

Background Information on Isle of Man Data Protection Legislation



The Isle of Man laws relating to data protection are contained in the Isle of Man Data Protection Act 2002 (the “DPA 2002”). The DPA 2002 mirrors much of the UK Data Protection Act 1998.

Definitions

The DPA 2002 uses a number of important definitions, the main ones of which are:

- **“Data controller”** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
 - **“Personal data”** means data which relate to a living individual who can be identified:
 - a) from those data, or
 - b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
- **“Processing”**. The term processing is given a very wide meaning and very little undertaken in regard to data is likely to fall outside of this definition. “Processing” in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:-
 - a) organisation, adaptation or alteration of the information or data;
 - b) retrieval, consultation or use of the information or data;
 - c) disclosure of the information or data by transmission, dissemination or otherwise making available; or
 - d) alignment, combination, blocking, erasure or destruction of the information or data.
 - **“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,
 - e) his physical or mental health or condition,
 - f) his sexual life,
 - g) the commission or alleged commission by him of any offence, or 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.
 - 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.

Where a data controller is processing sensitive personal data, extra provisions need to be complied with. For further details see below.

- **“Data processor”** means any person who processes data on behalf of the data controller (other than an employee of the data controller).
- **“Data subject”** means an individual who is the subject of personal data.
- **“Data Protection Supervisor”**. The Office of the Data Protection Supervisor is the body responsible for administration of the DPA 2002 in the Isle of Man.

Data Protection Principles

Data controllers are obliged to comply with eight data protection principles (the “Data Protection Principles”) each with detailed statutory guidelines. They can be summarised as follows:

1. First Data Protection Principle

Personal data must be processed fairly **and** lawfully and must not be processed unless:

- a) at least one of the conditions in schedule 2 to the DPA 2002 is met;

And

- b) in the case of sensitive personal data, at least one of the conditions in schedule 3 to the DPA 2002 is **also** met.

2. Second Data Protection Principle

Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with that purpose or those purposes.

The purpose or purposes for which personal data are obtained may be specified in a notice given by the data controller to the data subject or in a notification to the Data Protection Supervisor.

In determining whether any disclosure of

personal data is compatible with the purpose or purposes for which the data was obtained, regard must be had to the purpose or purposes for which the personal data is intended to be processed by any person to whom it is disclosed.

3. Third Data Protection Principle

Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. In complying with this principle, data controllers should seek to identify the minimum amount of information that is required in order properly to fulfil their purpose.

It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used.

4. Fourth Data Protection Principle

Personal data must be accurate and, where necessary, kept up to date.

5. Fifth Data Protection Principle

Personal data processed for any purpose or purposes must not be kept for longer than is necessary for that purpose or those purposes. To comply with the fifth data protection principle, data controllers will need to review their personal data regularly and delete the information which is no longer required for their purposes.

6. Sixth Data Protection Principle

Personal data must be processed in accordance with the rights of data subjects under the DPA 2002.

7. Seventh Data Protection Principle

Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Management and organisational measures taken by a data controller are as important as the technical ones.

A data controller must also take reasonable steps to ensure the reliability of any employees who have access to the personal data.

Where the processing of personal data is carried out by a data processor on behalf of a data controller, in order to comply with the seventh data protection principle, the data controller must:

- (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.

In addition, where a data processor does process data on behalf of a data controller, the data controller will not be regarded as complying with the seventh data protection principle unless:

- (a) the processing is carried out under a contract which is made or evidenced in writing and 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 data protection principle.

The seventh data protection principle relates to security of the processing of personal data as a whole and the measures to be taken by a data controller to provide security against any breaches of the DPA 2002, rather than just breaches of security.

8. **Eighth Data Protection Principle**

Personal data must not be transferred to a country or territory outside the Isle of Man 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. The level of protection must be adequate in all the

circumstances of the case (the interpretation provisions of the DPA 2002 provide further details to aid in the assessment of adequacy). Countries or territories within the European Economic Area (“EEA”) will be deemed to have an “adequate level of protection”. In addition, if the European Commission makes a finding that a particular country or territory has an “adequate level of protection” that will be sufficient for the purposes of the eighth data protection principle. The European Commission has made an adequacy finding for US companies that have “signed up” to the Safe Harbour provisions.

The European Commission also made a formal decision on 28 April 2004 recognising the Isle of Man as a jurisdiction with an adequate level of protection for personal data.

Notification Requirements

Data controllers are required to notify certain registrable particulars with the Data Protection Supervisor.

The particulars which a data controller is required to notify to the Data Protection Supervisor are:-

- a) his name and address;
- 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 for which the data are being or are to be processed;
- d) a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data; and
- e) the names, or a description of, any countries or territories outside the Isle of Man and to which the data controller directly or indirectly transfers or intends or may wish directly or indirectly to transfer, the data.

Notification lasts for twelve months and any changes in the particulars registered must be notified to the Data Protection Supervisor.

Personal data must not be processed unless an entry

in respect of the data controller is included in the Register maintained by the Data Protection Supervisor.

In addition to the registrable particulars referred to above, a notification must give a general description of the measures to be taken by a data controller for the purpose of complying with the seventh data protection principle (measures against misuse and loss of data).

Data being provided to a third party outwith the EEA

If the data is being provided to a third party outwith the EEA then the following questions must be asked:-

- 1) Is there an actual transfer of data taking place? There is a distinction between a transfer of data and data in transit. The eighth data protection principle only applies if there is a data move rather than just a pass through of personal data from one country to another.
- 2) Has the country in question been designated as adequate by the European Commission? Has the company in question signed up to the safe harbour arrangements in the USA?
- 3) Are there alternative grounds for concluding that the receiving company or country is nevertheless adequate in all the circumstances of the case?
- 4) Does one of the derogations under schedule 4 of the DPA 2002 apply? The most common example is that the data subject has given consent to the transfer – such consent must be freely given and the data subject must understand what he/she is agreeing to. A copy of schedule 4 of the DPA 2002 is attached.
- 5) Is there an alternative basis for transfer? (e.g. contracts based on standard terms approved by the EU Commission or arrangements approved by the Data Protection Supervisor in the IOM).

Should you have any questions or requests for further information please contact:

Claire Milne
Partner
cmilne@applebyglobal.com

Bahrain
Bermuda
British Virgin Islands

Cayman Islands
Hong Kong
Isle of Man

Jersey
London
Mauritius

Seychelles
Zurich