DATA PROTECTION ACT 2004

Principal Act

Act. No. 2004-01 *Commencement LN.(2006/040)* *See table below*
Assent 28.1.2004

Column 1 **Commencement Date**	**Column 2** **Sections**	**Column 3** **Personal data in respect of which commencement date applies**
(a) 13 April 2006;	1, 2, 20, 21, 28, 36, 37	
(b) 13 April 2006 in respect of personal data listed in column 3;	3 – 15 19 25 – 27 29 32 – 35	all personal data which may be transmitted to another Schengen state or territory pursuant to, or in connection with, proceedings under– (i) the Mutual Legal Assistance (European Union) Act 2004; (ii) the European Arrest Warrant Act 2004; (iii) the Transfer of Sentenced Persons Act 2002; (iv) the Drug Trafficking Offences Act 1995; (v) police co-operation under Articles 39 and 46 – 47 of the Convention of 19 June 1990 Implementing the Schengen Agreement of 14 June 1985; and (vi) customs and other co-operation under Article 73 of the Convention of 19 June 1990 Implementing the Schengen Agreement of 14 June 1985;
(c)1 June 2006 in respect of personal data listed in column 3;	3 – 19 22 – 27 29 – 35	all manual and automated personal data in respect of which the Act has not been commenced under paragraph(b) save where paragraph (d) applies;
(d) 1 September 2006 in respect of personal data listed in column 3.	6(1)(a)-(c), 6(3) 7, 8	manual personal data to which paragraph (b) does not apply and which is already held by data controllers on 1st June 2006.

Amending enactments	Relevant current provisions	Commencement date
LN. 2006/039	*Corrigenda*	
2014/233	ss. 2, 7(1)(e), 13A, 13B, 13C, 13D, 13E, 13F, 13G, 16(2)(b), 24(5)(b), 25(5), (6), 37(3)(a)(ii)	1.12.2014
Act. 2016-18	s. 5(1)(b)	23.4.2018
Ln. 2018/124	ss. 2, 3, 5(1)(a), 6-200, Sch. 1-17	25.5.2018

English sources:
None cited

EU Legislation/International Agreements involved:
Directive 95/46/EC
Directive (EU) 2016/680
Regulation (EU) 2016/679

ARRANGEMENT OF SECTIONS

Section

Enforcement

Information notices

Assessment notices

Enforcement notices

Powers of entry and inspection

Penalties

Guidance

Appeals

Complaints

AN ACT TO TRANSPOSE INTO THE LAW OF GIBRALTAR DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA AND TO IMPLEMENT ARTICLES 126 – 130 OF THE CONVENTION OF 19 JUNE 1990 APPLYING THE SCHENGEN AGREEMENT OF 14 JUNE 1985.

Part I
General

Title and Commencement.

1(1) This Act may be cited as the Data Protection Act 2004.

(2) This Act comes into operation on the day appointed by the Minister by notice in the Gazette and different days may be appointed for the coming into operation of different sections or for the coming into operation of the Act, or sections of the Act, in relation to different types or different purposes of processing.

Definitions.

2.(1) In this Act–

"blocking" in relation to data means marking the data so that it is not possible to process it for purposes in relation to which it is marked;

"the Commissioner" means the Data Protection Commissioner designated under section 123;

"competent authority" for the purposes of implementing the data protection provisions of the Schengen Agreement in Gibraltar, means the Commissioner;

"controller" and "processor", in relation to the processing of personal data to which Chapter 2 or 3 of Part II, Part III or Part IV applies, have the same meaning as in that Chapter or Part (see sections 7, 8, 41 and 92, and see also subsection (2)(c));

"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 from time to time;

"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 Gibraltar law for the purposes of the GDPR or the Law Enforcement Directive;

"data subject" means the identified or identifiable living individual to whom personal data relates;

"enforcement notice" means a written notice issued by the Commissioner under section 155 requiring specified actions to be taken;

"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;

"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);

"The applied GDPR" means the GDPR as applied by Chapter 3 of Part II.

"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;

"information notice" means a written notice issued by the Commissioner under section 150 requiring specified information to be provided to him;

"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;

"the Minister" means the Minister with responsibility for data protection;

"personal data" means , subject to subsection (2)(c), any information relating to an identified or identifiable living individual;

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

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

(b) adaptation or alteration;

(c) retrieval, consultation or use;

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

(e) alignment or combination; or

(f) restriction, erasure or destruction,

albeit subject to subsection (2)(c) and sections 7(7), 38(2) and 91(3), which make provision about references to processing in the different Parts of this Act.

"Schengen Agreement" means the Convention implementing the Schengen Agreement of 14th June 1985 between the Government of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, as the same may be amended from time to time, and to the extent that it applies to Gibraltar;

"Schengen State" means a State party to the Schengen Convention.

(2) In Parts V to VII, except where otherwise provided-

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

(b) references to Chapter 2 of Part II, or to a provision of that Chapter, include that Chapter or that provision as applied by Chapter 3 of Part II;

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

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

Subject matter and Application of Act.

3.(1) This Act makes provision about the processing of personal data, and most processing of personal data is subject to the GDPR.

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

(3) Part IIA makes provision about the additional general rules on the processing of personal data under the Schengen Agreement.

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

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

(6) Part V makes provision about the Commissioner.

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

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

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

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

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

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

Electronic communication and service of notices.

4.(1) For the purposes of this Act any communication or notification which may be done in writing may be done by electronic means.

(2) Where reference is made in this Act to the receipt of a written notice or notification, unless otherwise proved, the notice or notification shall be deemed to have been received–

(a) where the notice or notification has been sent by facsimile, electronic communication or hand delivery, on the date of delivery by the sender;

(b) where the notice or notification has been sent by post, 3 days after posting by the sender.

Acting for another.

5.(1) Where a data subject is–

(a) an individual under the age of 13, any action which may be taken by the data subject by virtue of this Act may be taken by his parent or legal guardian;

(b) a person who lacks capacity within the meaning of Part 5 of the Mental Health Act 2016 any action which may be taken by the data subject by virtue of this Act may be taken by the person who may act on his behalf under the Mental Health Act 2016 in relation to the management of his property or affairs.

(2) The words “any action” in this section include the giving of consent.

PART II

General processing

Chapter 1

Scope and definitions

Processing to which this Part applies.

6.(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; and

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

Definitions of Part II.

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

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

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

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

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

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

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

(8) Section 2 includes definitions of other expressions used in this Part.

Chapter 2

The GDPR

Meaning of certain terms used in the GDPR

Meaning of "controller".

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

(a) subsection (2);

(b) section 199; and

(c) section 200.

(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.

Meaning of "public authority" and "public body".

9.(1) For the purposes of the GDPR, the following, and only the following, are "public authorities" and "public bodies" under Gibraltar law-

(a) government departments;

(b) a body or other person, that carries out functions of public administration;

(c) a body or other person, that exercises functions of a public nature;

(d) a body or other person, that provides public services; or

(e) a body or other person specified or described by the Minister in regulations, subject to subsections (2) and (3).

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

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

Lawfulness of processing

Lawfulness of processing: public interest etc.

10. 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 Parliament;

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

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

Child's consent in relation to information society services.

11. 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

Special categories of personal data and criminal convictions etc data.

12.(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, Gibraltar law 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 Gibraltar law 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 Gibraltar law only if it meets a condition in Part 1, 2 or 3 of Schedule 1.

(6) The Minister may by regulations-

(a) amend Schedule 1-

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

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

(b) consequentially amend this section.

(7) In regards to the processing of criminal convictions, a complete register of criminal convictions may be kept only by the Royal Gibraltar Police.

Special categories of personal data etc: supplementary.

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

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

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

(2) In Article 10 of the GDPR and section 12, 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

Right to protection of personal data.

14.(1) A person ("P") has the right to protection of personal data concerning him or her.

(2) Personal data must be processed fairly for specified purposes as set out in the GDPR, and in accordance with the provisions, exceptions and derogations, of this Act.

(3) The Commissioner shall be responsible for ensuring compliance with the rights contained the GDPR.

Limits on fees that may be charged by controllers.

15.(1) The Minister may, after consulting the Commissioner, specify, by way of regulations, 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 Commissioner may by notice-

(a) require controllers of a description specified in the regulations made under subsection (1), to produce and publish guidance about the fees that they charge in reliance on those provisions; and

(b) specify what the guidance must include.

Obligations of credit reference agencies.

16.(1) Where a controller is a credit reference agency, 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.

(2) 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 to rectify incorrect information.

Automated decision-making authorised by law: safeguards.

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

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

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

(b) similarly significantly affects the data subject.

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

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

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

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

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

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

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

(i) reconsider the decision, or

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

(5) If a request is made to a controller under subsection (4), the controller must, within the period described in Article 12(3) of the GDPR-

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

(b) comply with the request; and

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

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

(ii) the outcome of complying with the request.

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

(7) The Minister may by regulations make such further provision as the Minister considers appropriate to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with

the taking of qualifying significant decisions based solely on automated processing.

(8) Regulations under subsection (7) may amend this section.

Data subject access requests.

18.(1) An individual making a subject access request shall supply the data controller concerned with such information as he may reasonably require in order to satisfy himself of the identity of the individual and to locate any relevant personal data or information.

(2) Nothing in this section obliges a data controller to disclose personal data relating to an individual other than the individual making the request unless that individual has consented to the disclosure or cannot be identified from the data, save-

(a) where the circumstances are such that it would be reasonable for the data controller to conclude that, if any particulars identifying the other individual were omitted, the data could then be disclosed without his being thereby identified to the data subject, the data controller shall be obliged to disclose the data to the data subject with the omission of those particulars;

(b) as may be provided by regulations made under section 20; or

(c) where it would otherwise be reasonable in all the circumstances.

(3) Where a data controller has previously complied with a subject access request, the data controller is not obliged to comply with a subsequent identical or similar request by the same individual unless, in the opinion of the data controller, a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(4) In determining whether a reasonable interval of time has elapsed under subsection (3), regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

(5) A person shall not, in connection with-

(a) the recruitment of another person as an employer;

(b) the continued employment of another person; or

(c) a contract for the provision of services to him by another person,

require that other person to make a subject access request or to supply him with data relating to that other person obtained as a result of such a request.

(6) A person who contravenes subsection (5) shall be guilty of an offence.

Restrictions on data subject's rights

Exemptions etc.

19.(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 and 34 of the GDPR in specified circumstances, as allowed for by Article 6(3) and Article 23(1) of the GDPR;

(b) Part 2 makes provision restricting the application of rules contained in Articles 13 to 21 and 34 of the GDPR in specified circumstances, as allowed for by Article 23(1) of the GDPR;

(c) Part 3 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, IV, V and VII of the GDPR for reasons relating to freedom of expression, as allowed for by Article 85(2) of the GDPR;

(f) Part 6 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 the security of Gibraltar and with defence, see Chapter 3 of this Part and the exemption in section 28.

Power to make further exemptions etc by regulations.

20.(1) The following powers to make provision altering the application of the GDPR may be exercised by way of regulations made by the Minister under this section-

(a) the power in Article 6(3) of the GDPR 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) of the GDPR 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) of the GDPR to provide for exemptions or derogations from certain Chapters of the GDPR where necessary to reconcile the protection of personal data with the freedom of expression and information.

(2) Regulations under this section may-

(a) amend Schedules 2 to 4-

(i) by adding or varying provisions, and

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

(b) consequentially amend section 15.

Accreditation of certification providers

Accreditation of certification providers.

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

(a) the Commissioner; or

(b) a national accreditation body appointed under subsection (9).

(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) A national accreditation body may only accredit a person as a certification provider where the Commissioner-

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

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

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

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

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

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

(8) In this section "certification provider" means a person who issues certification for the purposes of Article 42 of the GDPR.

(9) The Minister may appoint, by notice in the Gazette, a national accreditation body to undertake the responsibilities of accreditation of certification providers under this Act.

Transfers of personal data to third countries etc

Transfers of personal data to third countries etc.

22.(1) The Minister 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 Minister 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 Minister considers the restriction to be necessary for important reasons of public interest.

Specific processing situations

Processing for archiving, research and statistical purposes: safeguards.

23.(1) This section makes provision about-

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

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

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

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

(3) Such processing does not satisfy that requirement if the processing is carried out for the purposes of measures or decisions with respect to a

particular data subject, unless the purposes for which the processing is necessary include the purposes of approved medical research.

(4) In this section-

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

(a) a research ethics committee recognised or established by the United Kingdom's Health Research Authority under Chapter 2 of Part 3 of the Care Act 2014 passed by the Parliament at Westminster; or

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

(i) the Minister, or

(ii) the Gibraltar Health Authority.

(5) The Minister may by regulations amend the meaning of "approved medical research" for the purposes of this section.

Minor definition

Meaning of "court".

24. Section 7(1) (terms used in this Chapter to have the same meaning as in the GDPR) does not apply to references in this Chapter to a court and, accordingly, such references do not include a tribunal.

CHAPTER 3

OTHER GENERAL PROCESSING

Scope

Processing to which this Chapter applies.

25.(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 III (law enforcement processing) or Part IV (intelligence services processing) applies.

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

(3) In this section-

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

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

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

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

Application of the GDPR

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

26.(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 Gibraltar.

(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.

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

27.(1) The Minister 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 Minister considers appropriate.

(2) In this section, "GDPR regulations" means regulations made under Gibraltar law to 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 V to VII, in so far as they apply in relation to the applied GDPR.

Exemptions etc

Security of Gibraltar and defence exemption.

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

(a) the purpose of safeguarding the security of Gibraltar; 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 V of this Act-

(i) in section 124 (general functions of the Commissioner), subsections (3) and (8),

(ii) in section 124, subsection (9), so far as it relates to Article 58(2)(i) of the applied GDPR,

(iii) section 128 (inspection in accordance with international obligations);

(h) in Part VI of this Act-

(i) sections 150 to 160 and Schedule 15 (Commissioner's notices and powers of entry and inspection),

(ii) sections 175 to 178 (offences relating to personal data);

(i) in Part VII of this Act, section 189 (representation of data subjects with their authority).

Security of Gibraltar: certificate.

29.(1) Subject to subsection (3), a certificate signed by a Minister certifying that exemption from all or any of the provisions listed in section 28(2) is, or at any time was, required in relation to any personal data for the purpose of safeguarding the security of Gibraltar 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 Magistrate's Court against the certificate.

(4) If, on an appeal under subsection (3), the Magistrate's Court 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 Magistrate's Court 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 Magistrate's Court on the ground that the certificate does not apply to the personal data in question.

(6) 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 Magistrate's Court 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 as a true copy of a certificate issued by that Minister under subsection (1) is in any legal proceedings, evidence of that certificate.

(10) The power conferred by subsection (1) on a Minister is also exercisable by the Attorney General.

Security of Gibraltar and defence: modifications to Articles 9 and 32 of the applied GDPR.

30.(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 the security of Gibraltar 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 the security of Gibraltar; 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 IIA

Additional General Rules on the Processing of Personal Data Under the Schengen Agreement

Additional provisions for the processing of personal data under the Schengen Agreement.

31.(1) Subject to subsection (2), personal data communicated under the Schengen Agreement shall be used solely for the purposes for which the Schengen Agreement stipulates the personal data may be communicated for, and the transmission or receipt of that data must be recorded both in the source data file and in the data file in which it is entered.

(2) Personal data communicated under the Schengen Agreement may be used for a purpose other than that for which it was communicated where prior authorisation is sought from and approved by the authority which communicated the personal data.

(3) Where the Competent Authority receives approval from a Schengen State for the use of personal data communicated by it for a purpose other than that referred to in subsection (1), the use of that data shall be subject to the provisions of this Act and any other applicable Gibraltar law.

(4) Where the competent authority receives a request from a Schengen State for an authorisation to use personal data communicated to it for a purpose other than the purpose for which it originally sent the personal data, the competent authority may only grant such an authorisation in so far as Gibraltar law permits.

Designated users of the personal data communicated under Schengen Agreement.

32. Data referred to in section 31 may only be used by the–

(a) judicial authorities; and

(b) departments and authorities,

carrying out tasks or performing duties in connection with the purposes referred to in section 31.

Additional duties with respect to accuracy and improper communications.

33.(1) Where data is communicated pursuant to the Schengen Agreement the sender of that data must ensure the accuracy thereof.

(2) Where data controller has established, either on its own initiative or further to a request by the data subject that data has been provided that is inaccurate or should not have been communicated, the data controller must immediately inform the recipients.

(3) Where the data controller is the recipient of data from a Schengen State and the data controller is notified that the data is inaccurate or should not have been provided the data controller must correct or destroy the data, or indicate that the data is inaccurate or was unlawfully communicated.

(4) Nothing in this section shall be construed as a derogation from the protections provided elsewhere in this Act.

Additional duties in certain circumstances.

34. Where, in cases other than those governed by articles 126(1) and 127(1) of the Schengen Agreement, personal data is communicated to another Schengen State pursuant to the Schengen Agreement, article 126(3), with the exception of subparagraph (e), shall apply, in addition to the following requirements–

(a) a written record shall be kept of the transmission and receipt of personal data (unless such a record is not necessary given the use of the data, in particular if it is not used or is used only very briefly);

(b) where the recipient is in Gibraltar he shall ensure, in the use of communicated data, a level of protection at least equal to that laid down in this Act for the use of similar data;

(c) the decision concerning whether and under what conditions the data subject shall, at his request, be provided information concerning communicated data relating to him shall be governed by the provisions of this Act if the request was addressed to someone in Gibraltar.

Communication of personal data under the Schengen Agreement - police co-operation.

35.(1) Without prejudice to articles 126 and 127 of the Schengen Agreement, the communication of personal data between Schengen States under articles 39, 44, 46 and 47 of the Schengen Agreement shall be protected in accordance with the principles of Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector.

(2) In addition to subsection (1), the communication of personal data between Schengen States under article 46 of the Schengen Agreement and received in Gibraltar shall be afforded the following apply–

(a) the data must be used solely for the purposes indicated by and in compliance with the conditions laid down by the Schengen State sending the personal data;

(b) the data may only be communicated to police forces and police authorities;

(c) the data may not be communicated to authorities other than those specified in paragraph (b) without the prior authorisation of the Schengen State which sent the personal data; and

(d) when requested by the Schengen State which sent the personal data, the authority which received the data shall provide information regarding the use made of the personal data and the results obtained.

Liaison officers.

36.(1) Subject to subsection (2), the provisions of Title VI of the Schengen Agreement on the Protection of Personal Data shall not apply to a liaison officer as described in article 47 of the Schengen Agreement.

(2) The provisions of Title VI of the Schengen Agreement on the Protection of Personal Data shall apply to a liaison officer, as described in article 47 of the Schengen Agreement, where the liaison officer communicates such personal data to the Schengen State which seconded the officer to Gibraltar.

Disapplication of Act in certain cases.

37. This Act shall not apply to data communicated pursuant to Chapters 2 to 5 of Title III of the Schengen Agreement.".

Part III

LAW ENFORCEMENT PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

Scope

Processing to which this Part applies.

38.(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.

Definitions

Meaning of "competent authority".

39.(1) In this Part, "competent authority" means-

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

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

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

(3) The Minister may by regulations amend Schedule 7-

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

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

(4) Regulations under subsection (3) which make provision of the kind described in subsection (3)(a) may also make consequential amendments of section 82(4)(b).

(5) In this section-

"intelligence service" means a body falling under the defintion of intelligence service at Part IV;

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

"The law enforcement purposes".

40. 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.

Meaning of "controller" and "processor".

41.(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).

Other definitions.

42.(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 or the United Kingdom.

(8) Section 2 includes definitions of other expressions used in this Part.

CHAPTER 2

PRINCIPLES

Overview and general duty of controller.

43.(1) This Chapter sets out the six data protection principles as follows-

(a) section 44(1) sets out the first data protection principle (requirement that processing be lawful and fair);

(b) section 45(1) sets out the second data protection principle (requirement that purposes of processing be specified, explicit and legitimate);

(c) section 46 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 47(1) sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

(e) section 48(1) sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 49 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) In addition-

(a) each of sections 44, 45, 47 and 48 makes provision to supplement the principle to which it relates; and

(b) sections 50 and 51 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.

The first data protection principle.

44.(1) The first data protection principle is that 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 following two cases-

(a) The first case is where-

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

(ii) at the time when the processing is carried out, the controller has an appropriate policy document in place as per section 51.

(b) the second case is where-

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

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

(iii) at the time when the processing is carried out, the controller has an appropriate policy document in place as per section 51.

(4) The Minister may by regulations amend Schedule 8 by-

(a) adding conditions;

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

(5) 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.

The second data protection principle.

45.(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) subject to subsections (2) and (3), personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

(2) 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.

(3) 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.

The third data protection principle.

46. 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.

The fourth data protection principle.

47.(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.

The fifth data protection principle.

48.(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.

The sixth data protection principle.

49. 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).

Safeguards: archiving.

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

(a) for archiving purposes in the public interest;

(b) for scientific or historical research purposes; or

(c) for statistical purposes.

(2) The processing is not permitted if-

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

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

Safeguards: sensitive processing.

51.(1) This section applies for the purposes of section 44(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 43(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 70(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 70(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 44 (lawfulness of processing); and

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

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

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

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

CHAPTER 3

RIGHTS OF THE DATA SUBJECT

Overview and scope

Overview and scope.

52.(1) This Chapter-

(a) imposes general duties on the controller to make information available (see section 53);

(b) confers a right of access by the data subject (see section 54);

(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 55 to 57);

(d) regulates automated decision-making (see sections 58 and 59);

(e) makes supplementary provision (see sections 60 to 63).

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

(3) Sections 53 to 57 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

Information: controller's general duties.

53.(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 78 to 80);

(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,

(ii) rectification of personal data, and

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

(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 the security of Gibraltar;

(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 60;

(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 172.

(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

Right of access by the data subject.

54.(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) The information to be provided under subsection (1)(b) 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 as per section 55, and

(ii) erasure of personal data or the restriction of its processing as per section 56;

(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 defined at section 63.

(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 the security of Gibraltar;

(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 60;

(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 172.

(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

Right to rectification.

55.(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.

Right to erasure or restriction of processing.

56.(1) The controller must erase personal data without undue delay where-

(a) the processing of the personal data would infringe sections 44, 45(1) to (3), 46, 47(1), 48(1), 49, 50 or 51; 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 55 or in any other way, but it is not possible to ascertain whether it is accurate or not, the controller must restrict its processing.

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

Rights under section 55 or 56: supplementary.

57.(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; or

(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 60,

(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 172.

(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 as defined in section 63.

(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 the security of Gibraltar;

(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 172.

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

(6) The controller must-

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

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

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

(8) In subsection (7), the reference to a competent authority includes, in addition to a competent authority within the meaning of this Part, any person that is a competent authority for the purposes of the Law Enforcement Directive in a Member State or 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 56(3), the controller must inform the data subject before lifting the restriction.

Automated individual decision-making

Right not to be subject to automated decision-making.

58.(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.

Automated decision-making authorised by law: safeguards.

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

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

(b) it is required or authorised by law.

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

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

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

(i) reconsider the decision, or

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

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

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

(b) comply with the request; and

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

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

(ii) the outcome of complying with the request.

(4) The Minister may by regulations amend this section or make such further provision as the Minister 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) In this section "significant decision" has the meaning given by section 58(2).

Supplementary

Exercise of rights through the Commissioner.

60.(1) This section applies where a controller-

(a) restricts under section 53(4) the information provided to the data subject under section 53(2) (duty of the controller to give the data subject additional information);

(b) restricts under section 54(4) the data subject's rights under section 54(1) (right of access); or

(c) refuses a request by the data subject for rectification under section 55 or for erasure or restriction of processing under section 56.

(2) The data subject may-

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

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

(3) The Commissioner must take such steps as appear to the Commissioner to be appropriate to respond to a request under subsection (2) (which may include the exercise of any of the powers conferred by sections 150 and 153).

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

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

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

(5) The Commissioner must also inform the data subject of the data subject's right to apply to a court under section 172.

(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 VI.

Form of provision of information etc.

61.(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 54, 55, 56 or 59, 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 54, 55 or 56, 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 62, 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 54 to 59.

Manifestly unfounded or excessive requests by the data subject.

62.(1) Where a request from a data subject under section 54, 55, 56 or 59 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 54, 55, 56 or 59 is manifestly unfounded or excessive, it is for the controller to show that it is.

(4) The Minister may, after consulting the Commissioner, specify, by way of regulations, limits on the fees that a controller may charge in accordance with subsection (1)(a).

(5) The Commissioner may by notice-

(a) require controllers of a description specified in regulations made under subsection (4), to produce and publish guidance about the fees that they charge in reliance on those provisions; and

(b) specify what the guidance must include.

Meaning of "applicable time period".

63.(1) This section defines "the applicable time period" for the purposes of sections 54(3)(b) and 57(2)(b).

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

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

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

(b) when the controller receives the information, if any, requested in connection with a request under section 61(4);

(c) when the fee, if any, charged in connection with the request under section 62 is paid.

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

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

CHAPTER 4

CONTROLLER AND PROCESSOR

Overview and scope

Overview and scope.

64.(1) This Chapter-

(a) sets out the general obligations of controllers and processors (see sections 65 to 74);

(b) sets out specific obligations of controllers and processors with respect to security (see section 75);

(c) sets out specific obligations of controllers and processors with respect to personal data breaches (see sections 76 and 77);

(d) makes provision for the designation, position and tasks of data protection officers (see sections 78 to 80).

(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

General obligations of the controller.

65.(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.

Data protection by design and default.

66.(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.

Joint controllers.

67.(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.

Processors.

68.(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 subprocessors.

(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.

Processing under the authority of the controller or processor.

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

(a) on instructions from the controller; or

(b) to comply with a legal obligation.

Records of processing activities.

70.(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 75.

(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 68(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 75.

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

Logging.

71.(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.

Co-operation with the Commissioner.

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

Data protection impact assessment.

73.(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.

Prior consultation with the Commissioner.

74.(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 73 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 73; and

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

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

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

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

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

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

(b) provide reasons for the delay.

Obligations relating to security

Security of processing.

75.(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.

Notification of a personal data breach to the Commissioner.

76.(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 a Member State or the United Kingdom, 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

Communication of a personal data breach to the data subject.

77.(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 76 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 the security of Gibraltar;

(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 61(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

Designation of a data protection officer.

78.(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 80.

(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.

Position of data protection officer.

79.(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 80; 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 80;

(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 80.

(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.

Tasks of data protection officer.

80.(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 73 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 74, 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

Overview and interpretation.

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

(a) sections 82 to 85 set out the general conditions that apply;

(b) section 86 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 87 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;

"Member State" shall, unless otherwise stated, include the United Kingdom.

General principles for transfers

General principles for transfers of personal data.

82.(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, 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 as per section 83;

(b) if not based on an adequacy decision, is based on there being appropriate safeguards as per section 84; or

(c) if not based on an adequacy decision or on there being appropriate safeguards, is based on special circumstances as per section 85.

(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 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 86 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.

Transfers on the basis of an adequacy decision.

83. 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 European Commission no longer considers there to be an adequate level of protection of personal data.

Transfers on the basis of appropriate safeguards.

84.(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.

Transfers on the basis of special circumstances.

85.(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) 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

Transfers of personal data to persons other than relevant authorities.

86.(1) The additional conditions referred to in section 82(4)(b)(ii) are the following four conditions-

(a) 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;

(b) 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;

(c) 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;

(d) 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.

(2) 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.

(3) 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.

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

Subsequent transfers

Subsequent transfers.

87.(1) Where personal data is transferred in accordance with section 82, 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, 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

Security of Gibraltar: certificates by the Minister.

88.(1) A Minister may issue a certificate certifying, for the purposes of section 53(4), 54(4), 57(3) or 77(7), that a restriction is a necessary and proportionate measure to protect the security of Gibraltar.

(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 53(4), 54(4), 57(3) or 77(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 the security of Gibraltar.

(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 Magistrate's Court against the certificate.

(6) If, on an appeal under subsection (5), the Magistrate's Court 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 Magistrate's Court 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 Magistrate's Court on the ground that the restriction does not fall within that description.

(8) 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 Magistrate's Court 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 as a true copy of a certificate issued by that Minister under subsection (1) is in any legal proceedings, evidence of that certificate.

(12) The power conferred by subsection (1) on a Minister is exercisable also by the Attorney General.

(13) No power conferred by any provision of Part VI 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.

Special processing restrictions.

89.(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 or 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 Gibraltar 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) If any restrictions exist as referred under subsection (3), 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 or 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 Member State or the United Kingdom informs the controller, in accordance with any law of that Member State or the United Kingdom, 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 referred to in subsection (6).

Reporting of infringements.

90.(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 such 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.

Part IV

INTELLIGENCE SERVICES PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

Scope

Processing to which this Part applies.

91.(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 any body or person approved by the Minister to conduct intelligence services processing of personal data in Gibraltar.

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

(4) The Minister may by regulations amend the definition of "intelligence service" in subsection (3)-

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

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

(5) The Minister may by regulations establish a process by which bodies or persons may apply to carry out intelligence services processing of personal data in Gibraltar.

Definitions

Meaning of "controller" and "processor".

92.(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.

Other definitions.

93.(1) In this Part-

"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;

"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;

"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;

"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;

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

(2) Section 2 includes definitions of other expressions used in this Part.

CHAPTER 2

PRINCIPLES

Overview

Overview.

94.(1) This Chapter sets out the six data protection principles as follows-

(a) section 95 sets out the first data protection principle (requirement that processing be lawful, fair and transparent);

(b) section 96 sets out the second data protection principle (requirement that the purposes of processing be specified, explicit and legitimate);

(c) section 97 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 98 sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

(e) section 99 sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 100 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) Each of sections 95, 96 and 100 makes provision to supplement the principle to which it relates.

The data protection principles

The first data protection principle.

95.(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 Minister may by regulations amend Schedule 10-

(a) by adding conditions;

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

(4) 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.

(5) For the purposes of subsection (4), 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 Gibraltar.

(6) 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.

The second data protection principle.

96.(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) Subsection (1)(b) 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.

The third data protection principle.

97. 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.

The fourth data protection principle.

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

The fifth data protection principle.

99. 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.

The sixth data protection principle.

100.(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

Overview.

101.(1) This Chapter sets out the rights of the data subject as follows-

(a) section 102 deals with the information to be made available to the data subject;

(b) sections 103 and 104 deal with the right of access by the data subject;

(c) sections 105 and 106 deal with rights in relation to automated processing;

(d) section 107 deals with the right to information about decision-making;

(e) section 108 deals with the right to object to processing;

(f) section 109 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

Right to information.

102.(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.

Right of access.

103.(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) The information to be provided under subsection (1)(b) 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 as per section 109;

(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 Minister may by regulations-

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

(b) specify the maximum amount of a fee.

(5) Where a controller-

(a) reasonably requires further information-

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

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

(b) has informed that individual of that requirement,

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

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

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

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

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

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

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

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

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

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

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

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

(a) promptly; and

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

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

(12) A court may make an order under subsection (11) in relation to a joint controller whose responsibilities are determined in an arrangement under section 113 only if the controller is responsible for compliance with the obligation to which the order relates.

(13) The jurisdiction conferred on a court by this section is exercisable by the Magistrate's Court.

(14) In this section-

"the applicable time period" means-

(a) the period of 1 month; or

(b) such longer period, not exceeding 3 months, as may be specified in regulations made by the Minister,

beginning with the relevant time;

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

(a) when the controller receives the request;

(b) when the fee, if any, is paid; and

(c) when the controller receives the information, if any, required under subsection (5) in connection with the request.

Right of access: supplementary.

104.(1) The controller must comply with the obligation imposed by section 103(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 103(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 103 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 103 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 103 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 103(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.

Right not to be subject to automated decision-making.

105.(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.

Right to intervene in automated decision-making.

106.(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 1 month beginning with receipt of the notification, request the controller-

(a) to reconsider the decision; or

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

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

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

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

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

Right to information about decision-making.

107.(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.

Right to object to processing.

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

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

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

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

(2) Where the controller-

(a) reasonably requires further information-

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

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

(b) has informed that individual of that requirement,

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

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

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

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

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

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

(6) A court may make an order under subsection (5) in relation to a joint controller whose responsibilities are determined in an arrangement under section 113 only if the controller is responsible for compliance with the obligation to which the order relates.

(7) The jurisdiction conferred on a court by this section is exercisable by the Magistrate's Court.

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

(a) when the controller receives the notice; or

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

Rights to rectification and erasure.

109.(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 95 to 100, the court may order the controller to erase that data without undue delay.

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

(4) If-

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

(b) the court is satisfied that the controller is not able to ascertain whether the data is accurate or not, the court may, instead of ordering the controller to rectify or erase the personal data, order the controller to restrict its processing without undue delay.

(5) A court may make an order under this section in relation to a joint controller whose responsibilities are determined in an arrangement under section 113 only if the controller is responsible for carrying out the rectification, erasure or restriction of processing that the court proposes to order.

(6) The jurisdiction conferred on a court by this section is exercisable by the Magistrate's Court.

CHAPTER 4

CONTROLLER AND PROCESSOR

Overview

Overview.

110. This Chapter sets out-

(a) the general obligations of controllers and processors (see sections 111 to 115);

(b) specific obligations of controllers and processors with respect to security (see section 116);

(c) specific obligations of controllers and processors with respect to personal data breaches (see section 117).

General obligations

General obligations of the controller.

111. 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.

Data protection by design.

112.(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.

Joint controllers.

113.(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.

Processors.

114.(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.

Processing under the authority of the controller or processor.

115. 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

Security of processing.

116.(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

Communication of a personal data breach.

117.(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) 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 GIBRALTAR

Transfers of personal data outside Gibraltar.

118.(1) A controller may not transfer personal data to-

(a) a country or territory outside Gibraltar; 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 for the purposes of the controller's statutory functions.

CHAPTER 6

EXEMPTIONS

Security of Gibraltar.

119.(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 the security of Gibraltar.

(2) The provisions are-

(a) Chapter 2 (the data protection principles), except section 95(1)(a) and (2) and Schedules 9 and 10;

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

(c) in Chapter 4, section 117 (communication of a personal data breach to the Commissioner);

(d) in Part V-

(i) section 128 (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 VI-

(i) sections 150 to 160 and Schedule 15 (Commissioner's notices and powers of entry and inspection);

(ii) sections 175 to 177 (offences relating to personal data);

(iii) sections 179 to 181 (provision relating to the special purposes).

Security of Gibraltar: certificate.

120.(1) Subject to subsection (3), a certificate signed by a Minister certifying that exemption from all or any of the provisions mentioned in section 119(2) is, or at any time was, required for the purpose of safeguarding the security of Gibraltar 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 Magistrate's Court against the certificate.

(4) If on an appeal under subsection (3), the Magistrate's Court 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 Magistrate's Court 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

Magistrate's Court on the ground that the certificate does not apply to the personal data in question.

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

(7) On an appeal under subsection (5), the Magistrate's Court 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 as a true copy of a certificate issued by that Minister under subsection (1) is in any legal proceedings, evidence of that certificate.

(10) The power conferred by subsection (1) on a Minister is also exercisable by the Attorney General.

Other exemptions.

121. Schedule 11 provides for further exemptions.

Power to make further exemptions.

122. The Minister may by regulations amend Schedule 11-

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

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

Part V

THE COMMISSIONER

The Commissioner

The Commissioner.

123.(1) There shall be a Data Protection Commissioner ("the Commissioner") who shall be independent in the exercise of his functions under this Act.

(2) The Commissioner shall be the Gibraltar Regulatory Authority, who shall perform the functions conferred by this Act and any regulations enacted under it.

(3) The Minister may by regulations amend subsection (2).

(4) Schedule 12 makes provision about the Commissioner's powers.

General functions

General functions under the GDPR and safeguards.

124.(1) The Commissioner is to be the supervisory authority in Gibraltar 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 150.

(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 153.

(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 160); 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 153.

(8) The following powers are exercisable only by giving an enforcement notice under section 155-

(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 162.

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

Other general functions.

125.(1) The Commissioner-

(a) is to be the supervisory authority in Gibraltar for the purposes of Article 41 of the Law Enforcement Directive; and

(b) is to continue to be the designated authority in Gibraltar 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.

Competence in relation to courts etc.

126. 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

Co-operation and mutual assistance.

127.(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).

Inspection of personal data in accordance with international obligations.

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

(2) The power under subsection (1) is exercisable only if the personal data-

(a) is processed wholly or partly by automated means; or

(b) is processed otherwise than by automated means and forms part of a filing system or is intended to form part of a filing system.

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

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

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

(6) It is an offence-

(a) intentionally to obstruct a person exercising the power under subsection (1); or

(b) to fail without reasonable excuse to give a person exercising that power any assistance the person may reasonably require.

Further international role.

129.(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 Minister directs the Commissioner to carry out for the purpose of enabling the government to give effect to an international obligation of Gibraltar.

(4) 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 or the United Kingdom.

Codes of practice

Data sharing code.

130.(1) The Commissioner may 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 may consult such of the following as the Commissioner considers appropriate-

(a) trade associations;

(b) data subjects;

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

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

(5) In this section-

"good practice in the 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.

Direct marketing code.

131.(1) The Commissioner may 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 may consult such of the following as the Commissioner considers appropriate-

(a) trade associations;

(b) data subjects;

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

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

(5) In this section-

"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.

Age-appropriate design code.

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

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

(3) Before preparing a code or amendments under this section, the Commissioner may consult such persons as the Commissioner considers appropriate, including-

(a) children;

(b) parents;

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

(d) child development experts; and

(e) trade associations.

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

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

(b) to the United Nations Convention on the Rights of the Child.

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

(6) In this section-

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

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

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

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

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

"the United Nations Convention on the Rights of the Child" means the Convention on the Rights of the Child adopted by the General Assembly of the United Nations on 20 November 1989 (including any Protocols to that Convention).

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

133.(1) When a code is prepared under section 130, 131 or 132, the Commissioner must submit a final version to the Minister.

(2) The Commissioner must then issue the code, and it will come into force at the end of the period of 21 days beginning with the day on which it is issued.

(3) Where an amendment of a code is issued, the Commissioner must publish-

(a) the amendment; or

(b) the code as amended by it.

(4) The Commissioner must keep under review each code issued under this Act.

(5) Where the Commissioner becomes aware that the terms of such a code could result in a breach of an international obligation of Gibraltar, the Commissioner must exercise the power under section 130(2), 131(2) or 132(2) with a view to remedying the situation.

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

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

(2) A code issued under this Act, 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 this Act 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 relating to the data protection legislation, the Commissioner must take into account a provision of a code issued under this Act 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.

Other codes of practice.

135.(1) The Commissioner may encourage trade associations and other bodies representing categories of data controllers to prepare codes of practice to be complied with by those categories in processing personal data.

(2) Where a Code of Practice has been prepared by a trade association or other body representing a category of data controller it may be submitted to the Commissioner for his views and if, after conducting such consultations with interested parties and interested data subjects as appears appropriate to him-

(a) he considers that the Code of Practice provides appropriate protections for the rights of data subjects under this Act, he shall approve the code and encourage its dissemination to the data controllers and data subjects concerned; and

(b) in any event the Commissioner shall notify the authors of the Code of Practice of his decision to approve or not approve the Code.

(3) In proceedings before any court or tribunal any provision of a Code of Conduct or Practice approved by, or written by, the Commissioner which is relevant to the proceedings may be taken into account in determining the issues.

(4) The Minister 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.

(5) 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.

(6) 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.

(7) In this section-

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

others, including compliance with the requirements of the data protection legislation;

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

Consensual audits

Consensual audits.

136.(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 139.

Records of certificates relating to the security of Gibraltar

Records of certificates relating to the security of Gibraltar.

137.(1) A Minister who issues a certificate under section 29, 88 or 120 must send a copy of the certificate to the Commissioner.

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

(3) The record must contain-

(a) the name of the Minister who issued the certificate;

(b) the date on which the certificate was issued; and

(c) subject to subsection (4), the text of the certificate.

(4) The Commissioner must not publish the text, or a part of the text, of the certificate if-

(a) the Minister determines that publishing the text or that part of the text-

(i) would be against the interests of the security of Gibraltar,

(ii) would be contrary to the public interest, or

(iii) might jeopardise the safety of any person; and

(b) the Minister has notified the Commissioner of that determination.

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

(6) If a Minister revokes a certificate issued under section 29, 88 or 120, the Minister must notify the Commissioner.

Register of data protection officers

Register of data protection officers.

138. The Commissioner must establish and maintain a register of data protection officers, which shall be available to the public.

Information provided to the Commissioner

Disclosure of information to the Commissioner.

139. No enactment or rule of law prohibiting or restricting the disclosure of information-

(a) shall preclude a person from furnishing to the Commissioner any information which is necessary or expedient for the performance by the Commissioner of his functions;

(b) save that paragraph (a) does not apply to information which is, or at the time was, kept for the purpose of safeguarding the security of Gibraltar or information which is privileged from disclosure in court proceedings.

Confidentiality of information.

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

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

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

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

unless the disclosure is made with lawful authority.

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

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

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

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

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

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

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

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

Guidance about privileged communications.

141.(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) 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.

(4) In subsection (3)-

(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 (3)(a)(ii) or in subsection (3)(b)(ii) and (iii).

Fees

Fees for services.

142. 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.

Manifestly unfounded or excessive requests by data subjects etc.

143.(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.

Guidance about fees.

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

(a) section 142 or 143; or

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

(2) Before publishing the guidance, the Commissioner must consult the Minister.

Charges

Charges payable to the Commissioner by controllers.

145.(1) The Minister 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 Minister 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 in relation to data protection;

(b) any expenses of the Minister in respect of the Commissioner so far as attributable to those functions;

(c) to the extent that the Minister 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 Minister considers appropriate, expenses incurred by the Minister in respect of the inclusion of any officers or staff of the Commissioner in any public service pension scheme.

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

(6) The Minister 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.

Regulations under section 145: supplementary.

146.(1) Before making regulations under section 145(1) or (6), the Minister must consult such representatives of persons likely to be affected by the regulations as the Minister thinks appropriate (see section 184).

(2) The Commissioner-

(a) must keep under review the working of regulations under section 145(1) or (6); and

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

Reports etc

Reporting to Parliament.

147.(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.

(4) A report prepared under this section may form part of the report to be prepared by the Commissioner under section 19 of the Gibraltar Regulatory Authority Act 2000.

Publication by the Commissioner.

148. 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.

Notices from the Commissioner.

149.(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 unincorporated-

(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 the person by other means, including by electronic means, with the person's consent.

(5) 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 Gibraltar.

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

PART VI

ENFORCEMENT

Information notices

Information notices.

150.(1) The Commissioner may, by written notice (an "information notice")-

(a) require a controller or processor to provide the Commissioner with information that the Commissioner reasonably requires for the purposes of carrying out the Commissioner's functions under the data protection legislation; or

(b) require any person to provide the Commissioner with information that the Commissioner reasonably requires for the purposes of-

(i) investigating a suspected failure of a type described in section 155(2) or a suspected offence under this Act, or

(ii) determining whether the processing of personal data is carried out by an individual in the course of a purely personal or household activity.

(2) An information notice must state-

(a) whether it is given under subsection (1)(a), (b)(i) or (b)(ii); and

(b) why the Commissioner requires the information.

(3) Subject to subsections (5) to (7) an information notice may-

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

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

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

(d) specify the place where the information must be provided.

(4) An information notice must provide information about the rights of appeal under section 168.

(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 when the notice is given.

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

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

(10) Section 2(2)(c) does not apply to the reference to the processing of personal data in subsection (1)(b).

Information notices: restrictions.

151.(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 179 with respect to the data or the processing has taken effect; or

(b) the Commissioner-

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

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

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

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

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

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

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

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

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

(c) for the purposes of such proceedings.

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

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

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

(a) this Act; or

(b) section 466 of the Crimes Act 2011 (false statutory declarations and other false statements).

(8) An oral or written statement provided by a person in response to an information notice may not be used in evidence against that person on a

prosecution for an offence under this Act (other than an offence under section 152) unless in the proceedings-

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

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

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

False statements made in response to an information notice.

152. 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.

Information orders.

152A.(1) This section applies if, on an application by the Commissioner, a court is satisfied that a person has failed to comply with a requirement of an information notice.

(2) The court may make an order requiring the person to provide to the Commissioner some or all of the following-

(a) information referred to in the information notice;

(b) other information which the court is satisfied the Commissioner requires, having regard to the statement included in the notice in accordance with section 150(2)(b).

(3) The order-

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

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

(c) may specify the place where the information must be provided.

Assessment notices

Assessment notices.

153.(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) Subject to subsection (6) to (8), 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.

(5) An assessment notice must provide information about the rights of appeal under section 168.

(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 when the notice is given.

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

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

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

Assessment notices: restrictions.

154.(1) An assessment notice does not require a person to do something to the extent that requiring the person to do it would involve an infringement of Parliamentary privilege.

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

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

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

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

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

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

(c) for the purposes of such proceedings.

(4) In subsections (2) and (3)-

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

(b) references to a communication include-

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

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

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

Destroying or falsifying information and documents etc.

154A.(1) This section applies where a person-

(a) has been given an information notice requiring the person to provide the Commissioner with information; or

(b) has been given an assessment notice requiring the person to direct the Commissioner to a document, equipment or other material or to assist the Commissioner to view information.

(2) It is an offence for the person-

(a) to destroy or otherwise dispose of, conceal, block or, where relevant, falsify all or part of the information, document, equipment or material; or

(b) to cause or permit the destruction, disposal, concealment, blocking or, where relevant, falsification of all or part of the information, document, equipment or material,

with the intention of preventing the Commissioner from viewing, or being provided with or directed to, all or part of the information, document, equipment or material.

(3) It is a defence for a person charged with an offence under subsection (2) to prove that the destruction, disposal, concealment, blocking or falsification would have occurred in the absence of the person being given the notice.

Enforcement notices

Enforcement notices.

155.(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;

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

(c) both paragraphs (a) and (b) together.

(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 III or Chapter 2 of Part IV of this Act (principles of processing);

(b) a provision of Articles 12 to 22 of the GDPR or Part III or IV 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 76, 77 or 117 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 82 to 87 or 118 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 145.

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

(9) Regulations under this section-

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

(b) may amend this section and sections 156 to 159.

Enforcement notices: supplementary.

156.(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 155(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 155(2), the Commissioner's power under section 155(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) Subject to subsections (6) to (8), 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.

(5) An enforcement notice must provide information about the rights of appeal under section 168.

(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 when the notice is given.

(9) In this section, "specified" means specified in an enforcement notice.

Enforcement notices: rectification and erasure of personal data etc.

157.(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 55, 56 or 109 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 47(1) of this Act; or

(c) section 98 of this Act.

Enforcement notices: restrictions.

158.(1) The Commissioner may not give a controller or processor an enforcement notice in reliance on section 155(2) with respect to the processing of personal data for the special purposes unless-

(a) a determination under section 179 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 155(2) which is of substantial public importance; and

(b) the controller or processor has been given notice of the application for leave in accordance with rules of court or the case is urgent.

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

(4) In the case of a joint controller in respect of the processing of personal data to which Part III or IV applies whose responsibilities for compliance with that Part are determined in an arrangement under section 67 or 113, the Commissioner may only give the controller an enforcement notice in reliance on section 155(2) if the controller is responsible for compliance with the provision, requirement or principle in question.

Enforcement notices: cancellation and variation.

159.(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

Powers of entry and inspection.

160. Schedule 15 makes provision about powers of entry and inspection.

Authorised officers.

161.(1) In this section "authorised officer" means a person authorised in writing by the Commissioner to exercise, for the purposes of this Act, the powers conferred by this section.

(2) Authorised officers shall have such powers to enter, inspect, search premises, examine, operate and test any data equipment, inspect and copy or extract information from data, or inspect and copy or take extracts from such material and require persons to disclose or produce material or information as is necessary or expedient in the opinion of the Commissioner for the performance by the Commissioner of his functions.

(3) A person who obstructs or impedes an authorised officer in the exercise of a power provided by this Act, or, without reasonable excuse, does not comply with a requirement under this section or who in purported compliance with such a requirement gives information to an authorised officer that he knows to be false or misleading in a material respect, shall be guilty of an offence.

Penalties

Penalty notices.

162.(1) If the Commissioner is satisfied that a person-

(a) has failed or is failing as described in section 155(2), (3), (4) or (5); or

(b) has failed to comply with an information notice, an assessment notice or an enforcement notice,

the Commissioner may, by written notice (a “penalty notice”), require the person to pay to the Commissioner an amount in sterling specified in the notice.

(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant-

(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR;

(b) to the extent that the notice concerns another matter, the matters listed in subsection (3).

(3) The matters referred to in subsection (2) are-

(a) the nature, gravity and duration of the failure;

(b) the intentional or negligent character of the failure;

(c) any action taken by the controller or processor to mitigate the damage or distress suffered by data subjects;

(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor in accordance with section 66, 75, 112 or 116;

(e) any relevant previous failures by the controller or processor;

(f) the degree of co-operation with the Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;

(g) the categories of personal data affected by the failure;

(h) the manner in which the infringement became known to the Commissioner, including whether, and if so to what extent, the controller or processor notified the Commissioner of the failure;

(i) the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;

(j) adherence to approved codes of conduct or certification mechanisms;

(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure, whether directly or indirectly;

(l) whether the penalty would be effective, proportionate and dissuasive.

(4) Subsections (2) and (3) do not apply in the case of a decision or determination relating to a failure described in section 155(5).

(5) Schedule 16 makes further provision about penalty notices, including provision requiring the Commissioner to give a notice of intent to impose a penalty and provision about payment, variation, cancellation and enforcement.

(6) The Minister may by regulations-

(a) confer power on the Commissioner to give a penalty notice in respect of other failures to comply with the data protection legislation; and

(b) provide for the maximum penalty that may be imposed in relation to such failures to be either the standard maximum amount or the higher maximum amount.

(7) Regulations under this section-

(a) may make provision about the giving of penalty notices in respect of the failure; and

(b) may amend this section and sections 163 to 165.

(8) In this section, "higher maximum amount" and "standard maximum amount" have the same meaning as in section 164.

Penalty notices: restrictions.

163.(1) The Commissioner may not give a controller or processor a penalty notice in reliance on section 155(2) with respect to the processing of personal data for the special purposes unless-

(a) a determination under section 179 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 155(2) which is of substantial public importance; and

(b) the controller or processor has been given notice of the application for leave in accordance with rules of court or the case is urgent.

(3) The Commissioner may not give a controller or processor a penalty notice with respect to the processing of personal data where the purposes and manner of the processing are determined by or on behalf of Parliament.

(4) In the case of a joint controller in respect of the processing of personal data to which Part III or IV applies whose responsibilities for compliance with that Part are determined in an arrangement under section 67 or 113, the

Commissioner may only give the controller a penalty notice in reliance on section 155(2) if the controller is responsible for compliance with the provision, requirement or principle in question.

Maximum amount of penalty.

164.(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 III 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 44, 45, 46, 47(1), 48(1), 49, 53, 54, 55, 56, 57, 58, 61, 62, 82, 83, 84, 85, 86 or 87, the higher maximum amount; and

(b) otherwise, the standard maximum amount.

(3) In relation to an infringement of a provision of Part IV 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 95, 96, 97, 98, 99, 100, 102, 103, 109 or 118, the higher maximum amount; and

(b) otherwise, the standard maximum amount.

(4) In relation to a failure to comply with an information notice, an assessment notice or an enforcement notice, the maximum amount of the penalty that may be imposed by a penalty notice is the higher maximum amount.

(5) The "higher maximum amount" is-

(a) in the case of an undertaking, 20 million Euros or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher; or

(b) in any other case, 20 million Euros.

(6) The "standard maximum amount" is-

(a) in the case of an undertaking, 10 million Euros or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher; or

(b) in any other case, 10 million Euros.

(7) The maximum amount of a penalty in sterling must be determined by applying the spot rate of exchange set by the Bank of England on the day on which the penalty notice is given.

Fixed penalties for non-compliance with charges regulations.

165.(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 145.

(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 Minister; and

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

Amount of penalties: supplementary.

166.(1) For the purposes of Article 83 of the GDPR and section 164, the Minister 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 164 and section 165, the Minister may by regulations provide that a period is or is not a financial year.

Guidance

Guidance about regulatory action.

167.(1) The Commissioner must produce and publish guidance about how the Commissioner proposes to exercise the Commissioner's functions in connection with-

(a) assessment notices;

(b) enforcement notices; and

(c) penalty notices.

(2) The Commissioner may produce and publish guidance about how the Commissioner proposes to exercise the Commissioner's other functions under this Part.

(3) In relation to assessment notices, the guidance must include-

(a) provision specifying factors to be considered in determining whether to give an assessment notice to a person;

(b) provision specifying descriptions of documents or information that-

(i) are not to be examined or inspected in accordance with an assessment notice, or

(ii) are to be so examined or inspected only by a person of a description specified in the guidance;

(c) provision about the nature of inspections and examinations carried out in accordance with an assessment notice;

(d) provision about the nature of interviews carried out in accordance with an assessment notice;

(e) provision about the preparation, issuing and publication by the Commissioner of assessment reports in respect of controllers and processors that have been given assessment notices.

(4) The guidance produced in accordance with subsection (3)(b) must include provisions that relate to-

(a) documents and information concerning an individual's physical or mental health;

(b) documents and information concerning the provision of social care for an individual.

(5) In relation to penalty notices, the guidance must include-

(a) provision about the circumstances in which the Commissioner would consider it appropriate to issue a penalty notice;

(b) provision about the circumstances in which the Commissioner would consider it appropriate to allow a person to make oral representations about the Commissioner's intention to give the person a penalty notice;

(c) provision explaining how the Commissioner will determine the amount of penalties.

(6) The Commissioner-

(a) may alter or replace guidance produced under this section; and

(b) must publish any altered or replacement guidance.

(7) Before producing guidance under this section, including any altered or replacement guidance, the Commissioner must consult-

(a) the Minister; and

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

Appeals

Rights of appeal.

168.(1) A person who is given any of the following notices may appeal to the Magistrate's Court-

(a) an information notice;

(b) an assessment notice;

(c) an enforcement notice;

(d) a penalty notice;

(e) a penalty variation notice.

(2) A controller or processor on which a notice listed under subsection (1) has been served, who wants to appeal must do so within 28 days from the date on which the notice is served.

(3) Where a notice listed in subsection (1) contains a statement under section 150(7)(a), 153(8)(a) or 156(8)(a) (urgency), the person given the notice may appeal against-

(a) the Commissioner's decision to include the statement in the notice; or

(b) the effect of its inclusion as respects any part of the notice,

whether or not the person appeals against the notice.

(4) A person who is given an enforcement notice may appeal to the Magistrate's Court against the refusal of an application under section 159 for the cancellation or variation of the notice.

(5) 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.

(6) Where a determination is made under section 179 in respect of the processing of personal data, the controller or processor may appeal to the Magistrate's Court against the determination.

Determination of appeals.

169.(1) Subsections (2) to (4) apply where a person appeals to the Magistrate's Court under section 168(1) or (5).

(2) The Magistrate's Court may review any determination of fact on which the notice or decision against which the appeal is brought was based.

(3) If the Magistrate's Court 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 Magistrate's Court must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.

(4) If the Magistrate's Court does not allow the appeal or substitute another notice or decision under subsection (3), it must dismiss the appeal.

(5) On an appeal under section 168(3), the Magistrate's Court 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 150(7)(a), 153(8)(a) or 156(8)(a) (urgency); or

(b) that the inclusion of that statement is not to have effect in relation to any part of the notice,

and may make such modifications to the notice as are required to give effect to the direction.

(6) On an appeal under section 168(4), if the Magistrate's Court considers that the enforcement notice ought to be cancelled or varied by reason of a change in circumstances, the Magistrate's Court must cancel or vary the notice.

(7) On an appeal under section 168(6), the Magistrate's Court may cancel the Commissioner's determination.

Complaints

Complaints by data subjects.

170.(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 III or IV 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 171; 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 or 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, 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 or the United Kingdom.

Orders to progress complaints.

171.(1) This section applies where, after a data subject makes a complaint under section 170 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 when the Commissioner received the complaint; or

(c) if the Commissioner's consideration of the complaint is not concluded during that period, fails to provide the complainant with such information during a subsequent period of 3 months.

(2) The Magistrate's Court may, on an application by the data subject, make an order requiring the Commissioner-

(a) to take appropriate steps to respond to the complaint; or

(b) to inform the complainant of progress on the complaint, or of the outcome of the complaint, within a period specified in the order.

(3) An order under subsection (2)(a) may require the Commissioner-

(a) to take steps specified in the order;

(b) to conclude an investigation, or take a specified step, within a period specified in the order.

(4) Section 170(5) applies for the purposes of subsections (1)(a) and (2)(a) as it applies for the purposes of section 170(4)(a).

Remedies in the court

Compliance orders.

172.(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 IV 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 III applies whose responsibilities are determined in an arrangement under section 67, 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.

Compensation for contravention of the GDPR.

173.(1) In Article 82 of the GDPR (right to compensation for material or non-material damage), "non-material damage" includes distress.

(2) Subsection (3) applies where-

(a) in accordance with rules of court, proceedings under Article 82 of the GDPR are brought by a representative body on behalf of a person; and

(b) a court orders the payment of compensation.

(3) The court may make an order providing for the compensation to be paid on behalf of the person to-

(a) the representative body; or

(b) such other person as the court thinks fit.

Compensation for contravention of other data protection legislation.

174.(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 III or IV applies whose responsibilities are determined in an arrangement under section 67 or 113 is only liable as described in subsection (2) if the controller is responsible for compliance with the provision of the data protection legislation that is contravened.

(5) In this section, "damage" includes financial loss and damage not involving financial loss, such as distress.

Offences relating to personal data

Unlawful obtaining etc of personal data.

175.(1) It is an offence for a person knowingly or recklessly-

(a) to obtain or disclose personal data without the consent of the controller;

(b) to procure the disclosure of personal data to another person without the consent of the controller; or

(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

(2) It is a defence for a person charged with an offence under subsection (1) to prove that the obtaining, disclosing, procuring or retaining-

(a) was necessary for the purposes of preventing or detecting crime;

(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal; or

(c) in the particular circumstances, was justified as being in the public interest.

(3) It is also a defence for a person charged with an offence under subsection (1) to prove that-

(a) the person acted in the reasonable belief that the person had a legal right to do the obtaining, disclosing, procuring or retaining;

(b) the person acted in the reasonable belief that the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it; or

(c) the person acted-

(i) for the special purposes,

(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

(iii) in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or retaining was justified as being in the public interest.

(4) It is an offence for a person to sell personal data if the person obtained the data in circumstances in which an offence under subsection (1) was committed.

(5) It is an offence for a person to offer to sell personal data if the person-

(a) has obtained the data in circumstances in which an offence under subsection (1) was committed; or

(b) subsequently obtains the data in such circumstances.

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale is an offer to sell the data.

(7) In this section-

(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 68(8) or 114(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.

Re-identification of de-identified personal data.

176.(1) It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.

(2) For the purposes of this section and section 177-

(a) personal data is "de-identified" if it has been processed in such a manner that it can no longer be attributed, without more, to a specific data subject;

(b) a person "re-identifies" information if the person takes steps which result in the information no longer being de-identified within the meaning of paragraph (a).

(3) It is a defence for a person charged with an offence under subsection (1) to prove that the re-identification-

(a) was necessary for the purposes of preventing or detecting crime;

(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal; or

(c) in the particular circumstances, was justified as being in the public interest.

(4) It is also a defence for a person charged with an offence under subsection (1) to prove that-

(a) the person acted in the reasonable belief that the person-

(i) is the data subject to whom the information relates,

(ii) had the consent of that data subject, or

(iii) would have had such consent if the data subject had known about the re-identification and the circumstances of it;

(b) the person acted in the reasonable belief that the person-

(i) is the controller responsible for de-identifying the personal data,

(ii) had the consent of that controller, or

(iii) would have had such consent if that controller had known about the re-identification and the circumstances of it;

(c) the person acted-

(i) for the special purposes,

(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

(iii) in the reasonable belief that in the particular circumstances the re-identification was justified as being in the public interest; or

(d) the effectiveness testing conditions were met as per section 177.

(5) It is an offence for a person knowingly or recklessly to process personal data that is information that has been re-identified where the person does so-

(a) without the consent of the controller responsible for de-identifying the personal data; and

(b) in circumstances in which the re-identification was an offence under subsection (1).

(6) It is a defence for a person charged with an offence under subsection (5) to prove that the processing-

(a) was necessary for the purposes of preventing or detecting crime;

(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal; or

(c) in the particular circumstances, was justified as being in the public interest.

(7) It is also a defence for a person charged with an offence under subsection (5) to prove that-

(a) the person acted in the reasonable belief that the processing was lawful;

(b) the person acted in the reasonable belief that the person-

(i) had the consent of the controller responsible for de-identifying the personal data, or

(ii) would have had such consent if that controller had known about the processing and the circumstances of it; or

(c) the person acted-

(i) for the special purposes,

(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

(iii) in the reasonable belief that in the particular circumstances the processing was justified as being in the public interest.

(8) In this section-

(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 68(8) or 114(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.

Re-identification: effectiveness testing conditions.

177.(1) For the purposes of section 176, in relation to a person who re-identifies information that is de-identified personal data, "the effectiveness testing conditions" means the conditions in subsections (2) and (3).

(2) The first condition is that the person acted-

(a) with a view to testing the effectiveness of the de-identification of personal data;

(b) without intending to cause, or threaten to cause, damage or distress to a person; and

(c) in the reasonable belief that, in the particular circumstances, reidentifying the information was justified as being in the public interest.

(3) The second condition is that the person notified the Commissioner or the controller responsible for de-identifying the personal data about the reidentification-

(a) without undue delay; and

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

(4) Where there is more than one controller responsible for de-identifying personal data, the requirement in subsection (3) is satisfied if one or more of them is notified.

Alteration etc of personal data to prevent disclosure.

178.(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 54 of this Act (law enforcement processing: right of access by the data subject);

(d) section 103 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) The persons referred to in subsection (3) 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

The special purposes.

179.(1) In this Part, "the special purposes" means one or more of the following-

(a) the purposes of journalism;

(b) academic purposes;

(c) artistic purposes;

(d) literary purposes.

(2) In this Part, "special purposes proceedings" means legal proceedings against a controller or processor which relate, wholly or partly, to personal data processed for the special purposes and which are-

(a) proceedings under section 172 (including proceedings on an application under Article 79 of the GDPR); or

(b) proceedings under Article 82 of the GDPR or section 174.

(3) The Commissioner may make a written determination, in relation to the processing of personal data, that-

(a) the personal data is not being processed only for the special purposes;

(b) the personal data is not being processed with a view to the publication by a person of journalistic, academic, artistic or literary material which has not previously been published by the controller.

(4) The Commissioner must give written notice of the determination to the controller and the processor.

(5) The notice must provide information about the rights of appeal under section 168.

(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.

Provision of assistance in special purposes proceedings.

180.(1) An individual who is a party, or prospective party, to special purposes proceedings may apply to the Commissioner for assistance in those proceedings.

(2) As soon as reasonably practicable after receiving an application under subsection (1), the Commissioner must decide whether, and to what extent, to grant it.

(3) The Commissioner must not grant the application unless, in the Commissioner's opinion, the case involves a matter of substantial public importance.

(4) If the Commissioner decides not to provide assistance, the Commissioner must, as soon as reasonably practicable, notify the applicant of the decision, giving reasons for the decision.

(5) If the Commissioner decides to provide assistance, the Commissioner must-

(a) as soon as reasonably practicable, notify the applicant of the decision, stating the extent of the assistance to be provided; and

(b) secure that the person against whom the proceedings are, or are to be, brought is informed that the Commissioner is providing assistance.

(6) The assistance that may be provided by the Commissioner includes-

(a) paying costs in connection with the proceedings; and

(b) indemnifying the applicant in respect of liability to pay costs, expenses or damages in connection with the proceedings.

(7) 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.

Staying special purposes proceedings.

181.(1) In any special purposes proceedings before a court, if the controller or processor claims, or it appears to the court, that any personal data to which the proceedings relate-

(a) is being processed only for the special purposes;

(b) is being processed with a view to the publication by any person of journalistic, academic, artistic or literary material; and

(c) has not previously been published by the controller,

the court must stay the proceedings.

(2) In considering, for the purposes of subsection (1)(c), whether material has previously been published, publication in the immediately preceding 24 hours is to be ignored.

(3) Under subsection (1), the court must stay the proceedings until either of the following conditions is met-

(a) a determination of the Commissioner under section 179 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

Jurisdiction.

182.(1) The jurisdiction conferred on a court by the provisions listed in subsection (2) is exercisable by the Magistrate's Court.

(2) Those provisions are-

(a) section 158 (enforcement notices and processing for the special purposes);

(b) section 163 (penalty notices and processing for the special purposes);

(c) section 172 and Article 79 of the GDPR (compliance orders);

(d) sections 173 and 174 and Article 82 of the GDPR (compensation);

(e) section 152A (information orders).

Definitions

Interpretation of Part VI.

183. In this Part-

"assessment notice" has the meaning given in section 153;

"certification provider" has the meaning given in section 21;

"enforcement notice" has the meaning given in section 155;

"information notice" has the meaning given in section 150;

"penalty notice" has the meaning given in section 162;

"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 VII

SUPPLEMENTARY AND FINAL PROVISION

Regulations under this Act

Regulations, rules of court and consultation.

184.(1) The Minister may make regulations for-

(a) carrying out the purposes of this Act; or

(b) complying with-

(i) the GDPR,

(ii) the Law Enforcement Directive,

(iii) the Data Protection Convention, or

(iv) articles 126 to 130 of the Convention of 1990 Applying the Schengen Agreement of 14 June 1985.

(2) Before making regulations under this Act, the Minister must consult-

(a) the Commissioner; and

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

(3) Subsection (2) does not apply to regulations made under-

(a) section 27;

(b) section 39.

(4) Regulations under this Act may-

(a) make different provision for different purposes;

(b) include consequential, supplementary, incidental, transitional, transitory or saving provision.

(5) 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.

(6) The power to make regulations under this section includes-

(a) the power to amend any provision of this Act, including the Schedules; and

(b) the power to make any consequential amendments to Gibraltar law to amend references to this Act.

Changes to the Data Protection Convention

Power to reflect changes to the Data Protection Convention.

185.(1) The Minister may by regulations make such provision as the Minister 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 Gibraltar.

(2) The power under subsection (1) includes power-

(a) to amend or replace the definition of "the Data Protection Convention" in section 2;

(b) to amend Chapter 3 of Part II of this Act;

(c) to amend Part IV of this Act;

(d) to make provision about the functions of the Commissioner, courts or tribunals in connection with processing of personal data to which Chapter 3 of Part II or Part IV of this Act applies, including provision amending Parts V to VII of this Act;

(e) to make provision about the functions of the Commissioner in connection with the Data Protection Convention or an instrument replacing that Convention, including provision amending Parts 5 to 7 of this Act;

(f) to consequentially amend this Act.

Rights of the data subject

Prohibition of requirement to produce relevant records.

186.(1) It is an offence for a person ("P1") to require another person to provide P1 with, or give P1 access to, a relevant record in connection with-

(a) the recruitment of an employee by P1;

(b) the continued employment of a person by P1; or

(c) a contract for the provision of services to P1.

(2) It is an offence for a person ("P2") to require another person to provide P2 with, or give P2 access to, a relevant record if-

(a) P2 is involved in the provision of goods, facilities or services to the public or a section of the public; and

(b) the requirement is a condition of providing or offering to provide goods, facilities or services to the other person or to a third party.

(3) It is a defence for a person charged with an offence under subsection (1) or (2) to prove that imposing the requirement-

(a) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal; or

(b) in the particular circumstances, was justified as being in the public interest.

(4) The imposition of the requirement referred to in subsection (1) or (2) is not to be regarded as justified as being in the public interest on the ground that it would assist in the prevention or detection of crime.

(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.

Avoidance of certain contractual terms relating to health records.

187.(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 54 of this Act (law enforcement processing: right of access by the data subject);

(d) section 103 of this Act (intelligence services processing: right of access by the data subject).

Data subject's rights and other prohibitions and restrictions.

188.(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 III of this Act (law enforcement processing: rights of the data subject); and

(c) Chapter 3 of Part IV of this Act (intelligence services processing: rights of the data subject).

(3) The provisions providing exceptions are-

(a) in Chapter 2 of Part II of this Act, sections 19 and 20 and Schedules 2, 3 and 4;

(b) in Chapter 3 of Part II of this Act, sections 27 and 28;

(c) in Part III of this Act, sections 53(4), 54(4) and 57(3); and

(d) in Part IV of this Act, Chapter 6.

Representation of data subjects

Representation of data subjects with their authority.

189.(1) In relation to the processing of personal data to which the GDPR applies-

(a) Article 80(1) of the GDPR (representation of data subjects) enables a data subject to authorise a body or other organisation which meets the conditions set out in that Article to exercise the data subject's rights under Articles 77, 78 and 79 of the GDPR (rights to lodge complaints and to an effective judicial remedy) on the data subject's behalf; and

(b) a data subject may also authorise such a body or organisation to exercise the data subject's rights under Article 82 of the GDPR (right to compensation).

(2) In relation to the processing of personal data to which the GDPR does not apply, a body or other organisation which meets the conditions in subsections (3) and (4), if authorised to do so by a data subject, may exercise some or all of the following rights of a data subject on the data subject's behalf-

(a) rights under section 170(2), (4)(d) and (6)(c) (complaints to the Commissioner);

(b) rights under section 171(2) (orders for the Commissioner to progress complaints);

(c) rights under section 172(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.

Representation of data subjects with their authority: collective proceedings.

190.(1) The Minister may by regulations make provision for representative bodies to bring proceedings combining two or more relevant claims.

(2) In this section, "relevant claim", in relation to a representative body, means a claim in respect of a right of a data subject, which the representative body is authorised to exercise on the data subject's behalf under Article 80(1) of the GDPR or section 189.

(3) The power under subsection (1) includes power-

(a) to make provision about the proceedings; and

(b) to confer functions on a person, including functions involving the exercise of a discretion.

(4) The provision mentioned in subsection (3)(a) includes provision about-

(a) the effect of judgments and orders;

(b) agreements to settle claims;

(c) the assessment of the amount of compensation;

(d) the persons to whom compensation may or must be paid, including compensation not claimed by the data subject;

(e) costs.

Duty to review provision for representation of data subjects.

191.(1) The Minister may-

(a) review the matters listed in subsection (2) in relation to Gibraltar;

(b) prepare a report of the review; and

(c) lay a copy of the report before Parliament.

(2) Those matters are-

(a) the operation of Article 80(1) of the GDPR;

(b) the operation of section 189;

(c) the merits of exercising the power under Article 80(2) of the GDPR (power to enable a body or other organisation which meets the conditions in Article 80(1) of the GDPR to exercise some or all of a data subject's rights under Articles 77, 78 and 79 of the GDPR without being authorised to do so by the data subject); and

(d) the merits of making equivalent provision in relation to data subjects' rights under Article 82 of the GDPR (right to compensation).

(3) After the report under subsection (1) is laid before Parliament, the Minister may by regulations-

(a) exercise the powers under Article 80(2) of the GDPR in relation to Gibraltar; and

(b) make provision enabling a body or other organisation which meets the conditions in Article 80(1) of the GDPR to exercise a data subject's rights under Article 82 of the GDPR in Gibraltar without being authorised to do so by the data subject.

(4) The powers under subsection (3) include power-

(a) to make provision enabling a data subject to prevent a body or other organisation from exercising, or continuing to exercise, the data subject's rights;

(b) to make provision about proceedings before a court or tribunal where a body or organisation exercises a data subject's rights;

(c) to make provision for bodies or other organisations to bring proceedings before a court or tribunal combining two or more claims in respect of a right of a data subject;

(d) to confer functions on a person, including functions involving the exercise of a discretion;

(e) to amend sections 2, 171 to 173, 182, 189 and 197;

(f) to insert new sections and Schedules into Part VI or VII.

(5) The provision mentioned in subsection (5)(b) and (c) includes provision about-

(a) the effect of judgments and orders;

(b) agreements to settle claims;

(c) the assessment of the amount of compensation;

(d) the persons to whom compensation may or must be paid, including compensation not claimed by the data subject;

(e) costs.

Offences

Penalties for offences.

192.(1) A person who commits an offence under section 128, 161 or 178 or paragraph 15 of Schedule 15 is liable on summary conviction, to a fine not exceeding level 5 on the standard scale.

(2) A person who commits an offence under section 140, 152, 154A, 175, 176 or 186 is liable-

(a) on summary conviction, to a fine not exceeding the statutory maximum;

(b) on conviction on indictment, to a fine.

(3) Subsections (4) and (5) apply where a person is convicted of an offence under section 175 or 186.

(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.

(6) A person who commits an offence under section 18(6) is liable on summary conviction, to a fine not exceeding level 3 on the standard scale.

Prosecution.

193.(1) Proceedings for an offence under this Act may be instituted only-

(a) by the Commissioner; or

(b) by or with the consent of the Attorney General.

(2) Subject to subsection (3), summary proceedings for an offence under section 178 (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.

(3) 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.

(4) A certificate signed by or on behalf of the prosecutor and stating the day on which the 6 month period described in subsection (2) began is conclusive evidence of that fact.

(5) A certificate purporting to be signed as described in subsection (4) is to be treated as so signed unless the contrary is proved.

Liability of directors etc.

194.(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.

Court Proceedings

Disclosure of information re court proceedings.

195. No enactment or rule of law prohibiting or restricting the disclosure of information precludes a person from providing the court with information necessary for the discharge of-

(a) its functions under the data protection legislation; or

(b) its other functions relating to the Commissioner's acts and omissions.

Court proceedings: contempt.

196.(1) This section applies where-

(a) a person does something, or fails to do something, in relation to proceedings before a court-

(i) on an appeal under section 29, 88, 120 or 168, or

(ii) for an order under section 171; 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 Magistrate's Court may certify the offence to the Supreme Court.

(3) Where an offence is certified under subsection (2), the Supreme Court 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 Supreme Court.

(4) Before exercising the power under subsection (3)(b), the Supreme 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.

Court Procedure Rules.

197.(1) The Chief Justice may make such Court Procedure Rules as are necessary and expedient for the purposes of appeals under this Act.

(2) Court Procedure Rules may make provision for regulating-

(a) the exercise of the rights of appeal conferred by section 29, 88, 120 or 168, and

(b) the exercise of the rights of data subjects under section 171, including their exercise by a representative body.

(3) In relation to proceedings involving the exercise of those rights, Court 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.

Territorial application

Territorial application of this Act.

198.(1) This Act applies only to processing of personal data described in subsections (2) and (3).

(2) It applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in Gibraltar, whether or not the processing takes place in Gibraltar.

(3) It also applies to the processing of personal data to which Chapter 2 of Part II (the GDPR) applies where-

(a) the processing is carried out in the context of the activities of an establishment of a controller or processor in a country or territory that is not a Member State or the United Kingdom, whether or not the processing takes place in such a country or territory;

(b) the personal data relates to a data subject who is in Gibraltar when the processing takes place; and

(c) the processing activities are related to-

(i) the offering of goods or services to data subjects in Gibraltar, whether or not for payment, or

(ii) the monitoring of data subjects' behaviour in Gibraltar.

(4) Subsections (1) to (3) have effect subject to any provision made under section 129 providing for the Commissioner to carry out functions in relation to other processing of personal data.

(5) Section 2(2)(c) does not apply to the reference to the processing of personal data in subsection (2).

(6) The reference in subsection (3) to Chapter 2 of Part II (the GDPR) does not include that Chapter as applied by Chapter 3 of Part II (the applied GDPR).

(7) In this section, references to a person who has an establishment in Gibraltar include the following-

(a) an individual who is ordinarily resident in Gibraltar;

(b) a body incorporated under Gibraltar law;

(c) a partnership or other unincorporated association formed under Gibraltar law; and

(d) a person not within paragraph (a), (b) or (c) who maintains, and carries on activities through, an office, branch or agency or other stable arrangements in Gibraltar, and references to a

person who has an establishment in another country or territory have a corresponding meaning.

General

Application to the Crown.

199.(1) This Act binds the Crown.

(2) For the purposes of the GDPR and this Act, each government department is to be treated as a person separate from the other government departments, to the extent that is not already the case.

(3) Where government departments are not able to enter into contracts with each other, a provision of the GDPR or this Act that would require relations between them to be governed by a contract, or other binding legal act, in writing is to be treated as satisfied if the relations are the subject of a memorandum of understanding or a data sharing policy between them.

(4) As regards criminal liability-

(a) a government department is not liable to prosecution under this Act;

(b) a person in the service of the Crown is liable to prosecution under the provisions of this Act listed in subsection (5).

(5) Those provisions are-

(a) section 128;

(b) section 175;

(c) section 176;

(d) section 178;

(e) paragraph 15 of Schedule 15.

Application to Parliament.

200.(1) Parts 1, 2 and 5 to 7 of this Act apply to the processing of personal data by or on behalf 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 Parliament, the

controller in respect of that data for the purposes of the GDPR and this Act is the Clerk of the Parliament.

(3) As regards criminal liability-

(a) nothing in subsection (2) makes the Clerk of the Parliament liable to prosecution under this Act;

(b) a person acting on behalf of Parliament is liable to prosecution under the provisions of this Act listed in subsection (4).

(4) Those provisions are-

(a) section 175;

(b) section 176;

(c) section 178;

(d) paragraph 15 of Schedule 15.".

SCHEDULE 1

SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL CONVICTIONS ETC DATA

PART 1

CONDITIONS RELATING TO EMPLOYMENT, HEALTH AND RESEARCH ETC

Employment, social security and social protection.

1.(1) This condition is met if-

(a) the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection; and

(b) when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule).

(2) See also the additional safeguards in Part 4 of this Schedule.

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;

(f) the management of health care systems or services or social care systems or services; or

(g) medical research.

(3) See also the conditions and safeguards in Article 9(3) of the GDPR (obligations of secrecy) and section 13(1).

Public health.

3. This condition is met if the processing-

(a) is necessary for reasons of public interest in the area of public health; and

(b) is carried out-

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

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

Research etc.

4. This condition is met if the processing-

(a) is necessary for archiving purposes, scientific or historical research purposes or statistical purposes;

(b) is carried out in accordance with Article 89(1) of the GDPR (as supplemented by section 23); 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) Except as otherwise provided, a condition in this Part of this Schedule is met only if, when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule).

(2) See also the additional safeguards in Part 4 of this Schedule.

Statutory etc and government purposes.

6.(1) This condition is met if the processing-

(a) is necessary for a purpose listed in subparagraph (2); and

(b) is necessary for reasons of substantial public interest.

(2) Those purposes are-

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

(b) the exercise of a function of a Minister or a government department.

Administration of justice and parliamentary purposes.

7. This condition is met if the processing is necessary-

(a) for the administration of justice; or

(b) for the exercise of a function of Parliament.

Equality of opportunity or treatment.

8.(1) Subject to the exceptions in subparagraphs (3) to (5), 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.

(2) In subparagraph (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 subparagraph (1) if it is carried out for the purposes of measures or decisions with respect to a particular data subject.

(4) Processing does not meet the condition in subparagraph (1) if it is likely to cause substantial damage or substantial distress to an individual.

(5) Processing does not meet the condition in subparagraph (1) if-

(a) an individual who is the data subject, or one of the data subjects, has given notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject, and has not given notice in writing withdrawing that requirement;

(b) the notice gave the controller a reasonable period in which to stop processing such data; and

(c) that period has ended.

Racial and ethnic diversity at senior levels of organisations.

9.(1) This condition is met if the processing-

(a) is of personal data revealing racial or ethnic origin;

(b) is carried out as part of a process of identifying suitable individuals to hold senior positions in a particular organisation, a type of organisation or organisations generally;

(c) is necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation or organisations; and

(d) can reasonably be carried out without the consent of the data subject, subject to the exception in subparagraph (3).

(2) For the purposes of subparagraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where-

(a) the controller cannot reasonably be expected to obtain the consent of the data subject; and

(b) the controller is not aware of the data subject withholding consent.

(3) Processing does not meet the condition in subparagraph (1) if it is likely to cause substantial damage or substantial distress to an individual.

(4) For the purposes of this paragraph, an individual holds a senior position in an organisation if the individual-

(a) holds a position listed in subparagraph (5); or

(b) does not hold such a position but is a senior manager of the organisation.

(5) Those positions are-

(a) a director, secretary or other similar officer of a body corporate;

(b) a member of a limited liability partnership;

(c) a partner in a partnership or a limited partnership registered under Gibraltar law or an entity of a similar character formed under the law of a country or territory outside Gibraltar.

(6) In this paragraph, "senior manager", in relation to an organisation, means a person who plays a significant role in-

(a) the making of decisions about how the whole or a substantial part of the organisation's activities are to be managed or organized; or

(b) the actual managing or organising of the whole or a substantial part of those activities.

(7) The reference in subparagraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Preventing or detecting unlawful acts.

10.(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) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in subparagraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

(3) In this paragraph-

"act" includes a failure to act;

"competent authority" has the same meaning as in Part III of this Act (see section 38).

Protecting the public against dishonesty etc.

11.(1) This condition is met if the processing-

(a) is necessary for the exercise of a protective function;

(b) must be carried out without the consent of the data subject so as not to prejudice the exercise of that function; and

(c) is necessary for reasons of substantial public interest.

(2) In this paragraph, "protective function" means a function which is intended to protect members of the public against-

(a) dishonesty, malpractice or other seriously improper conduct;

(b) unfitness or incompetence;

(c) mismanagement in the administration of a body or association; or

(d) failures in services provided by a body or association.

Regulatory requirements relating to unlawful acts and dishonesty etc.

12 (1) This condition is met if-

(a) the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has-

(i) committed an unlawful act, or

(ii) been involved in dishonesty, malpractice or other seriously improper conduct;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; and

(c) the processing is necessary for reasons of substantial public interest.

(2) In this paragraph-

"act" includes a failure to act;

"regulatory requirement" means-

(a) a requirement imposed by legislation or by a person in exercise of a function conferred by legislation; or

(b) a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity.

Journalism etc in connection with unlawful acts and dishonesty etc.

13.(1) This condition is met if-

(a) the processing consists of the disclosure of personal data for the special purposes;

(b) it is carried out in connection with a matter described in subparagraph (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 subparagraph (1)(b) are any of the following, whether alleged or established-

(a) the commission of an unlawful act by a person;

(b) dishonesty, malpractice or other seriously improper conduct of a person;

(c) unfitness or incompetence of a person;

(d) mismanagement in the administration of a body or association;

(e) a failure in services provided by a body or association.

(3) The condition in subparagraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

(4) In this paragraph-

"act" includes a failure to act;

"the special purposes" means-

(a) the purposes of journalism;

(b) academic purposes;

(c) artistic purposes;

(d) literary purposes.

Preventing fraud.

14. 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 subparagraph (i) or (ii).

Suspicion of terrorist financing or money laundering.

15. This condition is met if the processing is necessary for the purposes of making a disclosure in good faith under either of the following-

(a) a disclosure between certain entities within regulated sector in relation to suspicion of commission of terrorist financing offence or for purposes of identifying terrorist property;

(b) a disclosure within regulated sector in relation to suspicion of money laundering.

Support for individuals with a particular disability or medical condition.

16.(1) This condition is met if the processing-

(a) is carried out by a not-for-profit body which provides support to individuals with a particular disability or medical condition;

(b) is of a type of personal data falling within subparagraph (2) which relates to an individual falling within subparagraph (3);

(c) is necessary for the purposes of-

(i) raising awareness of the disability or medical condition, or

(ii) providing support to individuals falling within subparagraph (3) or enabling such individuals to provide support to each other;

(d) can reasonably be carried out without the consent of the data subject; and

(e) is necessary for reasons of substantial public interest.

(2) The following types of personal data fall within this subparagraph-

(a) personal data revealing racial or ethnic origin;

(b) genetic data or biometric data;

(c) data concerning health;

(d) personal data concerning an individual's sex life or sexual orientation.

(3) An individual falls within this subparagraph if the individual is or has been a member of the body mentioned in subparagraph (1)(a) and-

(a) has the disability or condition mentioned there, has had that disability or condition or has a significant risk of developing that disability or condition, or

(b) is a relative or carer of an individual who satisfies paragraph (a) of this subparagraph.

(4) For the purposes of subparagraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where-

(a) the controller cannot reasonably be expected to obtain the consent of the data subject; and

(b) the controller is not aware of the data subject withholding consent.

(5) In this paragraph-

"carer" means an individual who provides or intends to provide care for another individual other than-

(a) under or by virtue of a contract; or

(b) as voluntary work;

"disability" means a physical or mental impairment which has a substantial and long-term adverse effect on a person's ability to carry out day-to-day activities.

(6) The reference in subparagraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Counselling etc.

17.(1) This condition is met if the processing-

(a) is necessary for the provision of confidential counselling, advice or support or of another similar service provided confidentially;

(b) is carried out without the consent of the data subject for one of the reasons listed in subparagraph (2); and

(c) is necessary for reasons of substantial public interest.

(2) The reasons mentioned in subparagraph (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 subparagraph (1)(a).

Safeguarding of children and of individuals at risk.

18.(1) This condition is met if-

(a) the processing is necessary for the purposes of-

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual;

(b) the individual is-

(i) aged under 18, or

(ii) aged 18 or over and at risk;

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in subparagraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in subparagraph (1)(c) are-

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in subparagraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual-

(a) has needs for care and support;

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm; and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In subparagraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

Safeguarding of economic well-being of certain individuals.

19.(1) This condition is met if the processing-

(a) is necessary for the purposes of protecting the economic well-being of an individual at economic risk who is aged 18 or over;

(b) is of data concerning health;

(c) is carried out without the consent of the data subject for one of the reasons listed in subparagraph (2); and

(d) is necessary for reasons of substantial public interest.

(2) The reasons mentioned in subparagraph (1)(c) are-

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in subparagraph (1)(a).

(3) In this paragraph, "individual at economic risk" means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness or disability.

Insurance.

20.(1) Subject to subparagraphs (2) and (3), this condition is met if the processing-

(a) is necessary for an insurance purpose;

(b) is of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health; and

(c) is necessary for reasons of substantial public interest.

(2) Subparagraph (3) applies where-

(a) the processing is not carried out for the purposes of measures or decisions with respect to the data subject; and

(b) the data subject does not have and is not expected to acquire-

(i) rights against, or obligations in relation to, a person who is an insured person under an insurance contract to which the insurance purpose mentioned in subparagraph (1)(a) relates, or

(ii) other rights or obligations in connection with such a contract.

(3) Where this subparagraph applies, the processing does not meet the condition in subparagraph (1) unless, in addition to meeting the requirements in that subparagraph, it can reasonably be carried out without the consent of the data subject.

(4) For the purposes of subparagraph (3), processing can reasonably be carried out without the consent of the data subject only where-

(a) the controller cannot reasonably be expected to obtain the consent of the data subject; and

(b) the controller is not aware of the data subject withholding consent.

(5) In this paragraph-

"insurance contract" means a contract of general insurance or longterm insurance;

"insurance purpose" means-

(a) advising on, arranging, underwriting or administering an insurance contract;

(b) administering a claim under an insurance contract; or

(c) exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law.

(6) The reference in subparagraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Occupational pensions.

21.(1) This condition is met if the processing-

(a) is necessary for the purpose of making a determination in connection with eligibility for, or benefits payable under, an occupational pension scheme;

(b) is of data concerning health which relates to a data subject who is the parent, grandparent, great-grandparent or sibling of a member of the scheme;

(c) is not carried out for the purposes of measures or decisions with respect to the data subject; and

(d) can reasonably be carried out without the consent of the data subject.

(2) For the purposes of subparagraph (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) The reference in subparagraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Political parties.

22.(1) Subject to the exceptions in subparagraphs (2) and (3), this condition is met if the processing-

(a) is of personal data revealing political opinions;

(b) is carried out by a political party; and

(c) is necessary for the purposes of the political party's political activities.

(2) Processing does not meet the condition in subparagraph (1) if it is likely to cause substantial damage or substantial distress to a person.

(3) Processing does not meet the condition in subparagraph (1) if-

(a) an individual who is the data subject, or one of the data subjects, has given notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject, and has not given notice in writing withdrawing that requirement;

(b) the notice gave the controller a reasonable period in which to stop processing such data; and

(c) that period has ended.

(4) In this paragraph, "political activities" include campaigning, fund-raising, political surveys and case-work.

Elected representatives responding to requests.

23.(1) Subject to subparagraph (2), 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.

(2) Where the request is made by an individual other than the data subject, the condition in subparagraph (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.

Disclosure to elected representatives.

24.(1) Subject to subparagraph (2), 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.

(2) Where the request to the elected representative came from an individual other than the data subject, the condition in subparagraph (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.

Informing elected representatives about prisoners.

25.(1) This condition is met if-

(a) the processing consists of the processing of personal data about a prisoner for the purpose of informing a member of Parliament about the prisoner; and

(b) the member is under an obligation not to further disclose the personal data.

(2) The references in subparagraph (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.

Publication of legal judgments.

26. This condition is met if the processing-

(a) consists of the publication of a judgment or other decision of a court or tribunal; or

(b) is necessary for the purposes of publishing such a judgment or decision.

Anti-doping in sport.

27.(1) This condition is met if the processing is necessary-

(a) for the purposes of measures designed to eliminate doping which are undertaken by or under the responsibility of a body

or association that is responsible for eliminating doping in a sport, at a sporting event or in sport generally; or

(b) for the purposes of providing information about doping, or suspected doping, to such a body or association.

(2) The reference in subparagraph (1)(a) to measures designed to eliminate doping includes measures designed to identify or prevent doping.

(3) If the processing consists of the disclosure of personal data to a body or association described in subparagraph (1)(a), or is carried out in preparation for such disclosure, the condition in subparagraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

Standards of behaviour in sport.

28.(1) This condition is met if the processing-

(a) is necessary for the purposes of measures designed to protect the integrity of a sport or a sporting event; and

(b) must be carried out without the consent of the data subject so as not to prejudice those purposes.

(2) In subparagraph (1)(a), the reference to measures designed to protect the integrity of a sport or a sporting event is a reference to measures designed to protect a sport or a sporting event against-

(a) dishonesty, malpractice or other seriously improper conduct; or

(b) failure by a person participating in the sport or event in any capacity to comply with standards of behaviour set by a body or association with responsibility for the sport or event.

PART 3

ADDITIONAL CONDITIONS RELATING TO CRIMINAL CONVICTIONS ETC

Consent.

29. This condition is met if the data subject has given consent to the processing.

Protecting individual's vital interests.

30. This condition is met if-

(a) the processing is necessary to protect the vital interests of an individual; and

(b) the data subject is physically or legally incapable of giving consent.

Processing by not-for-profit bodies.

31. This condition is met if the processing is carried out-

(a) in the course of its legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim; and

(b) on condition that-

(i) the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and

(ii) the personal data is not disclosed outside that body without the consent of the data subjects.

Personal data in the public domain.

32. This condition is met if the processing relates to personal data which is manifestly made public by the data subject.

Legal claims.

33. This condition is met if the processing-

(a) is necessary for the purpose of, or in connection with, any legal proceedings, including prospective legal proceedings;

(b) is necessary for the purpose of obtaining legal advice; or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Judicial acts.

34. This condition is met if the processing is necessary when a court or tribunal is acting in its judicial capacity.

Administration of accounts used in commission of indecency offences involving children.

35.(1) This condition is met if-

(a) the processing is of personal data about a conviction or caution for an offence under section 256 or 257 of the Crimes Act 2011;

(b) the processing is necessary for the purpose of administering an account relating to the payment card used in the commission of the offence or cancelling that payment card; and

(c) when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule).

(2) See also the additional safeguards in Part 4 of this Schedule.

(3) In this paragraph-

"caution" means a caution given to a person in Gibraltar in respect of an offence which, at the time when the caution is given, is admitted;

"payment card" includes a credit card, a charge card and a debit card.

Extension of conditions in Part 2 of this Schedule referring to substantial public interest.

36. This condition is met if the processing would meet a condition in Part 2 of this Schedule but for an express requirement for the processing to be necessary for reasons of substantial public interest.

Extension of insurance conditions.

37. This condition is met if the processing-

(a) would meet the condition in paragraph 20 in Part 2 of this Schedule (the "insurance condition"); or

(b) would meet the condition in paragraph 36 by virtue of the insurance condition,

but for the requirement for the processing to be processing of a category of personal data specified in paragraph 20(1)(b).

PART 4

APPROPRIATE POLICY DOCUMENT AND ADDITIONAL SAFEGUARDS

Application of this Part.

38. This Part of this Schedule makes provision about the processing of personal data carried out in reliance on a condition in Part 1, 2 or 3 of this Schedule which requires the controller to have an appropriate policy document in place when the processing is carried out.

Requirement to have an appropriate policy document in place.

39. The controller has an appropriate policy document in place in relation to the processing of personal data in reliance on a condition described in paragraph 38 if the controller has produced a document which-

(a) explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the condition in question; and

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

Additional safeguard: retention of appropriate policy document.

40.(1) Where personal data is processed in reliance on a condition described in paragraph 38, the controller must during the relevant period-

(a) retain the appropriate policy document;

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

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

(2) "Relevant period", in relation to the processing of personal data in reliance on a condition described in paragraph 38, means a period which-

(a) begins when the controller starts to carry out processing of personal data in reliance on that condition; and

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

Additional safeguard: record of processing.

41. A record maintained by the controller, or the controller's representative, under Article 30 of the GDPR in respect of the processing of personal data in reliance on a condition described in paragraph 38 must include the following information-

(a) which condition is relied on;

(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and

(c) whether the personal data is retained and erased in accordance with the policies described in paragraph 39(b) and, if it is not, the reasons for not following those policies.".

SCHEDULE 2

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 of this Schedule, "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 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing),

(viii) Article 20(1) and (2) (right to data portability),

(ix) Article 21(1) (objections to processing),

(x) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in subparagraphs (i) to (ix); 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 and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) do not apply to personal data processed for any of the following purposes-

(a) the prevention 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) Subparagraph (3) applies where-

(a) personal data is processed by a person ("Controller 1") for any of the purposes mentioned in subparagraph (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 form 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 subparagraph (1).

Crime and taxation: risk assessment systems.

3.(1) The GDPR provisions listed in subparagraph (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 subparagraph (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 subparagraph 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 subparagraph (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).

Information required to be disclosed by law etc or in connection with legal proceedings.

4.(1) The listed GDPR provisions do not apply to personal data consisting of information that the controller is obliged by an enactment to make available to the public, to the extent that the application of those provisions would prevent the controller from complying with that obligation.

(2) The listed GDPR provisions do not apply to personal data where disclosure of the data is required by an enactment, a rule of law or an order of a court or tribunal, to the extent that the application of those provisions would prevent the controller from making the disclosure.

(3) The listed GDPR provisions do not apply to personal data where disclosure of the data-

(a) is necessary for the purpose of, or in connection with, legal proceedings, including prospective legal proceedings;

(b) is necessary for the purpose of obtaining legal advice; or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights,

to the extent that the application of those provisions would prevent the controller from making the disclosure.

PART 2

RESTRICTIONS BASED ON ARTICLE 23(1): RESTRICTIONS OF RULES IN ARTICLES 13 TO 21 AND 34

GDPR provisions to be restricted: "the listed GDPR provisions".

5. In this Part of 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 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);

(h) Article 20(1) and (2) (right to data portability);

(i) Article 21(1) (objections to processing);

(j) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in subparagraphs (a) to (i).

Functions designed to protect the public etc.

6. The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a function that-

(a) is designed as described in column 1 of the Table; and

(b) meets the condition relating to the function specified in column 2 of the Table,

to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

TABLE

Description of function design	**Condition**
1. The function is designed to protect members of the public against- (a) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate; or	The function is- (a) conferred on a person by an enactment; (b) a function of the Crown, a Minister or a government department; or (c) of a public nature, and is exercised in the public interest.

(b) financial loss due to the conduct of discharged or undischarged bankrupts.	
2. The function is designed to protect members of the public against- (a) dishonesty, malpractice or other seriously improper conduct; or (b) unfitness or incompetence.	The function is- (a) conferred on a person by an enactment; (b) a function of the Crown, a Minister or a government department; or (c) of a public nature, and is exercised in the public interest.
3. The function is designed- (a) to protect charities or community interest companies against misconduct or mismanagement (whether by trustees, directors or other persons) in their administration; (b) to protect the property of charities or community interest companies from loss or misapplication; or (c) to recover the property of charities or community interest companies.	The function is- (a) conferred on a person by an enactment; (b) a function of the Crown, a Minister or a government department; or (c) of a public nature, and is exercised in the public interest.
4. The function is designed- (a) to secure the health, safety and welfare of persons at work; or (b) to protect persons other than those at work against risk to health or safety arising out of or in connection with the action of persons at work.	The function is- (a) conferred on a person by an enactment; (b) a function of the Crown, a Minister or a government department; or (c) of a public nature, and is exercised in the public interest.
5. The function is designed to	The function is-

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.	(a) conferred on a person by an enactment; or (b) of a public nature, and is exercised in the public interest.
6. The function is designed- (a) to protect members of the public against conduct which may adversely affect their interests by persons carrying on a business; (b) to regulate agreements or conduct which have as their object or effect the prevention, restriction or distortion of competition in connection with any commercial activity; or (c) to regulate conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market.	The function is- (a) conferred on a person by an enactment; (b) a function of the Crown, a Minister or a government department; or (c) of a public nature, and is exercised in the public interest.

Audit functions.

7.(1) The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a function listed in subparagraph (2) to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

(2) The functions are any function that is conferred by an enactment on the Principal Auditor.

Regulatory functions relating to legal services, the health service and children's services.

8. The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a regulatory function relating to legal services, the health service and children's services, to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

Parliamentary privilege.

9. The listed GDPR provisions and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) do not apply to personal data where this is required for the purpose of avoiding an infringement of the privileges of Parliament.

Judicial appointments, judicial independence and judicial proceedings.

10.(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 subparagraph (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.

PART 3

RESTRICTION BASED ON ARTICLE 23(1): PROTECTION OF RIGHTS OF OTHERS

Protection of the rights of others: general.

11.(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) Subparagraph (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.

12.(1) For the purposes of paragraph 12(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 at subparagraph (2) is met;

(b) the social work data test at subparagraph (3) is met; or

(c) the education data test at subparagraph (4) 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 the Department of Education or an education establishment in Gibraltar 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.

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".

13. In this Part of 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 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in subparagraphs (a) to (c).

Legal professional privilege.

14. The listed GDPR provisions do not apply to personal data that consists of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

Self incrimination.

15.(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 subparagraph (1) does not include an offence under-

(a) this Act, or

(b) section 466 of the Crimes Act 2011 (false statutory declarations and other false 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.

16.(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;

"price" includes value;

"relevant person" means a person or body that has permission under Gibraltar law to carry on regulated activities.

Management forecasts.

17. 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.

18. 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.

19. The listed GDPR provisions do not apply to personal data consisting of a reference given, or to be given, in confidence for the purposes of-

(a) the education, training or employment, or prospective education, training or employment, of the data subject;

(b) the placement, or prospective placement, of the data subject as a volunteer;

(c) the appointment, or prospective appointment, of the data subject to any office; or

(d) the provision, or prospective provision, by the data subject of any service.

Exam scripts and exam marks.

20.(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 subparagraph (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 5 months beginning when the question arises; or

(b) if earlier, before the end of the period of 40 days beginning with the announcement of the results.

(4) In this paragraph, "exam" means an academic, professional or other examination used for determining the knowledge, intelligence, skill or ability of a candidate and may include an exam consisting of an assessment of the candidate's performance while undertaking work or any other activity.

(5) For the purposes of this paragraph, the results of an exam are treated as announced when they are first published or, if not published, first communicated to the candidate.

Trusts.

21. The listed GDPR provisions do not apply to personal data that consists of information in respect of trusts registered or formed under Gibraltar law.

PART 5

EXEMPTIONS ETC BASED ON ARTICLE 85(2) FOR REASONS OF FREEDOM OF EXPRESSION AND INFORMATION

Journalistic, academic, artistic and literary purposes.

22.(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) Subparagraph (3) applies to the processing of personal data carried out for the special purposes if-

(a) the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material; and

(b) the controller reasonably believes that the publication of the material would be in the public interest.

(3) The listed GDPR provisions do not apply to the extent that the controller reasonably believes that the application of those provisions would be incompatible with the special purposes.

(4) In determining whether publication would be in the public interest the controller must take into account the special importance of the public interest in the freedom of expression and information.

(5) In determining whether it is reasonable to believe that publication would be in the public interest, the controller must have regard to any of the codes of practice or guidelines listed in subparagraph (6) that is relevant to the publication in question.

(6) The codes of practice and guidelines are-

(a) Programme Standards Code;

(b) Right of Reply Code;

(c) On-Demand Audiovisual Media Services Code;

(d) Audiovisual Commercial Communications Code; and

(e) Objectivity, Impartiality, Accuracy and Undue Prominence Code.

(7) The Minister may by regulations amend the list in subparagraph (6).

(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 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing),

(viii) Article 20(1) and (2) (right to data portability),

(ix) Article 21(1) (objections to processing);

(c) in Chapter IV of the GDPR (controller and processor)-

(i) Article 34(1) and (4) (communication of personal data breach to the data subject),

(ii) Article 36 (requirement for controller to consult Commissioner prior to high risk processing);

(d) in Chapter V of the GDPR (transfers of data to third countries etc), Article 44 (general principles for transfers);

(e) in Chapter VII of the GDPR (co-operation and consistency)-

(i) Articles 60 to 62 (co-operation),

(ii) Articles 63 to 67 (consistency).

PART 6

DEROGATIONS ETC BASED ON ARTICLE 89 FOR RESEARCH, STATISTICS AND ARCHIVING

Research and statistics.

23.(1) Subject to subparagraph (3), 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.

(2) For the purposes of this paragraph, 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 subparagraph (1) is available only where-

(a) the personal data is processed in accordance with Article 89(1) of the GDPR (as supplemented by section 23); 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.

24.(1) Subject to subparagraph (3), 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.

(2) For the purposes of this paragraph, 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 obligation regarding rectification or erasure of personal data or restriction of processing);

(e) Article 20(1) (right to data portability);

(f) Article 21(1) (objections to processing).

(3) The exemption in subparagraph (1) is available only where the personal data is processed in accordance with Article 89(1) of the GDPR (as supplemented by section 23).

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"

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 subparagraphs (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 there is no health professional available falling within paragraph (a) or (b).

(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. 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 family proceedings and proceedings involving children; and

(c) in accordance with those rules, the data may be withheld by the court in whole or in part from the data subject.

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) 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) 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 subparagraph (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) do 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 subparagraph (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 subparagraph (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) do 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) Subparagraph (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 subparagraph (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 14 of this Schedule;

"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 carrying out social work, because it would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

8.(1) This Part applies to personal data processed for any of the following descriptions-

(a) by a public authority in connection with social services functions;

(b) by a public authority in connection with the provision of social care;

(c) by a public authority in connection with functions designed for social security adjudications;

(d) by a public authority in connection with any functions relating to offender probation services;

(e) by a public authority in connection with any functions relating to ensuring that children of compulsory school age-

(i) receive suitable education whether by attendance at school or otherwise,

(ii) 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;

(f) by a public authority or a voluntary organization designated for the purposes of prevention of cruelty of children;

(g) by the Gibraltar Health Authority in the exercise of any functions similar to any social services functions

(h) 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 (g), and

(ii) which fell within any of those paragraphs while processed by that authority or body;

(i) data processed by a children's guardian appointed for the purposes of court proceedings.

(j) data processed by a court officer for family proceedings or proceedings involving children.

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 family proceedings or proceedings involving children; 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.

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) 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) 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 subparagraph (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) do not apply to social work data to the extent that the serious harm test is met with respect to the data.

PART 4

EDUCATION DATA

Educational records.

12. In this Part of this Schedule "educational record" means a record to which paragraph 13 applies.

13.(1) This paragraph applies to a record of information which-

(a) is processed by or on behalf of the proprietor of, or a teacher at, a school in Gibraltar;

(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 subparagraph (3).

(2) But this paragraph does not apply to information which is processed by a teacher solely for the teacher's own use.

(3) The persons referred to in subparagraph (1)(c) are-

(a) an employee of the Department of Education;

(b) a teacher or other employee at the school (including an educational psychologist);

(c) the pupil to whom the record relates;

(d) a parent or legal guardian of the pupil.

Other definitions.

14.(1) In this Part of this Schedule "education data" means personal data consisting of information which-

(a) constitutes an educational record; but

(b) is not data concerning health;

(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.

15.(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 family proceedings or proceedings involving children; and

(c) in accordance with those rules, the data may be withheld by the court in whole or in part from the data subject.

Exemption from Article 15 of the GDPR: serious harm.

16. Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) do not apply to education data to the extent that the serious harm test is met with respect to the data.

PART 5

CHILD ABUSE DATA

Exemption from Article 15 of the GDPR: child abuse data.

17.(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) do 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.

SCHEDULE 4

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).

2. The listed GDPR provisions do not apply to personal data consisting of the disclosure of information for the following-

(a) human fertilization and embryology records;

(b) adoption records and reports;

(c) statements of special educational needs;

(d) parental order records and reports.

SCHEDULE 5

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) a national accreditation body;

"certification provider" and "national accreditation body" have the same meaning as in section 21.

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 subparagraphs (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 Minister 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 Minister-

(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 appointed under subparagraph (3) or (4).

(8) If the applicant objects to a member of the appeal panel under subparagraph (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 subparagraph (8).

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 subparagraph (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.

Meaning of "working day".

7. In this Schedule, "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.

SCHEDULE 6

THE APPLIED GDPR AND THE APPLIED CHAPTER 2

PART 1

MODIFICATIONS TO THE GDPR

Introductory.

1. In its application by virtue of section 26(1), the GDPR has effect as if it were modified as follows.

References to the GDPR and its provisions.

2.(1) Subject to subparagraph (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.

(2) Subparagraph (1) does not have effect-

(a) in the case of the references which are modified or inserted by paragraphs 9(f), 15(b), 16(a)(ii), 35, 36(a) and (e)(ii) and 38(a)(i);

(b) in relation to the references in points (a) and (b) of paragraph 2 of Article 61, as 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 Gibraltar law.

(2) Subparagraph (1) is subject to the specific modifications made in this Part of this Schedule.

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 Gibraltar.

(2) Subparagraph (1) is subject to the specific modifications made in this Part of this Schedule (including paragraph 3(1)).

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) Subparagraph (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) Subparagraph (1) is also subject to the specific modifications made in this Part of this Schedule.

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 II of the 2004 Act applies (see section 25 of that Act)."

8. For Article 3 substitute-

"Article 3

Territorial application

Section 198 of the 2004 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 68(8) or 114(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 8 of the 2004 Act (meaning of "controller")";

(b) after paragraph (7) insert-

"(7A) "the 2004 Act" means the Data Protection Act 2004 as applied by section 26 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 Gibraltar";

(f) in paragraph (21) (meaning of "supervisory authority") for "Article 51" substitute "Article 51 of the GDPR";

(g) after paragraph (21) insert-

"(21A) "the Commissioner" means the Data Protection Commissioner (see section 123 of the 2004 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 of the 2004 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 19 and Part 1 of Schedule 2 of the 2004 Act, a legal basis for the processing referred to in point (c) and (e) of paragraph 1 may be laid down by the Minister in regulations (see section 20 of the 2004 Act).";

(c) in paragraph 3, in the second subparagraph, for "The Union or the 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 11 of the 2004 Act.";

(b) in paragraph 3, for "the general contract law of Member States" substitute "the general law of contract as it operates in Gibraltar 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 "Gibraltar law (see section 12 of the 2004 Act)";

(c) in paragraph 2, for point (g) substitute-

"(g) processing is necessary for reasons of substantial public interest and is authorised by Gibraltar law (see section 12 of the 2004 Act);";

(d) in paragraph 2(h), for "Union or Member State law" substitute "Gibraltar law (see section 12 of the 2004 Act)";

(e) in paragraph 2(i), for "Union or Member State law" insert "Gibraltar law (see section 12 of the 2004 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 23 of the 2004 Act) and is authorised by Gibraltar law (see section 12 of that Act).";

(g) in paragraph 3, for "national competent bodies", in both places, substitute "a national competent body of Gibraltar";

(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 "Gibraltar law (see section 12 of the 2004 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 Gibraltar law".

Section 3 of Chapter III 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 Gibraltar law";

(b) in paragraph 3(b), for "by Union or Member State law to which the controller is subject" substitute "under Gibraltar law".

18. In Article 18 (right to restriction of processing), in paragraph 2, for "of the Union or of a Member State" substitute "of Gibraltar".

Section 4 of Chapter III 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 17 of the 2004 Act; or".

Section 5 of Chapter III of the GDPR (rights of the data 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 19 and Schedules 2, 3 and 4 of the 2004 Act, the Minister";

(b) in point (e), for "of the Union or of a Member State", in both places, substitute "of Gibraltar";

(c) after point (j) insert-

"See section 20 of the 2004 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" substitute "Gibraltar 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 "Gibraltar law";

(b) in paragraph 3, in the second subparagraph, for "other Union or Member State data protection provisions" substitute "any other rule of Gibraltar 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 30(3) of the 2004 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 30(3) of the 2004 Act";

(g) in paragraph 4, omit "and, where applicable, the controller's or the 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 Minister 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 Gibraltar 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 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 organization-

(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;

(d) in paragraph 9, for "of this Article" substitute "of Article 45 of the GDPR".

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 Gibraltar";

(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 "Union law or in the law of the Member State to which the controller is subject" substitute "Gibraltar law (see section 22 of the 2004 Act which makes certain provision about the public interest)";

(c) for paragraph 5 substitute-

"5 Paragraph 1 is subject to any regulations made under section 22(2) of the 2004 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 shall on its territory" 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 30(3) of the 2004 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 "Gibraltar law";

(c) in paragraph 3, in point (b), for "the Member State government" substitute "the Minister";

(d) in paragraph 3, omit point (c);

(e) 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 Minister";

(b) omit ", to the Commission and 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 Gibraltar.";

(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 182 of the 2004 Act)."

53 In Article 80 (representation of data subjects)-

(a) in paragraph 1, omit "where provided for by Member State law";

(b) in paragraph 2, for "Member States" substitute "The Minister";

(c) after that paragraph insert-

"3 The power under paragraph 2 may only be exercised by making regulations under section 191 of the 2004 Act."

54. Omit Article 81 (suspension of proceedings).

55. In Article 82 (right to compensation and liability), for paragraph 6 substitute-

"6 Proceedings for exercising the right to receive compensation are to be brought before a court (see section 182 of the 2004 Act)."

56. In Article 83 (general conditions for imposing administrative fines)-

(a) in paragraph 5, in point (d), for "pursuant to Member State law adopted under Chapter IX" substitute "under Part 5 or 6 of Schedule 2 to the 2004 Act or under regulations made under section 20 of that Act";

(b) in paragraph 7-

(i) for "each Member State" substitute "the Minister";

(ii) for "that Member State" substitute "Gibraltar";

(c) for paragraph 8 substitute-

"8 Section 124(9) of the 2004 Act makes provision about the exercise of the Commissioner's powers under this Article. Part VI of the 2004 Act (enforcement) makes further provision in connection with administrative penalties (including provision about appeals).";

(d) 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 2004 Act (see in particular Part VI (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 Minister, in addition to the relevant provisions, may by way of regulations (see section 20 of the 2004 Act),";

(c) in paragraph 2, at the end insert-

"In this paragraph, "the relevant provisions" means section 19 of and Part 5 of Schedule 2 to the 2004 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 "Gibraltar 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 Minister, in addition to the relevant provisions, may in regulations (see section 20 of the 2004 Act)";

(b) in paragraph 3, for "Union or Member State law may" substitute "the Minister, in addition to the relevant provisions, may in regulations (see section 20 of the 2004 Act)";

(c) after paragraph 3, insert-

"3A In this Article "the relevant provisions" means section 19 of and Part 6 of Schedule 2 to the 2004 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 "Gibraltar 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 II

Introductory.

73. In its application by virtue of section 26(2), Chapter 2 of Part II has effect as if it were modified as follows.

General modifications.

74. (1) References to Chapter 2 of Part II 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 22(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 20 (power to make further exemptions etc by regulations), in subsection (1)(a), for “Member State law” substitute “the Minister”.

SCHEDULE 7

COMPETENT AUTHORITIES

1. Any government department.
2. Gibraltar Courts Service.

Policing bodies.

3. The Commissioner of Police.
4. The Royal Gibraltar Police.
5. Gibraltar Financial Intelligence Unit (GFIU).
6. Gibraltar Coordinating Centre for Criminal Intelligence and Drugs (GCID).
7. HM Prison.

Other authorities with investigatory functions.

8. The Collector of Customs.
9. HM Customs.
10. Borders & Coastguard Agency.
11. The Environmental Agency.
12. Gibraltar Regulatory Authority.
13. Gibraltar Financial Services Commission.
14. any other public authority or public body carrying out investigatory functions.
15. any other public authority or public body carrying out functions relating to offender management.

Other authorities.

16. Office of Criminal Prosecutions and Litigation.
17. Attorney General.
18. The Director of Public Prosecutions.
19. Gibraltar Bar Council.
20. A court or tribunal.

SCHEDULE 8

CONDITIONS FOR SENSITIVE PROCESSING UNDER PART III

Statutory etc purposes.

1. This condition is met if the processing-

(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law; and

(b) is necessary for reasons of substantial public interest.

Administration of justice.

2. This condition is met if the processing is necessary for the administration of justice.

Protecting individual's vital interests.

3. This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual.

Safeguarding of children and of individuals at risk.

4.(1) This condition is met if-

(a) the processing is necessary for the purposes of-

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual;

(b) the individual is-

(i) aged under 18, or

(ii) aged 18 or over and at risk;

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in subparagraph (2); and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in subparagraph (1)(c) are-

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in subparagraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual-

(a) has needs for care and support;

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm; and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In subparagraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

Personal data already in the public domain.

5. This condition is met if the processing relates to personal data which is manifestly made public by the data subject.

Legal claims.

6. This condition is met if the processing-

(a) is necessary for the purpose of, or in connection with, any legal proceedings, including prospective legal proceedings;

(b) is necessary for the purpose of obtaining legal advice; or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Judicial acts.

7. This condition is met if the processing is necessary when a court or other judicial authority is acting in its judicial capacity.

Preventing fraud.

8. 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 subparagraph (i) or (ii).

Archiving etc.

9. This condition is met if the processing is necessary-

(a) for archiving purposes in the public interest;

(b) for scientific or historical research purposes; or

(c) for statistical purposes.

SCHEDULE 9

CONDITIONS FOR PROCESSING UNDER PART IV

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 Parliament;

(c) for the exercise of any functions conferred on a person by an enactment or rule of law;

(d) for the exercise of any functions of a minister 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) Subparagraph (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

CONDITIONS FOR SENSITIVE PROCESSING UNDER PART IV

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.

Safeguarding of children and of individuals at risk.

4.(1) This condition is met if-

(a) the processing is necessary for the purposes of-

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual;

(b) the individual is-

(i) aged under 18, or

(ii) aged 18 or over and at risk;

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in subparagraph (2); and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in subparagraph (1)(c) are-

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in subparagraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual-

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In subparagraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

Data already published by data subject.

5. 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.

6. 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.

Administration of justice, parliamentary, statutory etc and government purposes.

7. The processing is necessary-

(a) for the administration of justice;

(b) for the exercise of any functions of Parliament;

(c) for the exercise of any functions conferred on any person by an enactment or rule of law; or

(d) for the exercise of any functions of a minister or a government department.

Medical purposes.

8.(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.

9.(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 as per section 95(6).

SCHEDULE 11

OTHER EXEMPTIONS UNDER PART IV

Preliminary.

1. In this Schedule, "the listed provisions" means-

(a) Chapter 2 of Part IV (the data protection principles), except section 84(1)(a) and (2) and Schedules 9 and 10;

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

(c) in Chapter 4 of Part IV, section 117 (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-

(a) is necessary for the purpose of, or in connection with, legal proceedings, including prospective legal proceedings;

(b) is necessary for the purpose of obtaining legal advice; or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights,

to the extent that the application of the listed provisions would prevent the controller from making the disclosure.

Parliamentary privilege.

4. The listed provisions do not apply to personal data where this is required for the purpose of avoiding an infringement of Parliamentary privilege.

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 Gibraltar.

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 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 subparagraph (3).

(3) Where the relevant time falls before the results of the exam are announced, the period mentioned in section 103(10)(b) is extended until the earlier of-

(a) the end of the period of 5 months beginning with the relevant time; and

(b) the end of the period of 40 days beginning with the announcement of the results.

(4) In this paragraph-

"exam" means an academic, professional or other examination used for determining the knowledge, intelligence, skill or ability of a candidate and may include an exam consisting of an assessment of

the candidate's performance while undertaking work or any other activity;

"the relevant time" has the same meaning as in section 103.

(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 subparagraph (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 subparagraph (1) is available only where the personal data is processed subject to appropriate safeguards for the rights and freedoms of data subjects.

SCHEDULE 12

Powers of the Commissioner.

1.(1) Subject to this or any other Act, the Commissioner shall have–

(a) the power to do all things necessary for or ancillary or reasonably incidental to the carrying out of his functions; and

(b) the powers set out in the Gibraltar Regulatory Authority Act 2000.

(2) Without prejudice to the generality of the powers conferred on him, the Commissioner, for the purposes of achieving the objects of this Act-

(a) may bring or defend legal actions in the Gibraltar or other courts (including applying to the court for any warrant that may be required);

(b) may liaise with any persons or organizations as useful or necessary to the performance of his functions;

(c) shall co-operate with and render assistance to supervisory authorities in States party to the Convention of 19 June 1990 applying the Schengen Agreement of 14 June 1985 by the furnishing of information on Gibraltar law and practice on data protection and automatic processing carried out in Gibraltar;

(d) may co-operate with and render assistance to supervisory authorities in other states or territories by the furnishing of information on Gibraltar law and practice on data protection and automatic processing carried out in Gibraltar;

(e) shall render assistance to data subjects whether resident in Gibraltar or abroad;

(f) may request supervisory authorities in other states to exercise their powers.

SCHEDULE 13

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 III or IV of this Act applies-

(a) to notify the controller or the processor of an alleged infringement of Part III or IV of this Act;

(b) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of Part III or IV of this Act;

(c) to issue reprimands to a controller or processor where processing operations have infringed provisions of Part III or IV 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 Gibraltar, 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 or the United Kingdom.

SCHEDULE 14

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 Gibraltar law.

(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 standardized format.

Fees.

3.(1) Subject to subparagraph (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 or 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 Gibraltar.

(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 Gibraltar 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 Gibraltar is made by a person resident outside Gibraltar, including where the request is forwarded to the Commissioner through the Minister or a foreign designated authority.

(2) The Commissioner must take appropriate measures to assist the person to exercise those rights.

Assisting Gibraltar 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 Gibraltar) specified in the request is-

(a) made by a person resident in Gibraltar; 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 Gibraltar, which is bound by that Data Protection Convention.

SCHEDULE 15

POWERS OF ENTRY AND INSPECTION

Issue of warrants in connection with non-compliance and offences.

1.(1) This paragraph applies if a judge 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 155(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 judge 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 179 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 subparagraphs (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 155(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 subparagraphs (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) Subparagraph (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) Subparagraphs (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 subparagraphs (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 subparagraph (1)(b) or in subparagraph (2)(b) and (c).

(5) In subparagraphs (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 Parliamentary privilege.

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 subparagraph (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; or

(b) section 466 of the Crimes Act 2011 (false statutory declarations and other false 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.

SCHEDULE 16

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 to a person in reliance on a notice of intent after the end of the period of 6 months beginning when the notice of intent is given, subject to subparagraph (3).

(3) The period for giving a penalty notice to a person may be extended by agreement between the Commissioner and the person.

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 subparagraph (2));

(c) an indication of the amount of the penalty the Commissioner proposes to impose, including any aggravating or mitigating factors that the Commissioner proposes to take into account.

(2) The information required under subparagraph (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 155(2), the nature of the personal data involved in the failure.

(3) A notice of intent must also-

(a) state that the person may make written representations about the Commissioner's intention to give a penalty notice; and

(b) specify the period within which such representations may be made.

(4) The period specified for making written representations must be a period of not less than 21 days beginning when the notice of intent is given.

(5) If the Commissioner considers that it is appropriate for the person to have an opportunity to make oral representations about the Commissioner's intention to give a penalty notice, the notice of intent must also-

(a) state that the person may make such representations; and

(b) specify the arrangements for making such representations and the time at which, or the period within which, they may be made.

Giving a penalty notice.

4.(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 subparagraph (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 168;

(h) details of the Commissioner's enforcement powers under this Schedule.

(2) The information required under subparagraph (1)(d) includes-

(a) a description of the circumstances of the failure; and

(b) where the notice is given in respect of a failure described in section 155(2), the nature of the personal data involved in the failure.

Period for payment of penalty.

6.(1) A penalty must be paid to the Commissioner within the period specified in the penalty notice.

(2) The period specified must be a period of not less than 28 days beginning when the penalty notice is given.

Variation of penalty.

7.(1) The Commissioner may vary a penalty notice by giving written notice (a "penalty variation notice") to the person to whom it was given.

(2) A penalty variation notice must specify-

(a) the penalty notice concerned; and

(b) how it is varied.

(3) A penalty variation notice may not-

(a) reduce the period for payment of the penalty;

(b) increase the amount of the penalty;

(c) otherwise vary the penalty notice to the detriment of the person to whom it was given.

(4) If-

(a) a penalty variation notice reduces the amount of the penalty; and

(b) when that notice is given, an amount has already been paid that exceeds the amount of the reduced penalty,

the Commissioner must repay the excess.

Cancellation of penalty.

8.(1) The Commissioner may cancel a penalty notice by giving written notice to the person to whom it was given.

(2) If a penalty notice is cancelled, the Commissioner-

(a) may not take any further action under section 162 or this Schedule in relation to the failure to which that notice relates; and

(b) must repay any amount that has been paid in accordance with that notice.

Enforcement of payment.

9.(1) The Commissioner must not take action to recover a penalty unless-

(a) the period specified in accordance with paragraph 6 has ended;

(b) any appeals against the penalty notice have been decided or otherwise ended;

(c) if the penalty notice has been varied, any appeals against the penalty variation notice have been decided or otherwise ended; and

(d) the period for the person to whom the penalty notice was given to appeal against the penalty, and any variation of it, has ended.

(2) A penalty is recoverable if a court so orders, as if it were payable under an order of that court.

SCHEDULE 17

RELEVANT RECORDS

Relevant records.

1. In section 186, "relevant record" means-

(a) a relevant health record (see paragraph 2); or

(b) a relevant record relating to a conviction or caution (see paragraph 3).

Relevant health records.

2. "Relevant health record" means a health record which has been or is to be obtained by a data subject in the exercise of a data subject access right.

Relevant records relating to a conviction or caution.

3.(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 subparagraph (2); and

(b) contains information relating to a conviction or caution.

(2) Those persons are-

(a) the Commissioner of Police;

(b) the Royal Gibraltar Police.

(3) In this paragraph "caution" means a caution given to a person in in respect of an offence which, at the time when the caution is given, is admitted.

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 54 of this Act (law enforcement processing: right of access by the data subject);

(d) section 103 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. The Minister may by regulations amend this Schedule.