is published at www.parliament.uk/site-information/copyright

PUBLISHED BY AUTHORITY OF THE HOUSE OF LORDS