



Amending  
enactments

Relevant current  
provisions

Commencement  
date

LN. 2006/039 *Corrigenda*

**English sources:**

None cited

**EU Legislation/International Agreements involved:**

Directive 95/46/EC

## ARRANGEMENT OF SECTIONS

### Section

#### **Part I**

##### *General*

1. Title and Commencement.
2. Definitions.
3. Subject matter and Application of Act.
4. Electronic communication and Service of Notices.
5. Acting for another.

#### **Part II**

##### *General Rules on the Lawfulness of the Processing of Personal Data*

6. Principles relating to Data Quality and Security.
7. Criteria for Making Data Processing Legitimate.
8. Sensitive Personal Data.
9. Application of this Act in relation to Defence and National Security.
10. Information to be given to the Data Subject.
11. Security of Processing.
12. Confidentiality of Processing.
13. Freedom of Journalistic, Artistic and Literary Expression.

#### **Part III**

##### *Data Subject's Rights*

14. Access.
15. Rectification etc. of Data.
16. Data Subject's Right to Object.
17. Direct Marketing.
18. Decisions based solely on automatic processing of data.
19. Exemptions from prohibitions on processing and Data Subjects' Rights.
20. Power to make additional Exemptions and Restrictions: Data Quality, Rights of data subjects, publicising of processing operations.

#### **Part IV**

##### *Supervisory Authority*

21. Supervisory Authority.
22. Data Protection Register.
23. Application for Registration.
24. Obligation to Register.

#### **Part V**

##### *Powers of Supervisory Authority*

- 25. Investigations, Mediation and Compensation.
- 26. Enforcement Notices.
- 27. Information Notices.
- 28. Information and Codes of Practice.
- 29. Authorised Officers.

**Part VI**

*Transfer of Personal Data to Third Countries*

- 30. Transfer of Personal Data.
- 31. Prohibition of data transfers.

**Part VII**

*Judicial Remedies, Liability and Sanctions*

- 32. Appeals.
- 33. Offences.
- 34. Proceedings.
- 35. Penalties.

**Part VIII**

*Personal Data Protection Officials and Exemptions from Registration*

- 36. Personal Data Protection Officials and Exemptions from Registration.

**Part IX**

*Regulations, Rules of Court*

- 37. Regulations and Rules of Court.

**SCHEDULE 1**

Powers of the Gibraltar Data Protection Commissioner.



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. In this Act, words and expressions have the same meaning as in the Directive, and unless the context otherwise requires–

“automated data” means information which–

- (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose; or
- (b) is recorded with the intention that it should be processed by means of such equipment;

“back-up data” means data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged;

“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 Commission” means the European Commission;

“the Commissioner” means the Data Protection Commissioner designated under section 21;

“compensation order” means decision of the Commissioner under section 25(4);

“data” means both automated and manual data;

“data controller” means a natural or legal person, public authority, agency or any other body who or which, alone or jointly with others determines the purposes and means of the processing of data;

“data processor” means

- (a) not being a data controller, or employee of a data controller,
- (b) a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller;

“data subject” means a natural person who is the subject of personal data;

“data subject’s consent” means any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed;

“direct marketing” means the communication by whatever means of any advertising or marketing material which is directed to particular individuals and includes direct mailing other than direct mailing carried out in the course of political activities by a political party or its members, or a body established by or under statute or a candidate for election to, or a holder of, elective political office;

“the Directive” means Directive 95/46/EC of the European Parliament and 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;

“EEA” means the European Economic Area;

“EEA state” means a state which is part of the European Economic Area;

“enforcement notice” means a written notice issued by the Commissioner under section 26 requiring specified actions to be taken;

“filing system” means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralised or dispersed on a functional or geographical basis;

“information notice” means a written notice issued by the Commissioner under section 27 requiring specified information to be provided to him;”

“manual data” means information that is recorded as part of a filing system or with the intention that it should form part of a filing system;

“the Minister” means the Minister with responsibility for Consumer Affairs and Civic Rights;

“personal data” means any information relating to a data subject;

“processing of personal data” (“processing”) means any operation or set of operations which is performed on personal data, whether or not by automatic means, including collecting, storing, recording, organising, consulting, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

“prohibition notice” means a written notice issued by the Commissioner under section 31 prohibiting the transfer of personal data to a state or territory outside Gibraltar;

“recipient” means a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

“right to privacy” means the right to respect for family, and private life, home and correspondence in accordance with Article 8 of the European Convention on Human Rights;

“statement of urgency” means a statement in an enforcement notice, information notice or prohibition notice to the effect that, by reason of special circumstances the Commissioner is of the opinion that the requirement specified in the notice should be complied with urgently;

“third party” means any natural or legal person, public authority, agency or any other body other than the data subject, the data controller, the data processor and the persons who, under the direct authority of the data controller or the data processor, are authorised to process the data.

### **Subject matter and Application of Act.**

3.(1) This Act shall apply to—

- (a) the processing of personal data wholly or partly by automatic means; and
- (b) the processing by non-automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

(2) Unless specifically provided, this Act shall not apply in relation to the processing of data by a natural person in the course of purely personal, family or household activity.

(3) Except as otherwise provided, this Act applies to the processing of personal data where—

- (a) the data controller is established in Gibraltar and the data is processed in the context of the activities of that establishment; or
- (b) the data controller is established outside Gibraltar, the United Kingdom or any EEA State, but makes use of equipment in Gibraltar for processing the data otherwise than solely for the purpose of transit through Gibraltar.

(4) A data controller falling within subsection (3)(b) shall nominate, for the purposes of this Act, a representative established in Gibraltar.

(5) For the purposes of subsections (3) and (4), each of the following is to be treated as established in Gibraltar—

- (a) an individual who is normally resident in Gibraltar;
- (b) a person who does not fall within paragraph (a), but maintains in Gibraltar—
  - (i) an office, branch or agency through which he carries on any activity, or
  - (ii) a regular practice,

and the reference to establishment in an EEA state shall be construed accordingly.

**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 16, 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 patient within the meaning of section 45 of the Mental Health Act 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 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 Rules on the Lawfulness of the Processing of Personal Data*

**Principles relating to Data Quality and Security.**

6.(1) A data controller shall, as respects personal data kept by him, comply with all of the following provisions—

- (a) the data, or as the case may be, the information constituting the data shall be obtained, and the data shall be processed fairly (including in accordance with section 10) and lawfully;
- (b) the data shall be accurate and complete and, where necessary, kept up to date;
- (c) the data shall—

- (i) be collected and kept only for one or more specified, explicit and legitimate purposes;
  - (ii) not be further processed in a manner incompatible with that purpose or purposes;
  - (iii) be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed; and
  - (iv) not be kept for longer than is necessary for that purpose or those purposes;
- (d) appropriate organisational and technical security measures shall be taken to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

(2) A data processor shall, as respects personal data processed by him, comply with subsection (1)(d).

(3)

- (a) Subsection (1)(c) (ii) and (iv) shall not apply to personal data which is kept for historical, statistical or scientific use provided that it is kept in a form which does not permit identification of the data subjects and is kept in accordance with any regulations or codes of conduct as may apply.
- (b) Data or information constituting such data shall not be regarded as having been obtained unfairly by reason only that its use for historical, statistical, research or other scientific purposes was not disclosed when it was obtained provided the data is not used in such a way that damage or distress is, or is likely to be caused, to any data subject.

(4) Subsection (1)(b) does not apply to back-up data.

## **Criteria for Making Data Processing Legitimate.**

7.(1) The processing of personal data is prohibited save where section 6 and section 11 on data quality and security are satisfied and at least one of the following conditions is met—

- (a) the data subject has unambiguously given his consent to the processing; or

- (b) the processing is necessary–
  - (i) for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
  - (ii) for compliance with a legal obligation to which the data controller is subject other than an obligation imposed by contract; or
- (c) the processing is necessary to prevent–
  - (i) injury or other damage to the health of the data subject; or
  - (ii) serious loss or damage to property of the data subject, or otherwise to protect his vital interests where the seeking of the consent of the data subject is likely to result in those interests being damaged; or
- (d) the processing is necessary-
  - (i) for the administration of justice;
  - (ii) for the performance of a function conferred on a person by or under an enactment;
  - (iii) for the performance of a function of the Government or a Minister of the Government;
  - (iv) for the performance of any other function of a public nature performed in the public interest by a person; or
- (e) processing is necessary for the purposes of the legitimate interests pursued by the controller or by third parties to whom the data are disclosed, except where such interests are overridden by the rights of the data subject under the European Convention on Human Rights or the Gibraltar Constitution Order 1969.

(2) The Minister may by regulations specify particular circumstances in which the provisions of subsection (1)(e) will, or will not, be satisfied.

#### **Sensitive Personal Data.**

8.(1) For the purpose of this Act the following shall be considered to be sensitive personal data –

- (a) data revealing racial or ethnic origin;
- (b) data revealing political opinions;
- (c) data revealing religious or philosophical beliefs;
- (d) data revealing trade-union membership;
- (e) data concerning health or sex life;
- (f) data concerning the commission or alleged commission of any offence by the data subject; and
- (g) data concerning any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

(2) The processing of sensitive personal data is prohibited save where sections 6 and 11 on data quality and data security are satisfied and at least one of the conditions in section 7(1) is met, and at least one of the following conditions is met—

- (a) the data subject has explicitly consented to the processing of the sensitive personal data;
- (b) the processing is necessary for the purposes of carrying out any legal obligation or right which is conferred or imposed by law on the data controller in connection with employment and the right of data subjects to privacy is safeguarded;
- (c) the processing is necessary to prevent injury or other damage to the health of the data subject or another person or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where—
  - (i) consent to the processing cannot be given by or on behalf of the data subject, or
  - (ii) the data controller cannot reasonably be expected to obtain such consent, or the processing is necessary to prevent injury to, or damage to the health of, another person, or serious loss in respect of or damage to, the property of another person, in a case where such consent has been unreasonably withheld;

- (d) processing is carried out in the course of the data controller's legitimate activities, in accordance with appropriate safeguards for the rights and freedoms of data subjects, and subject to such requirements as may be prescribed, by a non-profit-seeking body with a political, philosophical, religious or trade-union aim on condition that—
  - (i) the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes, and
  - (ii) the sensitive data is not disclosed to third parties without the consent of the data subject;
- (e) the information contained in the data has been made public as a result of steps deliberately taken by the data subject;
- (f) the processing is necessary—
  - (i) for the administration of justice,
  - (ii) for the performance of a function conferred on a person by or under an enactment, or
  - (iii) for the performance of a function of the Government or a Minister of the Government;
- (g) the processing—
  - (i) is required for the purpose of obtaining legal advice or for the purposes of, or in connection with, legal proceedings or prospective legal proceedings, or
  - (ii) is otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- (h) the processing of the sensitive data is required for the purposes of preventive medicine, medical diagnosis, the provision of medical care or treatment, medical research or the management of health-care services, and the sensitive personal data are processed—
  - (i) by a person registered under the Medical and Health Act 1989, who is under an enforceable obligation of professional secrecy, or

- (ii) by another person who, in the circumstances, owes a duty of confidentiality to the data subject which is equivalent to that in (i);
- (i) the processing is necessary in order to obtain information for use, subject to and in accordance with the Statistics Act, only for statistical, compilations and analysis purposes;
- (j) the processing is carried out by political parties, or candidates for election to, or holders of, elective political office in the course of electoral activities for the purpose of compiling data on people's political opinions on condition that the sensitive data is not disclosed to third parties, in a form which permits identification of the data subject, without the consent of the data subject;
- (k) the processing is necessary for the purpose of the assessment, collection or payment of any tax, duty, levy or other moneys owed or payable to the Crown and the data has been provided by the data subject solely for that purpose;
- (l) the processing is necessary for the purposes of determining entitlement to or control of, or any other purpose connected with the administration by the Crown of any benefit, pension, assistance, allowance, supplement or payment, or any non-statutory social security scheme; or
- (m) the processing is authorised by regulations that are made by the Minister and are made for reasons of substantial public interest.

(3) The Minister may make regulations to—

- (a) provide for additional exemptions to those provided in subsection (2) where necessary for reasons of substantial national interest, and
- (b) specify the particular circumstances in which the provisions of subsection (2) (m) will be satisfied.

Where such additional exemptions are made they shall be notified to the Commission.

(4) A complete register of criminal convictions may be kept only by the Royal Gibraltar Police.

## **Application of this Act in relation to Defence and National Security.**

9. Personal data are exempt from the provisions of—

- (a) sections 6 (except for section 6(1)(b)), 7 and 8,
- (b) section 10,
- (c) section 12,
- (d) sections 14 to 18,
- (e) section 24 and Part V,

if the exemption from that provision is required for the purposes of safeguarding defence or national security.

**Information to be given to the Data Subject.**

10.(1) Personal data shall not be treated, for the purposes of section 6(1)(a) of this Act, as processed fairly unless—

- (a) in the case of data obtained directly from the data subject, the data controller ensures, so far as practicable, that the data subject has, is provided with, or has made readily available to him, at least the information specified in subsection (2) of this section,
- (b) in any other case, the data controller ensures, so far as practicable, that the data subject has, is provided with, or has made readily available to him, at least the information specified in subsection (3)—
  - (i) not later than the time when the data controller first processes the data; or
  - (ii) if disclosure of the data to a third party is envisaged, not later than the time of such disclosure.

(2) The information referred to in subsection (1)(a) is—

- (a) the identity of the data controller;
- (b) if he has nominated a representative for the purposes of this Act, the identity of the representative;
- (c) the purpose or purposes for which the data are intended to be processed; and
- (d) any other information which is necessary, having regard to specific circumstances in which the data are or are to be

processed, to enable processing in respect of the data to be fair to the data subject such as information–

- (i) as to the recipients or categories of recipients of the data;
- (ii) as to whether replies to questions asked for the purpose of the collection of the data are obligatory;
- (iii) as to the possible consequences of failure to give such replies; and
- (iv) as to the existence of the right of access to and the right to rectify the data concerning him.

(3) The information referred to in subsection (1)(b) is–

- (a) the information specified in subsection (2);
- (b) the categories of data concerned; and
- (c) the name of the original data controller.

(4) Subsection (1)(b) does not apply–

- (a) where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of the information specified therein proves impossible or would involve a disproportionate effort, in the opinion of the Commissioner; or
- (b) in any case where the processing of the information contained or to be contained in the data by the data controller is necessary for compliance with a statutory obligation to which the data controller is subject. For the avoidance of doubt, this paragraph shall not apply to legal obligations imposed on the data controller by contract.

## **Security of Processing.**

11.(1) In determining appropriate organisational and technical security measures required by section 6(1)(d) and 6(2) data controllers and data processors–

- (a) shall have regard to the state of the technological development and the costs of implementing the measures;
- (b) shall ensure a level of security appropriate to–
  - (i) the risks represented by the processing;

- (ii) the harm which might result from accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access to, or of, the personal data concerned; and
- (iii) the nature of the data to be protected.

(2) A data controller or data processor shall take all reasonable steps to ensure that the following persons are aware of and comply with the relevant security measures–

- (a) persons employed by him; and
- (b) other persons at the place of work concerned.

(3) Where the processing of personal data is carried out by a data processor on behalf of a data controller, the data controller–

- (a) shall choose a data processor who provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out and must take reasonable measures to ensure compliance with those measures; and
- (b) shall ensure that the processing is only carried out under a written contract between the data processor and the data controller which stipulates that–
  - (i) the data processor will only act on and subject to instructions from the data controller; and
  - (ii) that the data processor complies with obligations equivalent to those imposed on the data controller by section 6(1)(d).

#### **Confidentiality of Processing.**

12(1) A person must not knowingly or recklessly, without the consent of the data controller–

- (a) obtain or disclose personal data or the information contained in personal data; or
- (b) procure the disclosure to another person of the data or information contained in the personal data.

(2) Subsection (1) does not apply to a person who shows–

- (a) that the obtaining, disclosing or procuring–
  - (i) was necessary for the purpose of preventing or detecting crime; or
  - (ii) was required or authorized by or under any enactment, by any rule of law or by the order of a court;
- (b) that he acted in the reasonable belief that he had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the data or information to the other person;
- (c) that he acted in the reasonable belief that he would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it; or
- (d) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

(3) A person who contravenes subsection (1) is guilty of an offence.

(4) A person who sells personal data, or information extracted from personal data, is guilty of an offence if he has obtained the data in contravention of subsection (1).

(5) A person who offers to sell personal data, or information extracted from personal data, is guilty of an offence if–

- (a) he has obtained the data in contravention of subsection (1), or
- (b) he subsequently obtains the data in contravention of that subsection.

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

(7) References to personal data in this section do not include references to personal data which is exempted by virtue of section 9.

## **Freedom of Journalistic, Artistic and Literary Expression.**

13.(1) Personal data that are processed only for journalistic, artistic or literary purposes shall be exempt from compliance with any provision of this Act specified in subsection (2) if–

- (a) the processing is undertaken solely with a view to the publication of any journalistic, literary or artistic material,
- (b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, such publication would be in the public interest, and
- (c) the data controller reasonably believes that, in all the circumstances, compliance with that provision would be incompatible with journalistic, artistic or literary purposes.

(2) The provisions referred to in subsection (1) are—

- (a) section 6, other than subsection (1)(d),
- (b) sections 7 to 8,
- (c) section 10,
- (d) sections 12, 14 to 18,
- (e) section 24,
- (f) section 30.

(3) In considering for the purposes of subsection (1)(b) of this section whether publication of the material concerned would be in the public interest, regard may be had to any code of practice approved under this Act.

(4) In this section “publication”, in relation to journalistic, artistic or literary material, means the act of making the material available to the public or any section of the public in any form or by any means

### **Part III**

#### *Data Subject's Rights*

#### **Access.**

14.(1) An individual who believes that a person keeps personal data shall, on written request to that person—

- (a) be informed by the person whether he keeps any such data; and
- (b) if he does, be given by the person a description of the data and the purposes for which they are kept.

The response must be given in writing within a reasonable period, and in any event, not more than 21 days after receipt of the request.

(2) An individual who makes a written request to a data controller shall be informed in writing whether personal data relating to him is being processed by, or on behalf of, the data controller. The data controller shall provide a written response within 21 days of receipt of the request.

(3) If data relating to any individual making a request under (2) is being processed by, or on behalf of, the data controller, the data controller shall, in writing—

- (a) provide him with—
  - (i) a description of the purpose or purposes of the processing;
  - (ii) a description of the categories of data being processed by or on behalf of the data controller;
  - (iii) a description of the recipients or categories of recipients to whom the data are disclosed;
  - (iv) in intelligible form, the information constituting any personal data of which he is the data subject; and
  - (v) any information known or available to the data controller as to the source of those personal data save as provided by this Act; and
- (b) communicate to him, in terms intelligible to the average person, the logic involved in any automatic processing of that data. There is no requirement to provide information which will adversely affect trade secrets or intellectual property (in particular any copyright protecting computer software);
- (c) a data controller is only obliged to comply with the requirements of subsection 3(b) where the personal data concerned has constituted or is likely to constitute the sole basis for any decision significantly affecting the data subject. In these circumstances the information in subsection 3(b) shall be provided free of charge.

(4) A request under subsection (3) shall be complied with by a data controller within 28 days of receipt of the request.

(5) A request under subsection (2) that does not relate to all of the subparagraphs of subsections (3) shall, in the absence of any indication to the contrary, be treated as relating to all of them.

(6) A fee—

- (a) may be payable to the data controller concerned in respect of a request made under subsection (2). The amount thereof shall not exceed such amount as in the opinion of the Commissioner is reasonable, having regard to the estimated cost to the data controller of compliance with the request;
- (b) paid by a person to a data controller under paragraph (a) of this paragraph shall be returned to him—
  - (i) if his request is not complied with within the specified time; or
  - (ii) if, on an application made by him or in accordance with an enforcement notice or a court order, the data controller rectifies, supplements, erases part of the data concerned (thereby materially modifying the data) or erases all of the data.

(7) Where, pursuant to provisions made under this Act, there are separate entries in the register in respect of data kept by a data controller for different purposes, this section shall apply as if it provided for the making of a separate request and the payment of a separate fee in respect of the data to which each entry relates.

(8) An individual making a request under this section 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.

(9) 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 as aforesaid 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.

(10)

- (a) Where personal data relating to a data subject consists of an expression of opinion about the data subject by another person, the data may be disclosed to the data subject without obtaining the consent of that person to the disclosure.
- (b) Paragraph (a) of this subsection does not apply—
  - (i) if the expression of opinion referred to in that paragraph was given in confidence or on the understanding that it would be treated as confidential; or
  - (ii) to personal data held by or on behalf of the person in charge of a prison or other place of criminal detention and consisting of an expression of opinion by another person about the data subject if the data subject is being or was detained in such an institution.

(11) Information supplied pursuant to a request under subsection (2) of this section may take account of any amendment of the personal data concerned made since the receipt of the request by the data controller (being an amendment that would have been made irrespective of the receipt of the request) and any amendment made pursuant to sub-section (9)(a), but not of any other amendment.

(12)

- (a) A request under subsection (2) in relation to the results of an examination at which the data subject was a candidate shall be deemed, for the purposes of this section, to be made on—
  - (i) the date of the first publication of the results of the examination, or
  - (ii) the date of the request, whichever is the later; and subsection (2) shall be construed and have effect in relation to such a request as if for "21 days" there were substituted "60 days".
- (b) In this subsection "examination" means any process for determining the knowledge, intelligence, skill or ability of a

person by reference to his performance in any test, work or other activity.

(13)

- (a) Where the data controller is the Crown acting in its executive capacity nothing in this section shall oblige it to disclose personal data where the refusal to disclose is necessary in the interests of—
- (i) public security;
  - (ii) the prevention, investigation, detection and prosecution of criminal offences or breaches of ethics for regulated professions;
  - (iii) an important economic or financial interest of Gibraltar or of the European Union including monetary, budgetary and taxation matters;
  - (iv) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (i), (ii) and (iii); or
  - (v) the protection of the data subject or of the rights and freedoms of others.
- (b) Paragraph (a) will not apply in any case where it would result in the breach of the data subject's fundamental rights and freedoms, in particular those under Article 8 of the European Convention on Human Rights.

(14)

- (a) Where a data controller has previously complied with a request under subsection (2), the data controller is not obliged to comply with a subsequent identical or similar request under that subsection 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.
- (b) In determining whether a reasonable interval of time has elapsed, 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.

(15)

- (a) A person shall not, in connection with—
  - (i) the recruitment of another person as an employee;
  - (ii) the continued employment of another person; or
  - (iii) a contract for the provision of services to him by another person,  
  
require that other person to make a request under subsection (2), or to supply him with data relating to that other person obtained as a result of such a request.
- (b) A person who contravenes paragraph (a) of this subsection shall be guilty of an offence.

(16) Where a data controller refuses a request for information made under this section he shall, in writing, notify the individual making the request of the refusal. The notification shall include—

- (a) a statement of the reasons for refusal, save where such a statement would undermine the reasons for the refusal; and
- (b) a statement that the individual may complain to the Commissioner about the refusal.

### **Rectification etc. of Data.**

15.(1) A data controller must, on request from a data subject or his representative rectify, erase or block data in relation to which there has been a contravention of this Act, in particular because the data is incomplete or inaccurate. Such rectification, erasure or blocking of data must take place within 28 days from receipt of the request.

(2) Where a data controller has complied with a request made under subsection (1), he must, within 35 days from receipt of the request, enforcement notice or court order, notify in writing the following persons—

- (a) the person making the request; and
- (b) any third party or parties to whom the data have been disclosed within the period of 12 months immediately before the giving or sending of the request of the rectification, erasure or blocking, as soon as possible, unless this proves impossible or involves a disproportionate effort.

(3) The data subject may complain to the Commissioner if a data controller—

- (a) has not complied with a request made under subsection (1) within the prescribed time period, or at all; or
- (b) has not notified recipients of the personal data of the rectification, erasure or blocking of the data in compliance with subsection (2)(b).

**Data Subject's Right to Object.**

16.(1) An individual is entitled at any time, unless otherwise provided by any enactment, to request a data controller to cease within a reasonable time, or not to begin, processing or processing for a specified purpose or in a specified manner any personal data in respect of which he is the data subject if the processing falls within subsection (2) on the ground that, for specific reasons—

- (a) the processing of those data or their processing for the purpose or in that manner is causing or likely to cause substantial damage or substantial distress to him or to another person; and
- (b) the damage or distress is or would be unwarranted.

(2) This section applies to processing that is necessary—

- (a) for—
  - (i) the administration of justice;
  - (ii) the performance of a function conferred on a person by or under any enactment;
  - (iii) the performance of a function of the Government or a Minister of the Government;
  - (iv) the performance of any other function of a public nature performed in the public interest by a person; or
- (b) for the purposes of the legitimate interests pursued by the data controller or by third parties to whom the data are disclosed, except where such interests are overridden by the rights of the data subject under the European Convention on Human Rights or the Gibraltar Constitution Order 1969.

(3) Subsection (1) does not apply—

- (a) if the data subject has given his unambiguous consent to the processing;
- (b) if the processing is necessary—
  - (i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; or
  - (ii) for compliance with a legal obligation to which the data controller is subject other than an obligation imposed by contract;
- (c) the processing is necessary to prevent—
  - (i) injury or other damage to the health of the data subject or other individual; or
  - (ii) serious loss or other damage to property of the data subject or other person, or otherwise to protect his vital interests where the seeking of the consent of the data subject or another person referred to in subsection (1)(a) is likely to result in those interests being damaged;
- (d) to processing carried out by political parties, or candidates for election to, or holders of elective office, in the course of electoral activities; or
- (e) in such other cases, if any, as may be specified in regulations made by the Minister.

(4) A request to a data controller under subsection (1) shall be made in writing. Where such a request is served on a data controller, he shall, as soon as practicable, and in any event not later than 21 days after the receipt of the request, inform the individual making the request, in writing—

- (a) that he has complied or intends to comply with the request concerned; or
- (b) that he does not intend to comply, or comply fully, with the request concerned since he considers the request is unjustified, or partly unjustified. Where this paragraph applies the notification must include—
  - (i) the data controller's opinion;
  - (ii) brief reasons for the opinion;

- (iii) the extent (if any) to which he has complied or intends to comply with the request; and
- (iv) a statement explaining that the individual may complain to the Commissioner and giving details of how to complain.

(5) If a complaint is made to him by or on behalf of an individual who has made a request under subsection (1), and the Commissioner is satisfied that the requirements of paragraph (a) are met, he may serve an enforcement notice on the data controller pursuant to section 26 containing the information set out in paragraph (b).

- (a) The requirements are that the Commissioner is satisfied that—
  - (i) the request is justified, or justified to any extent;
  - (ii) the data controller has failed to comply or comply fully with the request; and
  - (iii) more than 28 days have elapsed since the request was given or sent to the data controller.
- (b) The information is—
  - (i) an order that the data controller takes such steps for complying with the request, or for complying with it to such extent, as the Commissioner thinks fit and specifies in the enforcement notice; and
  - (ii) the Commissioner's reasons for issuing the enforcement notice.

### **Direct Marketing.**

17.(1) An individual may, at any time, in relation to personal data in respect of which he is the data subject, require a data controller to cease or not begin processing that personal data for the purposes of direct marketing. The request to the data controller must be made in writing and the data controller must comply with the request as soon as may be and in any event within 28 days after the receipt of the request.

(2) Where a request has been made under subsection (1) in respect of personal data which is kept for the sole purpose of direct marketing then that data shall be erased as soon as may be and in any event within 28 days of receipt of the request. Data recording a data subject's request under (1) are not required to be deleted.

(3) Where a request has been made under subsection (1) the data controller shall, as soon as may be and in any event within 35 days of receipt of the request, inform the data subject in writing of the action which has been taken on his request.

(4) Where a data controller anticipates that personal data which is kept by him, including personal data that is required by law to be made available to the public, may be processed for the purposes of direct marketing, the data controller shall inform the individuals to whom the data relates that they may object to such processing free of charge, by means of a request in writing to the data controller.

(5) Requests made under subsection (1) shall be complied with without any fee being requested by the data controller.

(6) Where a data controller fails to comply with a request made under subsection (1) or makes a charge the data subject may complain to the Commissioner.

## **Decisions based solely on automatic processing of data.**

18.(1) Subject to subsection (2), a decision which produces legal effects concerning a data subject or otherwise significantly affects a data subject may not be based solely on processing by automatic means of personal data intended to evaluate certain personal matters relating to him such as, for example (but without prejudice to the generality of the foregoing), his performance at work, creditworthiness, reliability or conduct.

(2) Subsection (1) does not apply–

(a) if the data subject consents to the processing referred to in subsection (1); or

(b) in a case in which a decision referred to in subsection (1)–

(i) is made in the course of steps taken–

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

(bb) in the course of performing such a contract,

and adequate steps have been taken to safeguard the data subject's legitimate interests, for example (but without prejudice to the generality of the foregoing), allowing him to

make representations to the data controller in relation to the proposal; or

- (ii) is authorised or required by law and the data subject has been informed of the proposal to make the decision; and either—
  - (aa) the effect of the decision is to grant a request made by the data subject; or
  - (bb) adequate steps have been taken to safeguard the data subject's legitimate interests, for example (but without prejudice to the generality of the foregoing), allowing him to make representations to the data controller in relation to the proposal.

(3) A data subject may complain to the Commissioner if he believes that a decision has been, or will be, made contrary to this section.

**Exemptions from prohibitions on processing and Data Subjects' Rights.**

19.(1) Personal data processed for the purposes set out in subsections (2) to (8) are exempt from compliance with the following sections of this Act to the extent that compliance would be likely to prejudice the proper discharge of those functions or prejudice those purposes—

- (a) section 6;
- (b) section 10;
- (c) section 14;
- (d) section 15;
- (e) section 24.

(2) Personal data processed for the purpose of—

- (a) preventing, detecting or investigating offences, apprehending or prosecuting offenders, sentencing offenders or detaining offenders of persons alleged to have committed an offence; or
- (b) assessing or collecting any tax, duty or other moneys owed or payable to the Crown or a person conducting a relevant function.

(3) Personal data processed for the purposes of discharging any relevant function designed—

- (a) to protect members of the public against—

- (i) 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 including any activity falling within Schedule 3 of the Financial Services Act 1989;
  - (ii) financial loss due to the conduct of discharged or undischarged bankrupts; or
  - (iii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, person authorised to carry on any profession or other activity;
- (b) for–
- (i) protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration;
  - (ii) protecting the property of charities from loss or misapplication; or
  - (iii) the recovery of the property of charities.

(4) For the purposes of subsection (2)(b) and subsection (3) “relevant function” means–

- (a) any function conferred on any person by or under law;
- (b) any function of the Crown, any Minister or government department; or
- (c) any other function which is of a public nature and is exercised in the public interest.

(5) Personal data which is processed for the purpose of discharging any function conferred by law on the Ombudsman and is designed to protect members of the public against–

- (a) mal administration 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 was a function of the body to provide.

(6) Personal data required–

- (a) by order of a court;
- (b) for the purposes of obtaining legal advice;
- (c) for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or witness.

(7) Personal data required to prevent injury or other damage to the health of a person or serious loss of or damage to property.

(8) Personal data disclosed—

- (a) to the data subject concerned or to a person acting on his behalf; or
- (b) at the request of, or with the consent of, the data subject or a person acting on his behalf.

**Power to make additional Exemptions & Restrictions: Data Quality, Rights of data subjects, publicising of processing operations.**

20.(1) The Governor may provide by regulations for the restriction of the rights and freedoms set out in sections 6, 10, 14, 15, 16, 24 where necessary to safeguard defence, national or public security.

(2) The Minister may provide by regulations for the restriction of the rights and freedoms set out in sections 6, 10, 14, 15, 16, 24 where necessary to safeguard—

- (a) the prevention, investigation, detection and prosecution of criminal offences or breaches of ethics for regulated professions;
- (b) an important economic or financial interest of Gibraltar or of the European Union including monetary, budgetary and taxation matters;
- (c) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b) and (c);
- (d) the protection of the data subject or of the rights and freedoms of others;
- (e) public safety.

## **Part IV**

### *Supervisory Authority*

#### **Supervisory Authority.**

21.(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 Data Protection Commissioner shall be the Gibraltar Regulatory Authority who shall perform the functions conferred by this Act and any regulations enacted under it.

(3) The provisions of Schedule 1 shall have effect in relation to the Commissioner.

#### **Data Protection Register.**

22.(1) The Commissioner shall establish and maintain a register (“the Register”) of processing operations and shall make, as appropriate, an entry in the register in respect of each application for registration accepted by the Commissioner. The entry shall contain the information specified in section 23(3)(a) – (e).

(2) Members of the public may–

- (a) inspect the Register free of charge at all reasonable times and may take copies of, or of extracts from, any entry in the Register;
- (b) on payment to the Commissioner of any reasonable fee prescribed, obtain from the Commissioner a copy (certified by him or by a member of his staff to be a true copy) of, or of an extract from, any entry in the Register.

(3) In any proceedings a copy of, or of an extract from, an entry in the register certified by the Commissioner or by a member of his staff to be a true copy shall be evidence of the entry or extract.

(4) In any proceedings a certificate signed by the Commissioner or by a member of his staff stating that there is no entry in the register in respect of a specified person as a data controller or as a data processor shall be evidence of that fact.

#### **Application for Registration.**

23.(1) A person wishing to register a processing operation on the Register or to have the particulars of an entry in the Register altered shall apply to

the Commissioner, in writing, or as may otherwise be required by procedures adopted by the Commissioner in accordance with subsection (8).

(2) A person wishing to register a prescribed processing operation on the Register or to have the particulars of any such entry in the Register altered—

- (a) shall apply to the Commissioner for prior checking of his application if he intends to carry out prescribed processing operations; and
- (b) shall not carry out prescribed processing operations until—
  - (i) he has been notified by the Commissioner that the application for registration is accepted; or
  - (ii) a period of 28 days, or such other period as the Minister may specify in the regulations, has passed since receipt by the Commissioner of the application.

In this subsection a “prescribed processing operation” means processing of a description specified in regulations made by the Minister. Where paragraph (b) is contravened, the data controller is guilty of an offence.

(3) Applications for registration of a processing operation shall include—

- (a) the name and address of the data controller and his representative, if any;
- (b) a description of the personal data being or to be processed by or on behalf of the data controller and of the category or categories of data subject to which they relate;
- (c) a description of the purpose or purposes of the processing;
- (d) a description of the recipients or categories of recipient to whom the data controller intends or may wish to disclose the data;
- (e) the names of any countries or territories outside the EEA to which the data controller transfers or intends or may wish to transfer the data;
- (f) a description of the security measures taken in compliance with section 11 which is adequate to allow a preliminary assessment of those security measures; and
- (g) such other information as is reasonably required by the Commissioner.

(4) The Commissioner shall accept any application made in the manner provided for in subsection (8) and in respect of which any fee payable has been paid except where—

- (a) the particulars proposed for inclusion in the register are insufficient or any other information required by him has not been provided or is insufficient; or
- (b) the application is one to which subsection (2) applies and the applicant for registration is likely to contravene any of the provisions of this Act.

(5) In a case—

- (a) to which subsection (1) applies the deemed entry in the Register provided for in section 24(3) shall expire on receipt by the data controller of written notification from the Commissioner that the application is not in accordance with the requirements of subsection (4) and the written notification shall—
  - (i) specify the reasons that the application is not in accordance with the requirements of subsection (4); and
  - (ii) state that the applicant may appeal to the Court under section 32 within 21 days from the date that the notification is received by him;
- (b) to which subsection (2) applies where the Commissioner refuses an application for registration he shall, within 28 days from the receipt by him, or such other period as the Minister may specify in regulations, of the application notify the applicant in writing of the refusal of the application. and the written notification shall—
  - (i) specify the reasons for the refusal; and
  - (ii) state that the applicant may appeal to the Court under section 32 within 21 days from the date that the notification is received by him.

(6) The Commissioner may—

- (a) at any time, on the request of the person to whom an entry relates, remove that entry from the register;

- (b) where a data controller or data processor, or an entry, has been found by the Commissioner or Court not to comply with this Act, remove it or him from the Register;
- (c) if provided for by Regulations made by the Minister, remove obsolete or redundant entries in the Register for the purpose of ensuring the accuracy of the Register.

(7) It is the responsibility of the data controller to notify the Commissioner of changes in the information listed in subsection (3).

(8) Procedures for applications for registration, or notification of changes to information in subsection (3) shall be such as the Commissioner may require and such requirements shall be publicised.

**Obligation to Register.**

24.(1) This section applies to data controllers except—

- (a) where they carry out—
  - (i) processing the sole purpose of which is the keeping, under any enactment, of a register that is intended to provide information to the public and is open to consultation either by the public in general or by any person demonstrating a legitimate interest;
  - (ii) processing of wholly manual data, other than such categories, if any, of such data as may be prescribed by regulation or Act; or
  - (iii) any combination of the foregoing categories of processing;
- (b) where the data controller is a body that is not established or conducted for profit and is carrying out processing only for the purposes of establishing or maintaining membership of or support for the body or providing or administering activities for individuals who are either members of the body or have regular contact with it;
- (c) as provided by regulations made under section 20;
- (d) as provided by regulations made under section 36(3); or
- (e) as provided by section 9 or 19.

(2) Data controllers who, by virtue of subsection (1), are exempt from the obligation to register their processing operations in the Register must make available the information set out in section 23(3)(a)-(e) in an appropriate and intelligible form to any person on request.

(3) Data controllers to whom this section applies, their employees and agents, shall not process personal data unless there is an entry in the Register in respect of the processing operation. An entry in the Register shall be deemed to exist in respect of any processing operation or any notification of changes to a registered processing operations which is notified in accordance with section 23(7) as from—

- (a) the date on which an application or notification in the form and manner required by section 23(4) has been submitted to the Commissioner; or
- (b) from such date after the submission of an application or notification as the Minister may provide by Regulations.

This subsection does not apply to prescribed processing operations described in section 23(2)(a).

(4) A person who contravenes subsection (3) is guilty of an offence.

(5) The Minister may provide by regulations that subsections (3) and (4) do not apply to particular categories of processing operations which are unlikely to adversely affect –

- (a) data subjects' rights under this Act; or
- (b) data subjects' rights under the European Convention on Human Rights or the Gibraltar Constitution Order 1969.

## **Part V**

### *Powers of Supervisory Authority*

#### **Investigations, Mediation and Compensation.**

25.(1) The Commissioner may carry out or cause to be carried out such investigations as he considers appropriate in order to ensure compliance with, and to identify any contravention(s) of, the provisions of this Act irrespective of whether or not a complaint has been made.

(2) Where an individual complains to the Commissioner that there has been, or is likely to be, a contravention of this Act in relation to him—

- (a) the Commissioner shall investigate the complaint, or cause it to be investigated, unless it is frivolous or vexatious, and
  - (b) if the Commissioner is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the complaint, he shall notify the parties in writing of his decision in relation to it and either party may, if aggrieved by the decision, appeal against it to the Magistrates' Court under section 32(1).
- (3) A data subject who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for the damage suffered.
- (4)
- (a) A compensation order is a decision made by the Commissioner that a data controller shall pay compensation to a data subject.
  - (b) The Commissioner may make a compensation order where he considers that a data subject has suffered damage by reason of any contravention by a data controller of any of the requirements of this Act.
  - (c) No compensation order shall be made where a data controller proves that he had taken such care as in all the circumstances was reasonably required to comply with the requirement, or requirements, of the Act concerned.
  - (d) The Commissioner shall notify parties in writing of his decision in relation to a compensation order and either party may, if aggrieved by the decision, appeal against it to the Supreme Court under section 32(5).

**Enforcement Notices.**

26.(1) If the Commissioner is of the opinion that a person has contravened or is contravening a provision of this Act he may, by notice in writing (referred to in this Act as an "enforcement notice") served on the person require him to take such steps to comply with the provision concerned as are specified in the notice, within such time as is specified.

(2) Without prejudice to the generality of subsection (1), if the Commissioner is of the opinion that a data controller has contravened section 6(1) of this Act, the relevant enforcement notice may require him—

- (a) to block, rectify, erase or destroy any of the data concerned; or

- (b) to supplement the data with such statement relating to the matters dealt with by them as the Commissioner may approve of, and as respects data that are inaccurate or not kept up to date, if he supplements them as aforesaid, he shall be deemed not to be in contravention of section 6(1)(b).

(3) An enforcement notice shall—

- (a) specify any provision of this Act that, in the opinion of the Commissioner, has been or is being contravened and the reasons for his having formed that opinion, and
- (b) subject to subsection (5), state that the person concerned may appeal to the Supreme Court under section 32(1) against the requirement specified in the notice within 21 days from the service of the notice on him.

(4) Subject to subsection (5), the time specified in an enforcement notice for compliance with any requirement specified therein shall not expire before the end of the period within which a person may appeal and, if such an appeal is brought, the enforcement notice need not be complied with, and subsection (8) shall not apply in relation thereto, prior to the determination or withdrawal of the appeal.

(5)

- (a) Where the Commissioner, by reason of special circumstances, is of the opinion that a requirement in the enforcement notice should be complied with urgently he shall include in the enforcement notice—
  - (i) a statement to this effect (“a statement of urgency”) and brief reasons for his opinion; and
  - (ii) the period within which the requirement must be complied with which must be at least 7 days from the date of service of the enforcement notice.
- (b) Where an enforcement notice contains a statement of urgency—
  - (i) subsections (3)(b) and (4) of this section do not apply; and
  - (ii) the enforcement notice shall state that the person concerned may appeal to the Supreme Court under section 32 against the requirement specified in this notice, or the making of the statement of urgency, within 7 days from service of the notice.

(6) On compliance by a data controller with a requirement under subsection (2), he shall, as soon as may be and in any event not more than 35 days after such compliance, notify—

- (a) the data subject concerned, and
- (b) if such compliance materially modifies the data concerned, any person to whom the data were disclosed during the period beginning 12 months before the date of service of the enforcement notice concerned and ending immediately before such compliance, unless such notification proves impossible or involves a disproportionate effort,

of the blocking, rectification, erasure, destruction or statement concerned.

(7) The Commissioner may cancel an enforcement notice and, if he does so, shall notify in writing the person on whom it was served accordingly.

(8) A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an enforcement notice shall be guilty of an offence.

### **Information Notices.**

27.(1) The Commissioner may, as is necessary or expedient for the purpose of performing his functions under this Act, by notice in writing (referred to as an “information notice”) served on a person, require that person to furnish to him in writing such information as is specified in the information notice within such time specified in the information notice.

(2) Subject to subsection (3) an information notice—

- (a) shall state that the person to whom it is addressed may appeal to the Supreme Court under section 32 against any requirement therein within 21 days; and
- (b) need not be complied with before the end of the period during which an appeal may be brought under subsection (2)(a) and, if an appeal is brought under subsection (2)(a) need not be complied with before the determination of the appeal.

(3)

- (a) Where the Commissioner, by reason of special circumstances, is of the opinion that a requirement in the information notice should be complied with urgently he shall include in the information notice—

- (i) a statement to this effect (“a statement of urgency”) and brief reasons for his opinion;
  - (ii) the period within which the requirement must be complied with which must be at least 7 days from the date of service of the information notice;
- (b) Where an information notice contains a statement of urgency–
- (i) subsection (2) of this section does not apply; and
  - (ii) the information notice shall state that the person concerned may appeal to the Supreme Court under section 32 against the requirement specified in the notice, or the making of the statement of urgency, within 7 days from service of the notice
- (4) 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 (a) does not apply to information which is, or at any time was, kept for the purpose of safeguarding the security of Gibraltar or information which is privileged from disclosure in court proceedings.
- (5) A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an information notice or who in purported compliance with such a requirement furnishes information to the Commissioner knowing it to be false or misleading in a material respect shall be guilty of an offence.

## **Information and Codes of Practice.**

28.(1) The Commissioner may, in such manner and by such means as he considers most effective, promote the following of good practice by data controllers and data processors so as to promote compliance with this Act including through–

- (a) drawing up Codes of Practice as to good practice in processing personal data in consultation with interested parties;
- (b) disseminating information to data controllers and the public about data protection;

- (c) giving advice with regard to data protection and matters covered by this Act.

(2) The Commissioner shall arrange for the dissemination in such manner and by such means as he considers most effective of –

- (a) any Community finding (as defined in section 30(2)) in relation to transfers of data to a country or territory outside the EEA;
- (b) any decision of the European Commission under the procedure provided for in Article 31(2) of the Directive that is made for the purposes of paragraphs 3 and 4 of Article 26 of the Directive; and
- (c) such other information as appears to him expedient to give data controllers in relation to transfers of data to a country or territory outside the EEA.

(3) The Commissioner shall 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.

(4) 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;
- (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.

(5) 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.

(6) The Commissioner may request any reasonable fee in respect of services provided under this section. The fee shall be–

- (a) as the Minister may approve from time to time, and

- (b) different fees may be requested in relation to different services and different classes of persons.

## **Authorised Officers.**

29.(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) The Minister may provide by Regulations for authorised officers to have such powers to enter, inspect, search premises, inspect, 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 Minister 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 regulations made under 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.

## **Part VI**

### *Transfer of Personal Data to Third Countries*

#### **Transfer of Personal Data.**

30.(1) The transfer of personal data by a data controller to a country or territory outside Gibraltar may not take place unless—

- (a) the country is a member of the EEA; or
- (b) the country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to—
  - (i) the nature of the data;
  - (ii) the purposes and length of time for which the data are intended to be processed;
  - (iii) the country or territory of origin of the information contained in the data;

- (iv) the country or territory of final destination of that information;
- (v) the law in force in the country or territory;
- (vi) the international obligations of that country or territory;
- (vii) any relevant codes of conduct or other rules which are enforceable in the country or territory;
- (viii) any security measures taken in respect of the data in the country or territory; and
- (ix) the international obligations of the country or territory.

(2) “Community finding” means a finding of the European Commission under Article 25(6) of the Directive and in accordance with the procedure provided for in Article 31(2) of the Directive in relation to whether the adequate level of protection specified in subsection (1) is ensured by a country or territory outside the EEA.

- (3) Where in any proceedings under this Act a question arises whether–
- (a) the adequate level of protection specified in subsection (1) is ensured by a country or territory outside the EEA to which personal data are to be transferred, and
  - (b) a Community finding has been made in relation to transfers of the kind in question,

the question shall be determined in accordance with that finding.

(4) The Commissioner shall inform the Commission and the supervisory authorities of the other Member States of any case where he considers that a third country does not ensure the adequate level of protection referred to in subsection (1) of this section.

- (5) Section 30(1) shall not apply if–
- (a) the data subject has unambiguously consented to the transfer;
  - (b) the transfer is necessary–
    - (i) for the performance of a contract between the data subject and the data controller;

- (ii) for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller; or
- (iii) for the agreement or performance of a contract concluded at the request of, and in the interest of, the data subject between the data controller and a person other than the data subject ;
- (c) the transfer of the data or the information constituting the data is required by any convention or other instrument imposing an international obligation on Gibraltar to transfer the data;
- (d) the transfer is necessary for reasons of substantial public interest;
- (e) the transfer is necessary for the purposes of obtaining legal advice or for the purposes of or in connection with legal proceedings or prospective legal proceedings or is otherwise necessary for the purposes of establishing or defending legal rights;
- (f) the transfer is necessary in order to prevent injury or other damage to the health of the data subject or serious loss or damage to property of the data subject or otherwise to protect his vital interests, and informing the data subject of, or seeking his consent to, the transfer is likely to damage those vital interests;
- (g) the transfer is of part only of the personal data on a register established by or under an enactment, being—
  - (i) a register of information open to consultation by the public, or
  - (ii) a register of information open to consultation by persons having a legitimate interest in its subject matter,and, in the case of a register referred to in (ii) of this subparagraph, the transfer is made, at the request of, or to, a person referred to in (ii) and any conditions to which such consultation is subject are complied with by any person by whom the data are or are to be transferred; or
- (h) the transfer has been authorised by the Commissioner where the data controller has adduced adequate safeguards with respect to and for the exercise by individuals of their rights under this Act or the transfer is made on terms of a kind

approved by the Commissioner as ensuring adequate safeguards for the rights of data subjects.

The Commissioner shall—

- (i) in deciding whether a contractual clause offers sufficient safeguards, comply with any decision of the European Commission made for the purpose of deciding whether certain contractual clauses offer sufficient protection for data subjects under the procedure laid down in Article 31.2 of the Directive;
- (ii) inform the European Commission and the supervisory authorities of the other states in the EEA of any authorisation or approval under this paragraph.

(6) The Minister may, after consultation with the Commissioner, by regulations specify the circumstances in which a transfer of data is necessary for reasons of substantial public interest for the purposes of subsection (5)(d).

(7) Where, in relation to a transfer of data to a third country, a data controller adduces the safeguards for the data subject concerned referred to in subsection (5)(h) by means of a contract embodying the contractual clauses referred to in paragraph 2 or 4 of Article 26 of the Directive, the data subject shall have the same right—

- (a) to enforce a clause of the contract conferring rights on him or her relating to such rights, and
- (b) to compensation or damages for breach of such a clause,

that he would have if he was a party to the contract.

#### **Prohibition of Data transfers.**

31.(1) The Commissioner may, subject to the provisions of this Part, prohibit the transfer of personal data from Gibraltar to a place outside Gibraltar unless such transfer is —

- (a) to a country or territory covered by 30(1); or
- (b) required or authorised by or under any enactment or required by any convention or other instrument imposing an international obligation on Gibraltar.

(2) In determining whether to prohibit a transfer of personal data, the Commissioner shall—

- (a) consider the provisions of this Act;
- (b) consider whether the transfer would be likely to cause damage or distress to any person; and
- (c) have regard to the desirability of facilitating international transfers of data.

(3) A prohibition under subsection (1) shall be effected by the service of a notice (referred to as “a prohibition notice”) on the person proposing to transfer the data concerned.

(4) A prohibition notice shall—

- (a) prohibit the transfer concerned either absolutely or until the person aforesaid has taken such steps as are specified in the notice for protecting the interests of the data subjects concerned;
- (b) specify the time when it is to take effect;
- (c) specify the grounds for the prohibition; and
- (d) subject to subsection (6), state that the person concerned may appeal to the Supreme Court under section 32 against the prohibition specified in the notice within 21 days from the service of the notice on him.

(5) Subject to subsection (6), the time specified in a prohibition notice for compliance with the prohibition specified therein shall not be expressed to expire before the end of the period of 21 days specified in subsection (4)(d) and, if an appeal is brought against the prohibition, the prohibition need not be complied with and subsection (8) shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(6)

- (a) If the Commissioner, by reason of special circumstances, is of the opinion that a prohibition specified in a prohibition notice must be complied with urgently he shall include in the prohibition notice—
  - (i) a statement to this effect (“a statement of urgency”) and brief reasons for his opinion, and
  - (ii) the period within which the prohibition must be complied with which must be at least 7 days from the date of service of the prohibition notice.

- (b) where a prohibition notice includes a statement of urgency—
  - (i) subsections (4) (d) and (5) shall not apply in relation to the notice, and
  - (ii) the prohibition notice shall state that the person concerned may appeal to the Supreme Court under section 32 against the prohibition within 7 days from service of the notice, and

(7) The Commissioner may cancel a prohibition notice and, if he does so, shall notify in writing the person on whom it was served accordingly.

(8) A person who, without reasonable excuse, fails or refuses to comply with a prohibition specified in a prohibition notice shall be guilty of an offence.

## PART VII

### *Judicial Remedies, Liability and Sanctions*

#### **Appeals.**

32.(1) An appeal may be made to and determined by the Magistrates' Court against—

- (a) a requirement specified in an enforcement notice or an information notice,
- (b) a prohibition specified in a prohibition notice,
- (c) a refusal by the Commissioner to register a data controller under section 23,
- (d) a decision of the Commissioner to remove a data controller from the register under section 23,
- (e) a refusal by the Commissioner to investigate a complaint under section 25(2)(a),
- (f) a decision of the Commissioner under section 25(2)(b),

and such appeal shall be brought within 21 days from the service on the person concerned of the relevant notice, save where subsection (2) applies.

(2) Where an appeal is brought under subsection (1) in respect of a notice or notification which contains an urgency statement then such appeal shall be brought within 7 days from the service on the person concerned of the relevant notice.

(3) Notwithstanding any provision of this Act, where—

- (a) a person appeals to the Court pursuant to subsection (1), and
- (b) the Commissioner has included an urgency statement in the relevant notice or notification,

then the Court may, on application to it, determine that non-compliance by the person with a requirement or prohibition specified in the notice, or a contravention by him of section 24 of this Act, during the period ending with the determination or withdrawal of the appeal or during such other period as may be determined, does not constitute an offence.

(4) A decision of the Magistrates' Court on an appeal made under subsection (1) shall be final save that an appeal may be brought to the Supreme Court on a point of law against such a decision and references in this Act to the determination of an appeal shall be construed as including references to the determination of an appeal to the Supreme Court and any appeal from the decision of that Court.

(5) An appeal may be made to and determined by the Supreme Court against any compensation order, or decision made with regard to a compensation order, by the Commissioner under section 25 and the Supreme Court shall have the power to make, quash, overturn or vary a compensation order. References in this Act to the determination of an appeal in relation to a compensation order shall be construed as including references to the determination of any appeal to the Court of Appeal and any appeal from the decision of that Court.

## **Offences.**

33. Where an offence under this Act has been committed by a legal person and is proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of a person, being a director, manager, secretary or other officer of that body corporate, or a person who was purporting to act in any such capacity, that person, as well as the body corporate, shall be guilty of that offence and be liable to be proceeded against and punished accordingly.

## **Proceedings.**

34.(1) A person responsible for any act or omission contrary to the provisions of this Act shall be guilty of an offence.

(2) Proceedings for an offence under this Act may be instituted within one year from the date of the offence.

(3) Proceedings for an offence under this Act may be brought and prosecuted by the Commissioner in the Magistrates' Court.

**Penalties.**

35.(1) A person guilty of an offence contrary to section 34(1) shall be liable—

- (a) on summary conviction, to a fine not exceeding level 4 on the standard scale; or
- (b) on conviction on indictment to a fine not exceeding level 5 on the standard scale.

(2) Where a person is convicted of an offence under this Act, the court may order any data material which appears to the court to be connected with the commission of the offence to be forfeited or destroyed and any relevant data to be erased.

(3) The court shall not make an order under subsection (2) of this section in relation to data material or data where it considers that some person other than the person convicted of the offence concerned may be the owner of, or otherwise interested in, the data unless such steps as are reasonably practicable have been taken for notifying that person and giving him an opportunity to show cause why the order should not be made.

**Part VIII**

*Personal Data Protection Officials and Exemption from Registration*

**Personal Data Protection Officials and Exemption from Registration.**

36.(1) The Minister may provide by regulations that data controllers or specific categories of data controller may, or shall, appoint a personal data protection official.

(2) A personal data protection official may be responsible for—

- (a) liaising with the Commissioner;
- (b) ensuring in an independent manner the internal application of this Act;
- (c) keeping a register of the data processing operations carried out including at least the information referred to in section 23(3)(a)–(e).

(3) The Minister may provide by regulations that data controllers or specific categories of data controller are exempt from the requirement to apply for registration under section 24 if–

- (a) they are obliged by regulations to appoint a personal data protection official in pursuance of regulations made under subsection (1); and
- (b) the personal data protection official is responsible under those regulations for–
  - (i) ensuring in an independent manner the internal application of this Act; and
  - (ii) keeping a register of the data processing operations carried out including at least the information referred to in section 23(3)(a)–(e).

## **Part IX**

### *Regulations, Rules of Court*

#### **Regulations and Rules of Court.**

37. (1) The Minister may make regulations for carrying out the purposes of this Act or for complying with the Directive, the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January 1981 or Articles 126 - 130 of the Convention of 19 June 1990 Applying the Schengen Agreement of 14 June 1985.

(2) The Minister shall consult the Commissioner before making regulations under this Act where they relate to the protection of individuals' rights and freedoms with regard to the processing of personal data.

(3) Regulations made for the purposes of–

- (a) section 23(2)(a) shall specify types of processing which appear particularly likely to the Minister to–
  - (i) cause substantial damage or substantial distress to data subjects; or
  - (ii) significantly to prejudice the rights and freedoms of data subjects' under the European Convention on Human Rights or the Gibraltar Constitution Order 1969.
- (b) section 24(5) shall specify–

- (i) the purposes of the processing;
- (ii) the data or categories of data undergoing the processing;
- (iii) the category or categories of data subject affected;
- (iv) the recipient or categories of recipient to whom the data are to be, or may be, disclosed; and
- (v) the length of time for which the data may be stored.

(4) Regulations made under this Act may contain such commencement and transitional provisions in relation to both this Act and those regulations as the Minister considers expedient for the purposes of this Act.

(5) The Chief Justice may make such Rules of Court as are necessary and expedient for the purposes of appeals to the court under this Act.

## SCHEDULE 1

Section 28(3)

Powers of the Gibraltar Data Protection 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.