11580/03/EN
WP 82

Opinion 6/2003 on the level of protection of personal data in the Isle of Man

Adopted on 21 November 2003

OPINION 6/2003 OF THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

On the level of protection of personal data in the Isle of Man

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA,

Having regard to 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[1], and in particular Articles 29 and 30 paragraph 1 (b) thereof,

Having regard to the Rules of Procedure of the Working Party[2], and in particular Article 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION: ACT ON DATA PROTECTION IN THE ISLE OF MAN

1.1. The situation of the Isle of Man

The Isle of Man is situated in the heart of the British Isles. The country is an internally self-governing dependent territory of the British Crown. It is not part of the United Kingdom but is a member of the British Commonwealth.

The Isle of Man has a special relationship with the European Union set out in Protocol 3 to the United Kingdom's Treaty of Accession. Under Protocol 3, the Isle of Man is part of the customs territory of the Union. It follows that there is free movement of industrial and agricultural goods in trade between the Island and the Union.

1.2. Existing data protection legal framework:

Data protection in the Isle of Man is now governed by the Data Protection Act 2002 (``the Act"). The Act repeals and replaces the Data Protection Act 1986 ("the 1986 Act") from April 1, 2003. Although the Isle of Man is not a member of the EU and therefore is not required to meet the requirement of the European Data Protection Directive 95/46/EC, it has taken measures intended to do so, in order to apply for an adequacy finding by the European Commission. The Act contains provisions substantially similar to the Data Protection Act 1998 of England and Wales. Its full title is "An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information".

[1] OJ L 281, 23.11.1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

[2] Adopted by the Working Party at its third meeting held on 11.9.1996

Most of the Act came into force on April 1, 2003, although transitional provisions set out in Schedules 10 and 11 may delay the coming into effect of provisions in relation to certain processing.

Other laws which impact or are likely to impact upon data protection include:

- Human Rights Act 2001, which was passed by Parliament on 16th January 2001 and not yet fully in force.

- Access to Health Records and Reports Act 1993.

The United Kingdom signed the Council of Europe Convention on May 14, 1981 and ratified it on August 26, 1987, with effect from December 1, 1987. It was then extended to the Isle of Man at the island's request on May 1, 1993.

2. ASSESSMENT OF THE DATA PROTECTION ACT OF THE ISLE OF MAN AS PROVIDING ADEQUATE PROTECTION OF PERSONAL DATA

The Working Party points out that its assessment on the adequacy of the Act on data protection in the Isle of Man focuses on the Data Protection Act, 2002.

The provisions of this Act have been compared with the main provisions of the Directive, taking into account the Working Party's opinion on "Transfers of personal data to third countries; Applying Articles 25 and 26 of the EU data protection Directive[3]". This opinion lists a number of principles which constitute *a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate*. In order to facilitate the reading of the text, the wording of long articles of the Act has been included as annex. The result of this analysis is as follows:

2.1. Content Principles

Basic principles

the purpose limitation principle - data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.

The Working Party is satisfied that the Act of the Isle of Man complies with this principle. Schedule 1, part 1 and in particular the second principle sets out that "*Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes*". Further, the fifth principle of the same schedule adds: *"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes*". This principle if further developed in the second part of the same schedule and in particular in Sections 13 and 14 (annex, number 1).

the data quality and proportionality principle - data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not

[3] WP 12 – Adopted by the Working Party on 24 July 1998, available at: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

excessive in relation to the purposes for which they are transferred or further processed.

The Working Party understands that this principle is complied with by the Act of The Isle of Man. Schedule 1, part 1, and in particular the third principle, provides that *"Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed"*. Further, the fourth principle of the same schedule stipulates that *"Personal data shall be accurate and, where necessary, kept up to date."*. This principle is further developed in the second part of the same schedule and in particular in Section 15 (annex, number 2).

> **the transparency principle -** individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the directive**.**

The Working Party notes that this principle is complied with by the Act of the Isle of Man. Schedule 1, part 1, and in particular the first principle, provides that "Personal data shall be processed fairly and lawfully". Fair processing is further developed in the second part of the same schedule and in particular paragraph 10 that stipulates that personal data are not to treated as processed fairly unless the data subject is provided with, or has made readily available to him the information specified in sub paragraph 10(3) namely:

(a) the identity of the data controller,
(b) if he has nominated a representative for the purposes of this Act, the identity of that representative,
(c) the purpose or purposes for which the data are intended to be processed, and
(d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

Further, the right of access to personal data stipulates in Section 5.1(a) that: *"Subject to the following provisions of this section and to sections 6 and 7, an individual is entitled to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller"* (for Sections 6 and 7, see annex, number 3). Section 5.1, letter (b) adds : "*if that is the case, an individual is entitled to be given by the data controller a description of (i) the personal data of which that individual is the data subject,(ii) the purposes for which they are being or are to be processed, and(iii) the recipients or classes of recipients to whom they are or maybe disclosed"*. With regard to notification by data controllers, this principle is further developed in Sections 13 and following (annex, number 4).

> **the security principle** - technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

The Working Party understands that the Act of the Isle of Man complies with this principle. Schedule 1, part 1, seventh principle, provides as follows:
"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or

damage to, personal data."
This principle is further explained in the second part of the same schedule and in particular in Sections 17, 18 and 19 and 20 (annex, number 5).

> **the rights of access, rectification and opposition -** the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.

As for the rights of the individuals, the Working Party notes that this principle is complied with by the Act of the Isle of Man. Schedule 1, part 1, and in particular the sixth principle, provides that "*personal data shall be processed in accordance with the rights of data subjects under this Act*". This principle is further developed in the second part of the same schedule and in particular in Section 16 (annex, number 6).

As for the right of access, the Working Party is satisfied that this principle is complied with by this Act, in particular by its Section 5.1, letter (c) (annex, number 7).

As for the right of rectification, the Working Party understands that this principle is complied with by the Act of the Isle of Man. In particular, Section 12 of the Act deals with the rights of rectification, blocking, erasure and destruction (annex, number 8).

The right of opposition is dealt with in Section 8. This section establishes the right to prevent processing likely to cause damage or distress (annex, number 9).

The exceptions to the right of access are contained in Part 4 of the Act (cases where the disclosure is likely to prejudice national security, crime prevention, detection and prosecution, assessment or collection of tax or duty, health education and social work, regulatory activity) (annex, number 10) as well as in the secondary legislation[4], allowing for well-defined restrictions in a number of specific cases.

The Working Party considers that these exceptions are in line with the provisions of Article 13 of the Directive.

> **restrictions on onward transfers -** further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive.

The Working Party understands that this principle is complied with by the Act of the Isle of Man. In particular, schedule 1, part 1, eighth principle reads as follows: "*Personal data shall not be transferred to a country or territory outside the Island unless that 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"*. This principle is further explained in schedule 1, part 2, sections 21, 22 and 23 (annex, number 11).

[4] In particular the Subject Access Exemptions Order 2003 (Adoption etc), the Subject Access Modification (Education) Order 2003, the Subject Access Modification (Health) Order 2003, the Subject Access Modification (Social Work) Order 2003, the Corporate Finance Exemption Order 2003, and the Crown Appointments Order 2003.

The exceptions to this principle are contained in Schedule 4 (annex, number 12). The Working Party notes with satisfaction that these exceptions are perfectly in line with article 26 of the Directive.

Additional principles to be applied to specific types of processing are:

> **sensitive data** - where 'sensitive' categories of data are involved (those listed in Article 8 of the directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

The Working Party understands that this principle is complied with by the Act of the Isle of Man. In particular, Section 1 of the Act defines "sensitive data" (annex, number 13); Schedule 1, part 1, first principle, letter b adds that sensitive data shall not be processed unless one of the conditions of Schedule 3 are met. This principle is further developed in the second part of the same Schedule, and in particular in Section 9 and following (annex, number 14). Schedule 3 lays down the conditions for processing sensitive data (annex, number 15).

> **direct marketing** - where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.

The Working Party notes that this principle is complied with by Section 9, that regulates the right to prevent processing for purposes of direct marketing (annex, number 16).

> **automated individual decision** - where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

The Working Party understands that this principle is complied with by the Act in The Isle of Man. In particular, by its Section 5.1, letter (d) (annex, number 17) and its Section 10 that elaborates on the rights in relation to automated decision taking (annex, number 18).

2.2. Procedural/ Enforcement mechanisms

The Working Party's opinion on "Transfers of personal data to third countries; Applying Articles 25 and 26 of the EU data protection Directive"[5] indicates that the assessment of the adequacy of a third country's legal system should identify the underlying objectives of a data protection procedural system, and on this basis judge the variety of different judicial and non-judicial procedural mechanisms used in third countries.

With that regard, the objectives of a data protection system are essentially threefold:

– to deliver a good level of compliance with the rules;
– to provide support and help to individual data subjects in the exercise of their rights;
– to provide appropriate redress to the injured party where rules are not complied with.

> **to deliver a good level of compliance with the rules -** A good system is generally characterised by a high degree of awareness among data controllers of

[5] WP 12 – Adopted by the Working Party on 24 July 1998, available at: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

The Working Party understands that the Act of the Isle of Man has put in place a number of elements to serve this objective. In particular:

(a) Data Protection Supervisor

The office, previously known as the Isle of Man Data Protection Registrar, was established by the 1986 Act and it continues to exist for the purposes of the Act but is renamed the office of the Data Protection Supervisor and the "Registrar" is referred to as the "Supervisor" in the Act.

The functions of the Supervisor are set out in Sections 47 to 49 of the Act and include promoting compliance with the Act by issuing guidelines and codes of practice, in order to assist interpretation of the Act.

In order to secure compliance with the Act, he Supervisor has certain powers of investigation and enforcement set out in Sections 36 to 42, including powers of entry and inspection set out in Schedule 8.

Further duties include the maintenance of the register of persons who have given notification under section 16.

(b) The existence of adequate enforcement means and sanctions

The Act provides a number of sanctions and enforcement means.

Complaints by data subjects to the Supervisor concerning notification offences under section 18 or unauthorised disclosure offences under section 50 would be dealt with as potential criminal prosecutions, while complaints involving non-compliance with principles are dealt with as a request for assessment under section 38.

The Supervisor may serve an enforcement notice where he has assessed that a data controller is not complying (Section 36) with the principles or an information notice where he needs more information to complete an assessment (Section 39, section 40 dealing with special information notices). Failure to comply with an enforcement or information notice is an offence under section 43.

The prosecution and penalties are set out in section 55 of the Act. In general the fine upon summary conviction would not exceed £5000 but serious offences can be heard in the High Court where the fine is unlimited. Where an offence is committed by a body corporate, section 56 stipulates that the directors, etc of the body corporate "*as well as the body corporate shall be guilty of that offence and be liable to be proceeded against and punished accordingly*." Further, section 58 stipulates that Government departments "*shall be subject to the same obligations and liabilities under this Act as a private person*".

In the view of these considerations, the Working Party understands that the Act of the Isle of Man contains the elements necessary to deliver a good level of compliance with the rules.

> **to provide support and help to individual data subjects in the exercise of their rights -** The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

The Working Party notes that the Act of the Isle of Man has put in place a number of elements to serve this objective. In particular, citizens can ask the Supervisor to make an assessment. This is regulated in Section 38 of the Act (annex, number 19).
The procedure for assessment is described in detail on the Supervisor's website and it involves no cost for the individuals.

In the view of these considerations, the Working Party understands that the Act of the Isle of Man contains the elements necessary to provide support and help to individual data subjects in the exercise of their rights.

> **to provide appropriate redress to the injured party where rules are not complied with** - This is a key element, which must involve a system of independent adjudication, or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

The Act of the Isle of Man provides for a compensation scheme in Section 11 (annex, number 20). A person has the right to seek compensation for failure to comply with certain requirements.

Of particular note is section 11(2)(c) which permits a person to seek compensation for distress alone, where the contravention consists of a failure to comply with a request under section 5 (right of access to personal data). In addition, section 5(9)(b) provides that the Court may impose a penalty not exceeding £5000 if a data controller has unjustifiably failed to comply with a request under section 5.

In the view of these considerations, the Working Party understands that the Act of the Isle of Man contains the elements necessary to provide appropriate redress to the injured party where rules are not complied with.

3. RESULTS OF THE ASSESSMENT

In conclusion, on the basis of the above mentioned findings, the Working Party is satisfied that the Isle of Man ensures an adequate level of protection within the meaning of Article 25(6) of 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 an on the free movement of such data.

Done at Brussels, 21 November 2003

For the Working Party
The Chairman
Stefano RODOTA

Annex: Relevant provisions of the Isle of Man Data Protection Law

(1)*"13. The purpose or purposes for which personal data are obtained may in particular be specified —*

(a) in a notice given for the purposes of paragraph 10 by the data controller to the data subject, or

(b) in a notification given to the Supervisor under Part 3 of this Act.

14. In determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed."

(2) *"15. The fourth principle is not to be regarded as being contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where —*

(a) having regard to the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data, and

(b) if the data subject has notified the data controller of the data subject's view that the data are inaccurate, the data indicate that fact."

(3) *"6. Provisions supplementary to section 5*

(1) The Council of Ministers may by regulations provide that, in such cases as may be prescribed, a request for information under any provision of subsection (1) of section 5 is to be treated as extending also to information under other provisions of that subsection.

(2) The obligation imposed by section 5(1)(c)(i) must be complied with by supplying the data subject with a copy of the information in permanent form 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 5(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

(3) Where a data controller has previously complied with a request made under section 5 by an individual, the data 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.

(4) In determining for the purposes of subsection (3) whether requests under section 5 are made at reasonable intervals, 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) Section 5(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in any decision-taking if, and to the extent that, the information constitutes a trade secret.

(6) The information to be supplied pursuant to a request under section 5 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.

(7) For the purposes of section 5(4) and (5) another individual can be identified from the information being disclosed if he can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.

7. Application of section 5: credit reference agencies
(1) Where the data controller is a credit reference agency, section 5 has effect subject to the provisions of this section.
(2) An individual making a request under section 5 may limit his request to personal data relevant to his financial standing, and shall be taken to have so limited his request unless the request shows a contrary intention.
(3) Where the data controller receives a request under section 5 in a case where personal data of which the individual making the request is the data subject are being processed by or on behalf of the data controller, the obligation to supply information under that section includes an obligation to give the individual making the request a statement, in such form as may be prescribed by the Council of Ministers by regulations, of such of the individual's rights under this Act as are specified in the form."

(4) "*13. Preliminary*
(1) In this Part "the registrable particulars", in relation to a data controller, means
(a) his name and address,
(b) if he has nominated a representative for the purposes of this Act, the name and address of the representative,
(c) 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,
(d) a description of the purpose or purposes for which the data are being or are to be processed,
(e) a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data, and
(f) the names, or a description of, any countries or territories outside the Island to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data.
(2) In this Part — "fees regulations" means regulations made by the Treasury under section 15(5) or 16(4) or (7); "notification regulations" means regulations made by the Council of Ministers under the other provisions of this Part; "prescribed", except where used in relation to fees regulations, means prescribed by notification regulations.
(3) For the purposes of this Part, so far as it relates to the addresses of data controllers
(a) the address of a registered company is that of its registered office, and
(b) the address of a person (other than a registered company) carrying on a business is that of his principal place of business in the Island.
14. Prohibition on processing without registration
(1) Subject to the following provisions of this section, personal data must not be processed unless an entry in respect of the data controller is included in the register maintained by the Supervisor under section 16 (or is treated by notification regulations made by virtue of section 16(3) as being so included).
(2) Except where the processing is assessable processing for the purposes of section 19, subsection (1) does not apply in relation to personal data consisting of information which falls within neither paragraph (a) nor paragraph (b) of the definition of "data" in section 1(1).
(3) If it appears to the Council of Ministers that processing of a particular description is unlikely to prejudice the rights and freedoms of data subjects, notification regulations may provide that, in such cases as may be prescribed, subsection (1) is not to apply in relation to processing of that description.
(4) Subsection (1) does not apply in relation to any processing whose sole purpose is the maintenance of a public register.
15. Notification by data controllers

(1) Any data controller who wishes to be included in the register maintained under section 16 shall give a notification to the Supervisor under this section.
(2) A notification under this section must specify in accordance with notification regulations —
(a) the registrable particulars, and (b) a general description of measures to be taken for the purpose of complying with the seventh data protection principle (measures against misuse and loss of data).
(3) Notification regulations made by virtue of subsection (2) may provide for the determination by the Supervisor, in accordance with any requirements of the regulations, of the form in which the registrable particulars and the description mentioned in subsection (2)(b) are to be specified, including in particular the detail required for the purposes of section 13(1)(c), (d), (e) and (f) and subsection (2)(b).
(4) Notification regulations may make provision as to the giving of notification —
(a) by partnerships, or
(b) in other cases where 2 or more persons are the data controllers in respect of any personal data.
(5) The notification must be accompanied by such fee as may be prescribed by fees regulations.
(6) Notification regulations may provide for any fee paid under subsection (5) or section 16(4) to be refunded in prescribed circumstances.
16. Register of notifications
(1) The Supervisor shall —
(a) maintain a register of persons who have given notification under section 15, and (b) make an entry in the register in pursuance of each notification received by him under that section from a person in respect of whom no entry as data controller was for the time being included in the register.
(2) Each entry in the register shall consist of —
(a) the registrable particulars notified under section 15 or, as the case requires, those particulars as amended in pursuance of section 17(4), and
(b) such other information as the Supervisor may be authorised or required by notification regulations to include in the register.
(3) Notification regulations may make provision as to the time as from which any entry in respect of a data controller is to be treated for the purposes of section 14 as having been made in the register.
(4) No entry shall be retained in the register for more than the relevant time except on payment of such fee as may be prescribed by fees regulations.
(5) In subsection (4) "the relevant time" means 12 months or such other period as may be prescribed by notification regulations.
(6) The Supervisor —
(a) shall provide facilities for making the information contained in the entries in the register available for inspection (in visible and legible form) by members of the public at all reasonable hours and free of charge, and
(b) may provide such other facilities for making the information contained in those entries available to the public free of charge as he considers appropriate.
(7) The Supervisor shall, on payment of such fee, if any, as may be prescribed by fees regulations, supply any member of the public with a duly Data Protection Act 2002 certified copy in writing of the particulars contained in any entry made in the register.
17. Duty to notify changes
(1) For the purpose specified in subsection (2), notification regulations shall include provision imposing on every person in respect of whom an entry as a data controller is for the time being included in the register maintained under section 16 a duty to notify to

the Supervisor, in such circumstances and at such time or times and in such form as may be prescribed, such matters relating to the registrable particulars and measures taken as mentioned in section 15(2)(b) as may be prescribed.
(2) The purpose referred to in subsection (1) is that of ensuring, so far as practicable, that at any time —
(a) the entries in the register maintained under section 16 contain current names and addresses and describe the current practice or intentions of the data controller with respect to the processing of personal data, and
(b) the Supervisor is provided with a general description of measures currently being taken as mentioned in section 15(2)(b).
(3) Section 15(3) has effect in relation to notification regulations made by virtue of subsection (1) as it has effect in relation to notification regulations made by virtue of section 15(2).
(4) On receiving any notification under notification regulations made by virtue of subsection (1), the Supervisor shall make such amendments of the relevant entry in the register maintained under section 16 as are necessary to take account of the notification.
18. Offences
(1) If section 14(1) is contravened, the data controller is guilty of an offence.
(2) Any person who fails to comply with the duty imposed by notification regulations made by virtue of section 17(1) is guilty of an offence.
(3) It shall be a defence for a person charged with an offence under subsection (2) to show that he exercised all due diligence to comply with the duty."

(5) "*The seventh principle (measures against misuse and loss of data)*
17. Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to —
(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
(b) the nature of the data to be protected.
18. The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.
19. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle —
(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
(b) take reasonable steps to ensure compliance with those measures."
20. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless —
(a) the processing is carried out under a contract —
(i) which is made or evidenced in writing, and
(ii) under which the data processor is to act only on instructions from the data controller, and
(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle."

(6) "*The sixth principle (rights of data subjects)*
16. A person is to be regarded as contravening the sixth principle if, but only if —
(a) he contravenes section 5 by failing to supply information in accordance with that section,
(b) he contravenes section 8 by failing to comply with a notice given under section 8(1) to the extent that the notice is justified or by failing to give a notice under section 8(3),

(c) he contravenes section 9 by failing to comply with a notice given under section 9(1), or
(d) he contravenes section 10 by failing to comply with a notice given under section 10(1) or (2)(b) or by failing to give a notification under section 10(2)(a) or a notice under section 10(3)."

(7) *"5. (1) Subject to the following provisions of this section and to sections 6 and 7, an individual is entitled —*
(c) to have communicated to him in an intelligible form —
(i) the information constituting any personal data of which that individual is the data subject, and
(ii) any information available to the data controller as to the source of those data"

(8) *"12. Rectification, blocking, erasure and destruction*
(1) If the High Court is satisfied on the application of a data subject that personal data of which the applicant is the subject are inaccurate, the court may order the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which he is the data controller and which contain an expression of opinion which appears to the court to be based on the inaccurate data.
(2) Subsection (1) applies whether or not the data accurately record information received or obtained by the data controller from the data subject or a third party but where the data accurately record such information, then —
(a) if the requirements mentioned in paragraph 15 of Schedule 1 have been complied with, the High Court may, instead of making an order under subsection (1), make an order requiring the data to be supplemented by such statement of the true facts relating to the matters dealt with by the data as the court may approve, and
(b) if all or any of those requirements have not been complied with, the High Court may, instead of making an order under that subsection, make such order as it thinks fit for securing compliance with those requirements with or without a further order requiring the data to be supplemented by such a statement as is mentioned in paragraph (a).
(3) Where the High Court —
(a) makes an order under subsection (1), or
(b) is satisfied on the application of a data subject that personal data of which he was the data subject and which have been rectified, blocked, erased or destroyed were inaccurate, it may, where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.
(4) If the High Court is satisfied on the application of a data subject —
(a) that he has suffered damage by reason of any contravention by a data controller of any of the requirements of this Act in respect of any personal data, in circumstances entitling him to compensation under section 11, and
(b) that there is a substantial risk of further contravention in respect of those data in such circumstances, the court may order the rectification, blocking, erasure or destruction of any of those data.
(5) Where the court makes an order under subsection (4) it may, where it considers it reasonably practicable, order the data controller to notify Data Protection Act 2002 third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.
(6) In determining whether it is reasonably practicable to require such notification as is mentioned in subsection (3) or (5) the court shall have regard, in particular, to the number of persons who would have to be notified."

(9) *“8. Right to prevent processing likely to cause damage or distress*
(1) Subject to subsection (2), an individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, 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, on the ground that, for specified reasons —
(a) the processing of those data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another, and
(b) that damage or distress is or would be unwarranted.
(2) Subsection (1) does not apply —
(a) in a case where any of the conditions in paragraphs 1 to 4 of Schedule 2 is met, or
(b) in such other cases as may be prescribed by the Council of Ministers by order.
(3) The data controller must within 21 days of receiving a notice under subsection (1) ("the data subject notice") give the individual who gave it a written notice —
(a) stating that he has complied or intends to comply with the data subject notice, or
(b) stating his reasons for regarding the data subject notice as to any extent unjustified and the extent (if any) to which he has complied or intends to comply with it.
(4) If the High Court is satisfied, on the application of any person who has given a notice under subsection (1) which appears to the court to be justified (or to be justified to any extent), that the data controller in question has failed to comply with the notice, the court may order him to take such steps for complying with the notice (or for complying with it to that extent) as the court thinks fit.
(5) The failure by a data subject to exercise the right conferred by subsection (1) or section 9(1) does not affect any other right conferred on him by this Part."

(10) *"PART 4 - EXEMPTIONS*
23. Preliminary
(1) References in any of the data protection principles or any provision of Parts 2 and 3 to personal data or to the processing of personal data do not include references to data or processing which by virtue of this Part are exempt from that principle or other provision.
(2) In this Part "the subject information provisions" means —
(a) the first data protection principle (fair and lawful processing) to the extent to which it requires compliance with paragraph 10 of Schedule 1, and
(b) section 5.
(3) In this Part "the non-disclosure provisions" means the provisions specified in subsection (4) to the extent to which they are inconsistent with the disclosure in question.
(4) The provisions referred to in subsection (3) are —
(a) the first data protection principle (fair and lawful processing), except to the extent to which it requires compliance with the conditions in Schedules 2 and 3,
(b) the second data protection principle (purpose for which data are obtained and processed),
(c) the third data protection principle (adequacy and relevance of data),
(d) the fourth data protection principle (accuracy of data),
(e) the fifth data protection principle (time for keeping data), and
(f) sections 8 and 12(1) to (3).

(5) Except as provided by this Part, the subject information provisions shall have effect notwithstanding any statutory provision or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information.

24. National security

(1) Personal data are exempt from any of the provisions of —

(a) the data protection principles,

(b) Parts 2, 3 and 5, and

(c) section 50, if the exemption from that provision is required for the purpose of safeguarding national security.

(2) Subject to subsection (4), a certificate signed by the Chief Minister certifying that exemption from all or any of the provisions mentioned in subsection (1) is or at any time was required for the purpose there mentioned in respect of any personal data shall be conclusive evidence of that fact.

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

(4) Any person directly affected by the issuing of a certificate under subsection (2) may appeal to the Tribunal against the certificate.

(5) If on an appeal under subsection (4), the Tribunal finds that, applying the principles applied by the High Court on a petition of doleance, the Chief Minister did not have reasonable grounds for issuing the certificate, the Tribunal may allow the appeal and quash the certificate.

(6) Where in any proceedings under or by virtue of this Act it is claimed by a data controller that a certificate under subsection (2) which identifies the personal data to which it applies by means of a general description applies to any personal data, then, subject to any determination under subsection (7), the certificate shall be conclusively presumed so to apply.

(7) Any other party to proceedings referred to in subsection (6) may appeal to the Tribunal on the ground that the certificate does not apply to the personal data in question, and the Tribunal may determine that the certificate does not so apply.

(8) A document purporting to be a certificate under subsection (2) shall be received in evidence and deemed to be such a certificate unless the contrary is proved.

(9) No power conferred by any provision of Part 5 may be exercised in relation to personal data which by virtue of this section are exempt from that provision.

(10) Schedule 6 shall have effect in relation to appeals under subsection (4) or (7) and the proceedings of the Tribunal in respect of any such appeal.

25. Crime and taxation

(1) 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 any tax or duty or of any imposition of a similar nature, are exempt from the first data protection principle (fair and lawful processing) (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 5 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

(2) Personal data which —

(a) are processed for the purpose of discharging statutory functions, and

(b) consist of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in subsection (1),

are exempt from the subject information provisions to the same extent as personal data processed for any of the purposes mentioned in that subsection.

(3) Personal data are exempt from the non-disclosure provisions in any case in which

(a) the disclosure is for any of the purposes mentioned in subsection (1), and
(b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.
(4) Personal data in respect of which the data controller is a relevant authority and which —
(a) consist of a classification applied to the data subject as part of a system of risk assessment which is operated by that authority for either of the following purposes —
(i) the assessment or collection of any tax or duty or any imposition of a similar nature, or
(ii) the prevention or detection of crime, or apprehension or prosecution of offenders, where the offence concerned involves any unlawful claim for any payment out of, or any unlawful application of, public funds, and
(b) are processed for either of those purposes, are exempt from section 5 to the extent to which the exemption is required in the interests of the operation of the system.
(5) In subsection (4) "relevant authority" means a Department, Statutory Board, local authority or joint board.
26. Health, education and social work
(1) The Council of Ministers may by order exempt from the subject information provisions, or modify those provisions in relation to, personal data consisting of information as to the physical or mental health or condition of the data subject.
(2) The Council of Ministers may by order exempt from the subject information provisions, or modify those provisions in relation to personal data —
(a) in respect of which the data controller is the proprietor of, or a teacher at, a school or college, and which consist of information relating to persons who are or have been pupils at the school or college; or
(b) in respect of which the data controller is the Department of Education, and which consist of information relating to persons who are or have been pupils at a school or college maintained by that Department.
(3) The Council of Ministers may by order exempt from the subject information provisions, or modify those provisions in relation to, personal data of such other descriptions as may be specified in the order, being information —
(a) processed by the Department of Health and Social Security or by voluntary organisations or other bodies designated by or under the order, and
(b) appearing to it to be processed in the course of, or for the purposes of, carrying out social work in relation to the data subject or other individuals; but the Council of Ministers shall not under this subsection confer any exemption or make any modification except so far as it considers that the application to the data of those provisions (or of those provisions without modification) would be likely to prejudice the carrying out of social work.
27. Regulatory activity
(1) Personal data processed for the purposes of discharging functions to which this subsection applies are exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of those functions.
(2) Subsection (1) applies to any relevant function which is designed for —
(a) protecting 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 or in the management of bodies corporate,
(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, persons authorised to carry on any profession or other activity,
(b) protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration, protecting the property of charities from loss or misapplication, or the recovery of the property of charities,
(c) securing the health, safety and welfare of persons at work, or protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work.
(3) In subsection (2) "relevant function" means —
(a) any function conferred on any person by or under any statutory provision, or
(b) any other function which is of a public nature and is exercised in the public interest.
(4) Personal data processed for the purpose of discharging any function of the Isle of Man Office of Fair Trading under the Fair Trading Act 1996 are exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.
28. Journalism, literature and art
(1) Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if —
(a) the processing is undertaken with a view to the publication by any person 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, publication would be in the public interest, and
(c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.
(2) Subsection (1) relates to the provisions of —
(a) the data protection principles except the seventh data protection principle (measures against misuse and loss of data),
(b) section 5,
(c) section 8,
(d) section 10, and
(e) section 12(1) to (3).
(3) In considering for the purposes of subsection (1)(b) whether the belief of a data controller that publication would be in the public interest was or is a reasonable one, regard may be had to his compliance with any code of practice which —
(a) is relevant to the publication in question, and
(b) is designated by the Council of Ministers by order for the purposes of this subsection.
(4) Where at any time ("the relevant time") in any proceedings against a data controller under section 5(9), 8(4), 10(8) or 12 or by virtue of section 11 the data controller claims, or it appears to the High Court, that any personal data to which the proceedings relate are being processed —
(a) only for the special purposes, and
(b) with a view to the publication by any person of any journalistic, literary or artistic material which, at the time 24 hours immediately before the relevant time, had not previously been published by the data controller, the court shall stay the proceedings until either of the conditions in subsection (5) is met.
(5) Those conditions are —
(a) that a determination of the Supervisor under section 41 with respect to the data in question takes effect, or
(b) in a case where the proceedings were stayed on the making of a claim, that the claim is withdrawn.

(6) For the purposes of this Act "publish", in relation to journalistic, literary or artistic material, means make available to the public or any section of the public.

29. Research, history and statistics

(1) In this section —

"research purposes" includes statistical or historical purposes; "the relevant conditions", in relation to any processing of personal data, means the conditions —

(a) that the data are not processed to support measures or decisions with respect to particular individuals, and

(b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

(2) For the purposes of the second data protection principle (purpose for which data are obtained and processed), the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

(3) Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle (time for keeping data), be kept indefinitely.

(4) Personal data which are processed only for research purposes are exempt from section 5 if —

(a) they are processed in compliance with the relevant conditions, and

(b) the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.

(5) For the purposes of subsections (2) to (4) personal data are not to be treated as processed otherwise than for research purposes merely because the data are disclosed —

(a) to any person, for research purposes only,

(b) to the data subject or a person acting on his behalf,

(c) at the request, or with the consent, of the data subject or a person acting on his behalf, or

(d) in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (a), (b) or (c).

30. Information available to the public by or under statutory provision

Personal data are exempt from —

(a) the subject information provisions,

(b) the fourth data protection principle (accuracy of data) and section 12(1) to (3), and

(c) the non-disclosure provisions, if the data consist of information which the data controller is obliged by or under any statutory provision to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.

31. Disclosures required by law or made in connection with legal proceedings etc.

(1) Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any statutory provision, by any rule of law or by the order of a court.

(2) Personal data are exempt from the non-disclosure provisions where the disclosure is necessary —

(a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or

(b) for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

32. Tynwald privilege

Personal data are exempt from —

(a) the first data protection principle, except to the extent to which it requires compliance with the conditions in Schedules 2 and 3,
(b) the second, third, fourth and fifth data protection principles,
(c) section 5, and
(d) sections 8 and 12(1) to (3),
if the exemption is required for the purpose of avoiding an infringement of the privileges of Tynwald, the Council or the Keys.
33. Domestic purposes
Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes) are exempt from the data protection principles and the provisions of Parts 2 and 3.
34. Miscellaneous exemptions
Schedule 7 (which confers further miscellaneous exemptions) has effect.
35. Powers to make further exemptions by order
(1) The Council of Ministers may by order exempt from the subject information provisions personal data consisting of information the disclosure of which is prohibited or restricted by or under any statutory provision if and to the extent that it considers it necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other individual that the prohibition or restriction ought to prevail over those provisions.
(2) The Council of Ministers may by order exempt from the nondisclosure provisions any disclosures of personal data made in circumstances specified in the order, if it considers the exemption is necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other individual."

(11) *"The eighth principle (transfer of data abroad)*
21. An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to —
(a) the nature of the personal data,
(b) the country or territory of origin of the information contained in the data,
(c) the country or territory of final destination of that information,
(d) the purposes for which and period during which the data are intended to be processed,
(e) the law in force in the country or territory in question,
(f) the international obligations of that country or territory,
(g) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases), and
(h) any security measures taken in respect of the data in that country or territory.
22. The eighth principle does not apply to a transfer falling within any paragraph of Schedule 4, except in such circumstances and to such extent as the Council of Ministers may by order provide.
23. (1) Where in any proceedings under this Act any question arises as to whether the requirement of the eighth principle as to an adequate level of protection is met in relation to the transfer of any personal data to a country or territory within the European Economic Area, it shall be conclusively presumed that that requirement is met in relation to that transfer.
(2) Where —
(a) in any proceedings under this Act any question arises as to whether the requirement of the eighth principle as to an adequate level of protection is met in relation to the transfer of any personal data to a country or territory outside the European Economic Area, and

(b) a Community finding has been made in relation to transfers of the kind in question, that question is to be determined in accordance with that finding.
(3) In sub-paragraph (2) "Community finding" means a finding of the European Commission, under the procedure provided for in Article 31(2) of the Data Protection Directive, that a country or territory outside the European Economic Area does, or does not, ensure an adequate level of protection within the meaning of Article 25(2) of the Directive."

(12) *"SCHEDULE 4 - CASES WHERE THE EIGHTH PRINCIPLE DOES NOT APPLY*
1. The data subject has given his consent to the transfer.
2. The transfer is necessary —
(a) for the performance of a contract between the data subject and the data controller, or
(b) 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.
3. The transfer is necessary —
(a) for the conclusion of a contract between the data controller and a person other than the data subject which —
(i) is entered into at the request of the data subject, or
(ii) is in the interests of the data subject, or
(b) for the performance of such a contract.
4. (1) The transfer is necessary for reasons of substantial public interest.
(2) The Council of Ministers may by order specify —
(a) circumstances in which a transfer is to be taken for the purposes of subparagraph (1) to be necessary for reasons of substantial public interest, and
(b) circumstances in which a transfer which is not required by or under a statutory provision is not to be taken for the purpose of sub-paragraph (1) to be necessary for reasons of substantial public interest.
5. The transfer —
(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.
6. The transfer is necessary in order to protect the vital interests of the data subject.
7. The transfer is of part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer.
8. The transfer is made on terms which are of a kind approved by the Supervisor as ensuring adequate safeguards for the rights and freedoms of data subjects.
9. The transfer has been authorised by the Supervisor as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects."

(13) *"sensitive personal data" means personal data consisting of information as to —*
(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Unions Act 1991),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings;"

(14) *"The first principle (fair and lawful processing)*
9. (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.
(2) Subject to paragraph 10, for the purposes of the first principle data are to be treated as obtained fairly if they consist of information obtained from a person who —
(a) is authorised by or under any statutory provision to supply it, or
(b) is required to supply it by or under any statutory provision or by any convention or other instrument imposing an international obligation on the United Kingdom and extending to the Island.
10. (1) Subject to paragraph 11, for the purposes of the first principle personal data are not to be treated as processed fairly unless —
(a) in the case of data obtained 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, the information specified in sub-paragraph (3), and
(b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).
(2) In sub-paragraph (1)(b) "the relevant time" means —
(a) the time when the data controller first processes the data, or
(b) in a case where at that time disclosure to a third party within a reasonable period is envisaged —
(i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,
(ii) if within that period the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware, or
(iii) in any other case, the end of that period.
(3) The information referred to in sub-paragraph (1) is as follows, namely —
(a) the identity of the data controller,
(b) if he has nominated a representative for the purposes of this Act, the identity of that representative,
(c) the purpose or purposes for which the data are intended to be processed, and
(d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.
11. (1) Paragraph 10(1)(b) does not apply where either of the primary conditions in sub-paragraph (2), together with such of the further conditions in sub-paragraphs (3) to (7) as are relevant, are met.
(2) The primary conditions referred to in sub-paragraph (1) are —
(a) that the provision of that information would involve a disproportionate effort, or
(b) that the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
(3) Where either of the primary conditions in sub-paragraph (2) is met, a further condition is that set out in sub-paragraph (6).

(4) Where the primary condition in sub-paragraph (2)(a) is met, a further condition is that the data controller shall record the reasons for his view that that primary condition is met in respect of the data.
(5) Where the primary condition in sub-paragraph (2)(b) is met by virtue of the fact that the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller —
(a) is not a function conferred on him by or under any statutory provision or an obligation imposed on him by order of a court, but
(b) is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract, a further condition is that set out in sub-paragraph (6).
(6) The condition referred to in sub-paragraphs (3) to (5) is that, in respect of any particular data subject, either —
(a) no notice in writing has been received at any time by the data controller from an individual, requiring that data controller to provide the information set out in paragraph 10(3) before the relevant time (as defined in paragraph 10(2)) or as soon as practicable after that time; or
(b) where such notice in writing has been received but the data controller does not have sufficient information about the individual in order readily to determine whether he is processing personal data about that individual, the data controller shall send to the individual a written notice stating that he cannot provide the information set out in paragraph 10(3) because of his inability to make that determination, and explaining the reasons for that inability.
(7) The requirement in sub-paragraph (6) that notice should be in writing is satisfied where the text of the notice —
(a) is transmitted by electronic means,
(b) is received in legible form, and
(c) is capable of being used for subsequent reference.
(8) The Council of Ministers may by order amend sub-paragraphs (1) to (7).
12. (1) Personal data which contain a general identifier falling within a description prescribed by the Council of Ministers by order are not to be treated as processed fairly and lawfully unless they are processed in compliance with any conditions so prescribed in relation to general identifiers of that description.
(2) In sub-paragraph (1) "a general identifier" means any identifier (such as, for example, a number or code used for identification purposes) which —
(a) relates to an individual, and
(b) forms part of a set of similar identifiers which is of general application."

(15) *"SCHEDULE 3 - CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA*
1. The data subject has given his explicit consent to the processing of the personal data.
2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
(2) The Council of Ministers may by order —
(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
(b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
3. The processing is necessary —

(a) in order to protect the vital interests of the data subject or another person, in a case where —
(i) consent cannot be given by or on behalf of the data subject, or
(ii) the data 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.
4. The processing —
(a) is carried out in the course of its legitimate activities by any body or association which —
(i) is not established or conducted for profit, and
(ii) exists for political, philosophical, religious or trade-union purposes,
(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes,
and
(d) does not involve disclosure of the personal data to a third party without the consent of the 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.
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.
7. (1) The processing is necessary —
(a) for the administration of justice,
(b) for the exercise of any functions of Tynwald, the Council or the Keys;
(c) for the exercise of any functions conferred on any person by or under any statutory provision, or
(d) for the exercise of any functions of the Crown, a Department or a Statutory Board.
(2) The Council of Ministers may by order —
(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
(b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
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 preventive medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
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) The Council of Ministers may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. (1) The processing —

(a) is in the substantial public interest;

(b) is necessary for the purposes of the prevention or detection of any unlawful act; and

(c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.

(2) In this paragraph, "act" includes a failure to act.

11. The processing —

(a) is in the substantial public interest;

(b) is necessary for the discharge of any function which is designed for protecting members of the public against —

(i) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person, or

(ii) mismanagement in the administration of, or failures in services provided by, any body or association; and

(c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the discharge of that function.

12. (1) The disclosure of personal data —

(a) is in the substantial public interest;

(b) is in connection with —

(i) the commission by any person of any unlawful act (whether alleged or established),

(ii) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person (whether alleged or established), or

(iii) mismanagement in the administration of, or failures in services provided by, any body or association (whether alleged or established);

(c) is for the special purposes as defined in section 1(1); and

(d) is made with a view to the publication of those data by any person and the data controller reasonably believes that such publication would be in the public interest.

(2) In this paragraph, "act" includes a failure to act.

13. The processing —

(a) is in the substantial public interest;

(b) is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service;

and

(c) is carried out without the explicit consent of the data subject because the processing —

(i) is necessary in a case where consent cannot be given by the data subject,

(ii) is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject, or

(iii) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, advice, support or other service.

14. (1) The processing —

(a) is necessary for the purpose of —

(i) carrying on insurance business, or

(ii) making determinations in connection with eligibility for, and benefits payable under, an occupational pension scheme as defined in section 1 of the Pension Schemes Act 1993 (an Act of Parliament)21, as it has effect in the Island;

(b) is of sensitive personal data consisting of information as to the physical or mental health or condition of a data subject who is the parent, grandparent, great grandparent or sibling of the insured person or the member of the scheme, as the case may be;

(c) is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of that data subject and the data controller is not aware of the data subject withholding his consent; and

(d) does not support measures or decisions with respect to that data subject.

(2) In this paragraph —

(a) "insurance business" means insurance business, as defined in section 34 of the Insurance Act 198623, falling within such classes as are prescribed by the Council of Ministers by regulations, and

(b) "insured" and "member" includes an individual who is seeking to become an insured person or member of the scheme respectively.

15. The processing —

(a) is of sensitive personal data in relation to any particular data subject that are subject to processing which was already under way immediately before the ommencement of this Schedule;

(b) is necessary for the purpose of —

(i) carrying on insurance business, as defined in section 34 of the Insurance Act 1986, falling within such classes as are prescribed by the Council of Ministers by regulations; or

(ii) establishing or administering an occupational pension scheme as defined in section 1 of the Pension Schemes Act 1993 (an Act of Parliament), as it has effect in the Island; and

(c) either —

(i) is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject and that data subject has not informed the data controller that he does not so consent, or

(ii) must necessarily be carried out even without the explicit consent of the data subject so as not to prejudice those purposes.

16. (1) Subject to the provisions of sub-paragraph (2), the processing —

(a) is of sensitive personal data consisting of information falling within paragraph (c) or (e) of the definition of that expression in section 1(1);

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons —

(i) holding different beliefs as described in paragraph (c) of that definition, or

(ii) of different states of physical or mental health or different physical or mental conditions as described in paragraph (e) of that definition, with a view to enabling such equality to be promoted or maintained;

(c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and

(d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

(2) Where any individual has given notice in writing to any data controller who is processing personal data under the provisions of sub-paragraph (1) requiring that data controller to cease processing personal data in respect of which that individual is the data subject at the end of such period as is reasonable in the circumstances, that data controller must have ceased processing those personal data at the end of that period.

17. The processing —
(a) is in the substantial public interest;
(b) is necessary for research purposes (within the meaning of section 29);
(c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and
(d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.
18. The processing is necessary for the exercise of any functions conferred on a constable by any rule of law.
19. The personal data are processed in circumstances specified in an order made by the Council of Ministers for the purposes of this paragraph."

(16) *"9. Right to prevent processing for purposes of direct marketing*
(1) An individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which he is the data subject.
(2) If the High Court is satisfied, on the application of any person who has given a notice under subsection (1), that the data controller has failed to comply with the notice, the court may order him to take such steps for complying with the notice as the court thinks fit.
(3) In this section "direct marketing" means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals."

(17) *"5. (1) Subject to the following provisions of this section and to sections 6 and 7, an individual is entitled —*
(d) where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking."

(18) "*10. Rights in relation to automated decision-taking*
(1) An individual is entitled at any time, by notice in writing to any data controller, to require the data controller to ensure that no decision taken by or on behalf of the data controller which significantly affects that individual is based solely on the processing by automatic means of personal data in respect of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct.
(2) Where, in a case where no notice under subsection (1) has effect, a decision which significantly affects an individual is based solely on such processing as is mentioned in subsection (1) —
(a) the data controller must as soon as reasonably practicable notify the individual that the decision was taken on that basis,and
(b) the individual is entitled, within 21 days of receiving that notification from the data controller, by notice in writing to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis.
(3) The data controller must, within 21 days of receiving a notice under subsection (2)(b) ("the data subject notice") give the individual a written notice specifying the steps that he intends to take to comply with the data subject notice.

(4) A notice under subsection (1) does not have effect in relation to an exempt decision; and nothing in subsection (2) applies to an exempt decision.
(5) In subsection (4) "exempt decision" means any decision —
(a) in respect of which the conditions in subsections (6) and (7) are met, or
(b) which is made in such other circumstances as may be prescribed by the Council of Ministers by order.
(6) The condition in this subsection is that the decision —
(a) is 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, or
(b) is authorised or required by or under any enactment.
(7) The condition in this subsection is that either —
(a) the effect of the decision is to grant a request of the data subject, or
(b) steps have been taken to safeguard the legitimate interests of the data subject (for example, by allowing him to make representations).
(8) If the High Court is satisfied on the application of a data subject that a person taking a decision in respect of him ("the responsible person") has failed to comply with subsection (1) or (2)(b), the court may order the responsible person to reconsider the decision, or to take a new decision which is not based solely on such processing as is mentioned in subsection (1).
(9) An order under subsection (8) shall not affect the rights of any person other than the data subject and the responsible person."

(19) *"38. Request for assessment*
(1) A request may be made to the Supervisor by or on behalf of any person who is, or believes himself to be, directly affected by any processing of personal data for an assessment as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of this Act.
(2) On receiving a request under this section, the Supervisor shall make an assessment in such manner as appears to him to be appropriate, unless he has not been supplied with such information as he may reasonably require in order to —
(a) satisfy himself as to the identity of the person making the request, and
(b) enable him to identify the processing in question.
(3) The matters to which the Supervisor may have regard in determining in what manner it is appropriate to make an assessment include —
(a) the extent to which the request appears to him to raise a matter of substance,
(b) any undue delay in making the request, and
(c) whether or not the person making the request is entitled to make an application under section 5 in respect of the personal data in question.
(4) Where the Supervisor has received a request under this section he shall notify the person who made the request —
(a) whether he has made an assessment as a result of the request, and
(b) to the extent that he considers appropriate, having regard in particular to any exemption from section 5 applying in relation to the personal data concerned, of any view formed or action taken as a result of the request."

(20) *"11. Compensation for failure to comply with certain requirements*
(1) An individual 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 that damage.

(2) An individual who suffers distress 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 that distress if —
(a) the individual also suffers damage by reason of the contravention, or
(b) the contravention relates to the processing of personal data for the special purposes, or
(c) the contravention consists of a failure to comply with a request under section 5 in the circumstances specified in section 5(9)(b).
(3) In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned."