

## INTRODUCTION

The Isle of Man Data Protection Act 2002 came into operation on the 1<sup>st</sup> April 2003.

The Act has been drafted in order to meet the standards set out in the European Data Protection Directive 95/46/EC and is similar to the UK's Data Protection Act 1998. The Act also repeals and replaces the Data Protection Act 1986 and extends data protection principles to include personal data held in any form including manual records.

The European Data Protection Directive states in Article 1:

*"In accordance with this directive, Member States shall protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with the respect to the processing of personal data."*

The Act seeks to uphold these rights by ensuring that when a business or organisation lawfully requires to process information about an individual that it does so in a fair, reasonable and responsible manner.

This overview is intended to provide a basic understanding of the main provisions of the Act and what it means to you either as an individual or within your organisation. It does not provide a detailed interpretation of the Act

### **Acknowledgement**

Some of the information contained in this document has been extracted from guidance documents published by other Data Protection Authorities in the British Isles.

## CONTENTS

EXPRESSIONS.....	2
<i>DATA CONTROLLER</i> .....	3
<i>DATA PROCESSOR</i> .....	3
<i>PERSONAL DATA</i> .....	3
<i>PROCESSING</i> .....	3
<i>DATA SUBJECT</i> .....	3
DATA PROTECTION PRINCIPLES .....	4
<i>The First Principle: Fair and Lawful Processing</i> .....	5
<i>The Second Principle: Purpose for Which Data Are Obtained and Processed</i> .....	6
<i>The Third Principle: Adequacy and Relevance of Data</i> .....	7
<i>The Fourth Principle: Accuracy of Data</i> .....	7
<i>The Fifth Principle: Time for Keeping Data</i> .....	7
<i>The Sixth Principle: Rights of Data Subjects</i> .....	7
<i>The Seventh Principle: Measures Against Misuse and Loss of Data</i> .....	7
<i>The Eighth Principle: Transfer of Data Abroad</i> .....	8
INDIVIDUALS' RIGHTS .....	10
<i>Right of Access to Personal Information</i> .....	10
<i>Right to Prevent Processing Likely to Cause Damage Or Distress</i> .....	12
<i>Right to Prevent Processing for the Purposes of Direct Marketing</i> .....	13
<i>Rights In Relation To Automated Decision Making</i> .....	14
<i>Right to Seek Compensation for the Failure of A Data Controller to Comply with the Act</i> .....	14
<i>Right To Take Action To Rectify, Block, Erase Or Destroy Inaccurate Data</i> .....	15
ASSESSMENT BY THE SUPERVISOR .....	15
NOTIFICATION .....	16
EXEMPTIONS.....	17
APPENDIX A – LEGAL DEFINITIONS.....	19

# EXPRESSIONS

The Data Protection Act 2002 introduces new expressions. The legal definitions of some of these expressions are set out in Appendix A.

Some of the most important expressions are:

## DATA CONTROLLER

A Data Controller is a person business or organisation who decides for what purposes and how personal information will be used.

A Data Controller is obliged to follow the provisions of the Act. This obligation applies irrespective of whether the Data Controller is exempt from the notification regulations under the Act or has not notified (registered) in accordance with the Act.

## DATA PROCESSOR

A Data Processor is a person business or organisation (other than an employee of the Data Controller) that carries out processing of personal information on behalf of a Data Controller. A typical example of a Data Processor may be a business that processes a payroll on behalf of another business.

It is important to appreciate that a Data Controller remains fully responsible for the actions of the Data Processor under the Act. (See: The Seventh Principle)

## PERSONAL DATA

The definition of personal data means any information held in whatever form that can identify or more importantly could identify a living individual when combined with other information.

The Act applies to personal data held in any form including paper, recordings, CCTV images as well as data held on Computer.

## PROCESSING

It is important to appreciate that the definition of processing is so wide that it is difficult to envisage any action involving personal data that does not amount to processing within this definition.

## DATA SUBJECT

The person to whom the personal data relates. This definition is important when the rights of the Data Subject are considered.

# DATA PROTECTION PRINCIPLES

The Data Protection Act 2002 applies to personal information about a living individual.

Any organisation or business (Data Controller), which uses personal information ([personal data](#)) in any form, including paper, must do so in a manner that is compliant with the Act and, in particular, the eight Data Protection principles:

## Summary of the Principles

### **Personal data must be:**

1. Used fairly **and** lawfully;
2. Used for specific and lawful purposes, in a manner that is compatible with those purposes;
3. Adequate, relevant and not excessive;
4. Accurate and where necessary kept up to date;
5. Kept for no longer than necessary;
6. Used in accordance with the rights of individuals under this Act;
7. Kept secure to avoid unauthorised or unlawful use and accidental loss, destruction, or damage;

### **Personal data must NOT be:**

8. Transferred to another country unless that country has an adequate level of protection.

For a full description of the principles, refer to Schedule 1 of the Data Protection Act 2002

## **The First Principle: Fair and Lawful Processing**

### **Fair Processing**

The First Principle requires that not only must personal data be processed lawfully it must also be processed fairly. This means that an organisation should be open and honest with the individual and explain why the information is required and what it will be used for. Paragraphs 9 to 12 of Schedule 1 of the Act provides further information on fair processing.

The basic requirements of fair processing are that when an organisation obtains personal data from an individual it must ensure that the individual knows:

- The identity of the organisation
- The purpose for which the organisation intends to process the information
- And other information which is necessary. For example, if the organisation also intends to use the information for direct marketing it must inform the individual.

### **Lawful Processing**

For the processing to be lawful, it must meet one or more of the following conditions:

#### **Summary of the conditions for processing personal data**

- with the consent of the individual;
- for the performance of a contract with the individual;
- to comply with a legal obligation;
- to protect the vital interests of the individual;
- for the administration of justice, or the exercise of any statutory function;
- for the legitimate interests of the organisation, unless the interests of the individual would be prejudiced.

*For a full description of the conditions, refer to Schedule 2 of the Data Protection Act 2002*

It is a common misconception that an individual must consent to the use of their personal information. While an organisation must always use personal information fairly and lawfully, provided the organisation can satisfy at least one of the other conditions listed above then the consent of an individual is not required.

If an organisation uses [sensitive personal data](#) (see Appendix A) then, in an addition to the above conditions, one or more of the following conditions must also be met:

### **Summary of the conditions for processing sensitive personal data**

- with the explicit consent of the individual;
- to perform any right or obligation under employment law;
- to protect the vital interests of the data subject or another person;
- for the legitimate interests of a not-for-profit organisation;
- where the data have been made public by the individual;
- in connection with legal proceedings;
- for the administration of justice, or the exercise of any statutory function;
- for medical purposes;
- for equal opportunity monitoring;
- for any other purposes specified by Order by the Council of Ministers.

*For a full description of the conditions, refer to Schedule 3 of the Data Protection Act 2002*

### **The Second Principle: Purpose for Which Data Are Obtained and Processed**

In most cases, the second principle requires an organisation to inform the Data Protection Supervisor (see [Notification](#)) of the organisation's purposes for using personal information. Personal information can only be used for the purposes that have been defined.

If you intend to pass personal information to another organisation (disclosure), you must be satisfied that this disclosure will be fair and lawful. You need to consider the following:

- Is the individual aware that their personal information is to be passed to another organisation?
- Is the disclosure compatible with the purpose for which the personal information was obtained?
- Does the disclosure of the information satisfy one or more of the conditions set out in the First Principle?
- Has the organisation to which the disclosure will be made notified the Supervisor of their purpose for using the personal information?

### **The Third Principle: Adequacy and Relevance of Data**

This principle requires organisations, which use personal information to monitor the amount of personal information held to ensure that neither too much, nor too little, personal information is used and that the personal information is relevant for a specified purpose.

There may be occasions when an organisation wishes to use personal information that is not necessary for a specified purpose. Provided the individual has been made aware that this additional information is “optional” and has freely consented then it is acceptable for this additional information to be used.

### **The Fourth Principle: Accuracy of Data**

An organisation must take reasonable steps to ensure that information is accurate and, where necessary, kept up to date.

It is not necessary for all information to be kept up to date, for example, if the information is only used as an historical record, then it is not necessary for that information to be kept to date

Cases may arise when an individual states that the information held is inaccurate but the organisation disagrees. In such cases, a note to this effect must be attached to the information.

### **The Fifth Principle: Time for Keeping Data**

Organisations should develop a data retention policy and in accordance with that policy review the personal data held and remove any data which is no longer required for their purposes. The data retention policy must consider any statutory obligations with regard to the retention of data and ensure that the retention policy accords with the minimum statutory retention periods.

Organisations may consider the value of the information for historical purposes. The Act permits personal data processed for historical, statistical purposes to be kept indefinitely.

### **The Sixth Principle: Rights of Data Subjects**

Personal data must be processed in accordance with the rights of individuals (data subjects). For further information see [Individual Rights](#).

### **The Seventh Principle: Measures Against Misuse and Loss of Data**

Organisations must ensure that they provide adequate security for any personal data they use taking into account the nature and sensitivity of the information. In particular, organisations must consider the harm that could arise from unauthorised disclosure or loss of data.

Adequate security will be dependent upon the size of an organisation and the scale of its operation. Matters that need to be considered include:

- Does the Organisation have a Security policy?
- Is access to the information controlled?
- Are staff properly trained and aware of their responsibilities?
- Do procedures exist for detecting breaches?
- Where an organisation uses a third party (data processor) to process information; is this processing carried out under contract to ensure the third party only processes information in accordance with the organisation's instruction and does the third party have adequate security measures in place?

*Organisations are encouraged to follow the good practice standards set out in BS 7799 or ISO 17799.*

### **Staff Awareness**

The importance of staff awareness cannot be over stressed.

Many complaints and breaches of the Act occur due to inadvertent disclosure of information by a member of staff. Paragraph 18 of Schedule 1 of the Act specifically states that a business must take reasonable steps to ensure the reliability of staff who have access to personal data. If a breach occurs it will be important for a data controller to demonstrate that staff have been properly trained.

**Under Section 50, a person who discloses personal data without the consent of the data controller may be guilty of an offence.**

### **The Eighth Principle: Transfer of Data Abroad**

Before personal information can be transferred outside the Island an organisation must ensure that adequate protection exists for the information in the receiving country.

Countries within the European Economic Area, that is, European Union member states plus Norway, Iceland and Liechtenstein are deemed to have adequate protection. In addition, the European Commission has made adequacy findings for other countries, including Argentina, Guernsey, Jersey, Switzerland and Canada, and US companies that have "signed up" to the Safe Harbor provisions.

On the 28<sup>th</sup> April 2004, the European Commission formally decided that the Isle of Man has adequate data protection legislation.

There are cases where the eighth principle does **not** apply these include:

- Where consent of the individual has been given
- Is necessary for a contract with the individual
- For reasons of substantial public interest
- Where legal proceedings are involved
- To protect the vital interests of the individual
- Where the information is on a public register

*See Schedule 4 of the Act for further Information*

### **Transfers to other countries**

The European Commission has approved Model Contracts for the transfer of personal data to third countries.

The Model Contracts are available on

[http://ec.europa.eu/justice\\_home/fsj/privacy/modelcontracts/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm)

**Please ensure that you use the current Model Contract**

# INDIVIDUALS' RIGHTS

The Act gives rights to individuals in respect of personal data held about them.

These rights are:

- Right of Access to Personal Information
- Right to Prevent Processing likely to cause damage or distress
- Right to prevent processing for the purposes of direct marketing
- Rights in relation to automated decision making
- Right to seek compensation for any damage or distress caused by the failure of a Data Controller to comply with the requirements of the Act
- Right to take action to rectify, block, erase or destroy inaccurate data

*See sections 5 to 12 of the Act for further information*

## **Right of Access to Personal Information**

This is usually referred to as a Subject Access Request.

### **Your Right**

Under Section 5 of the Act, you have the right to know what personal information is processed about you and you can exercise your right by writing to the data controller.

In response to a subject access request you are entitled to a copy of the information held about you, both on computer and as part of a relevant filing system. You also have the right to receive a description of why your information is processed, anyone it may be disclosed to, and any information available to you about the source of the data.

### **Advice to Data Controllers**

#### **Recognising a Subject Access Request**

Although the Data Protection Supervisor has sample letters that an individual may use they are not required to do so. A letter requesting a data subject access does not need to mention the Data Protection Act 2002 – it may just say something as simple as “I want to see what you hold about me”.

#### **Responding to a Subject Access Request**

If you receive a written subject access request, you must deal with it promptly and in any case within 40 days from the date of receipt. It may be that you need further information from the person making the request to help you to locate the data. You may also require further information in order to satisfy yourself as to the identity of the person making the request or to assist you to locate the information being sought.

A data controller is entitled, to ask for a fee of not more than £10 (£50 for Health Records in certain circumstances) and the 40 days does not begin until this is received. However you must not delay informing the individual that a fee is required and you must endeavour to response to the request as soon as possible, that is, do not wait 40 days.

You may send the information as a computer printout, in a letter, or on a form. However, it should be easy to understand and any codes should be explained.

Subject access should be handled in the light of an on-going relationship with the data subject. Routine requests for limited information, which would in any case form part of normal transactions, should continue to be processed in that way. It is also possible that by simply providing access to inspect and make copies of any files would satisfy the person making the request.

***Do not try to turn everything into a subject access request, however, it is important that your staff know how to recognise a subject access request and realise that it must be dealt with urgently.***

### **Exemptions from Subject Access Request**

In replying to a Subject Access request there are certain exemptions from disclosure which may apply:

**Summary of exemptions from subject access**

- 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
- Journalism, literature and art
- Public information
- As specified by Order

Tynwald has approved further exemptions in the following Orders:

**Orders**

- Data Protection (Subject Access Modification)(Health) Order 2003
- Data Protection (Subject Access Modification)(Social Work) Order 2003
- Data Protection (Subject Access Modification)(Education) Order 2003
- Data Protection (Subject Access Exemptions)(Adoption Etc.) Order 2003
- Data Protection (Corporate Finance Exemption) Order 2003
- Data Protection (Crown Appointments) Order 2003

Further miscellaneous exemptions are provided in Schedule 7 of the Act.

*If you rely on an exemption you are not obliged to inform the Data Subject that an exemption has been applied.*

### **Data about other individuals (third parties)**

Sometimes, giving full access to personal data cannot be done without revealing information about others. *Third party information should not normally be disclosed without the consent of the individuals concerned.*

When you decide that information about other individuals must be excluded, there is still an obligation to supply as much information to the data subject as possible. Do not remove information about other individuals if it is clear that consent is not required, either because the data subject already knows the information, or is given by professionals as part of their normal duties (e.g. a medical practitioner). Do blank out information about others so as to protect their identity.

Provide this edited response to the data subject and if he/she is satisfied you need take no further steps to seek consent from third parties.

### **Failure to comply with a Subject Access Request**

If a Data Controller fails to comply with a subject access request then the individual may apply to the High Court. The Court may:

- Order the Data Controller to Comply with the request
- Impose a fine up to £5000

An individual may also seek compensation for distress (alone) where a failure to comply with a request has occurred.

*Under section 58 of the Act, Government Departments are not exempt from prosecution.*

### **Right to Prevent Processing Likely to Cause Damage Or Distress**

#### **Your Right**

Under section 8 of the Act, you have the right to object to any processing of your personal data that is causing or would cause unwarranted substantial damage or distress either to you or another person.

However this right does not apply when:

## **Summary of instances when right does not apply**

The processing is performed

- with the consent of the individual;
- for the performance of a contract with the individual;
- to comply with a legal obligation;
- to protect the vital interests of the individual;
- as specified by Order

Refer to paragraphs 1 to 4 of Schedule 2 of the Data Protection Act 2002

## **Right to Prevent Processing for the Purposes of Direct Marketing**

### **Your Right**

Under section 9 of the Act, you are entitled to require a data controller to cease, or not to start, processing your personal data for the purpose of direct marketing. This right applies even if you had previously consented.

You can exercise this right by writing to the data controller, who must comply as soon as possible. If a data controller fails to comply, then you may apply to the Court for an Order.

### **Junk Mail**

There are other actions you can take to prevent personalised "Junk Mail" and unsolicited phone calls or faxes. Please contact the Data Protection Supervisor if you require further information.

## **Advice to Data Controllers**

When collecting data from members of the public, you should give them the opportunity to let you know whether or not they wish to receive marketing material from you. If they do not wish to receive your promotional materials, you must ensure that you can suppress their details on any mailing lists you use.

If you intend to pass personal data to other companies, including companies in the same group, for direct marketing purposes, again you must first inform the individuals concerned and receive their consent. This should be done when you first collect the data, perhaps on an application form. You must not pass on the details of anyone who objects to their details being used in this way.

If you have not previously sent out marketing material or passed on details to third parties for marketing, you should obtain the consent of existing customers before beginning to process their data for either of those purposes.

The above advice constitutes fair processing as required by the First Principle.

## **Rights In Relation To Automated Decision Making**

### **Your Right**

Under Section 10 of the Act, you have the right, by notice in writing, to require a data controller to ensure that no decision that significantly affects you is based solely on the processing by automatic means of personal data.

Although not exhaustive, specific examples are provided in the Act, such as performance at work. Another example may be a web site where a credit decision is based solely upon information provided by you in response to questions asked.

A data controller must inform you if a decision was based solely upon processing by automatic means as soon as reasonably practical. Once a data controller has replied, you have a further 21 days in which to write to the data controller to require the data controller to reconsider the decision or to take a new decision on a different basis.

The data controller has a further 21 days to write to you and explain what steps will be taken.

There are decisions that are exempt from this right. An exemption would apply if the following conditions were met:

#### **Summary of exempt decision**

The decision was taken either with

- a view to entering into a contract with the individual; or
- for the performance of a contract with the individual; or
- to comply with a legal obligation;

and

- the effect of the decision must be to grant a request of the individual; or
- steps have been taken to safeguard the interests of the individual, such as allowing the individual to make representations.

Refer subsections 10(5) and 10(6) for further information

If a data controller fails to comply, then you may apply to the Court. The Court may order the decision to be reconsidered or to take a new decision, provided the Court is satisfied that the data controller has failed to comply.

## **Right to Seek Compensation for the Failure of A Data Controller to Comply with the Act**

### **Your Right**

Under section 11, you have the right to seek compensation through the Court for any damage suffered as a result of any contravention of the Act by a data controller. You may also seek compensation for distress if the contravention:

- also caused damage, or
- relates to processing for the special purposes of Journalism, Literature or Art; or
- consists of a failure of a data controller to comply with a subject access request under section 5 of the Act.

Refer to Section 11 for further information

It is a defence for a data controller to prove that he had taken all reasonable care to comply.

The individual may seek compensation from the data controller. If the matter is not settled between the parties, the individual may apply to the Court. A claim for compensation may be made alone or combined with an application in respect of any breach of the Act.

The Data Protection Supervisor has no power to award compensation, nor can the Supervisor assist with legal proceedings. Anyone considering legal action should always seek the advice of a qualified Manx Advocate.

## **Right To Take Action To Rectify, Block, Erase Or Destroy Inaccurate Data**

### **Your Right**

Under section 12, you have the right to apply to the Court for an order requiring the data controller to rectify, block, erase, or destroy such data relating to you as are inaccurate, including any expression of opinion contained in personal data relating to you which the Court finds inaccurate.

### **Right to correct or remove incorrect data by a credit reference agency**

Under the Consumer Credit Act 1974 (an Act of the UK Parliament) you also have the right to have any incorrect information removed or amended.

## **ASSESSMENT BY THE SUPERVISOR**

In addition to the specific rights listed above, a data controller must process your personal data in accordance with the Act and, in particular, the eight data protection principles.

If you believe that a data controller is breaching any of the provisions of the Act, you may, under section 38 of the Act, request the Data Protection Supervisor to undertake an assessment to determine whether the processing is being carried out in accordance with the Act.

If the Supervisor determines that processing is being carried out in breach of the Act, then the Supervisor can take enforcement action against the data controller.

Under section 36 of the Act, the Supervisor may issue an Enforcement Notice against the data controller. Failure to comply with an Enforcement Notice is an offence.

## NOTIFICATION

Notification replaces the registration scheme under the 1986 Act. See sections 13 to 22 of the Act for further information.

Notification is the method by which a data controller informs the Supervisor of the purposes for processing personal data. The details provided by the data controller are then used by the Supervisor to make an entry describing this processing in the register, which is open to public inspection.

The process of Notification is regulated by the Data Protection (Notification) Regulations 2003. These regulations provide some exemptions from Notification.

Detailed information about Notification can be found in the Notification Handbook, which is available from the Supervisor's Office and can also be found on the web site.

Details of the fee for Notification by a data controller can be obtained from the Supervisor's Office. There is an exemption for "not for profit" organisations from the payment of fees.

The period of Notification is one year.

If a person wishes a certified copy of an entry in the register, there is a fee of £2 payable.

It is an offence to process personal data without Notification unless an exemption applies.

# EXEMPTIONS

There are a number of exemptions and modifications to various provisions of the Act. The main exemptions are contained in Sections 23 to 35 of the Act and Schedule 7 (miscellaneous exemptions).

Further exemptions and modifications are provided in the following Orders:

## Orders

- Data Protection (Subject Access Modification)(Health) Order 2003
- Data Protection (Subject Access Modification)(Social Work) Order 2003
- Data Protection (Subject Access Modification)(Education) Order 2003
- Data Protection (Subject Access Exemptions)(Adoption Etc.) Order 2003
- Data Protection (Corporate Finance Exemption) Order 2003
- Data Protection (Crown Appointments) Order 2003

It is not easy to categorise the exemptions, but, in most cases, the exemptions either provide an exemption from **“the subject information provisions”** or **the non disclosure provisions”**. Further information on these provisions can be found in Section 23 of the Act.

## Subject Information Provisions

- The first principle (fair and lawful processing) but only to the extent that the data must be processed fairly in accordance with paragraph 10 of Schedule 1
- Subject Access Request under section 5.

Exemption or modifications from the subject information provisions are provided under

- Section 25(2) Crime and Taxation
- Section 26 Orders relating to Health Education and Social work
- Section 27 Regulatory activity
- Section 30 Information available to the public by or under statutory provision

### Non Disclosure Provisions

- The first principle (fair and lawful processing) but only to the extent that the data must be processed in accordance with the conditions in Schedule 2 and 3.
- The Second, Third, Fourth and Fifth principles.
- Prevention of processing likely to cause damage or distress under section 8.
- Rectification, blocking, erasure and destruction under sections 12(1) to 12(3)

But only to the extent that the disclosure would be inconsistent with these provisions.

Exemption or modifications from the non-disclosure provisions are provided under

- Section 25(3) Crime and Taxation
- Section 30 Information available to the public by or under statutory provision
- Section 31 Disclosures required by law or made in connection with legal proceedings

For further information and advice please contact the ODPS:

<b>By Post:-</b>	PO Box 69 DOUGLAS Isle of Man IM99 1EQ	<b>In Person:</b>	Willow House Main Road Onchan Isle of Man
		Office Hours: 9.00am to 5.00pm Monday to Friday	

**By Telephone:** 01624 693260

**By E-mail:** [enquiries@odps.gov.im](mailto:enquiries@odps.gov.im)

**Website:** [www.gov.im/odps](http://www.gov.im/odps)

## APPENDIX A – Legal Definitions

**DATA** means information which:

- (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
- (b) is recorded with the intention that it should be processed by means of such equipment,
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or
- (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record

**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

**DATA PROCESSOR**, means

in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller

**DATA SUBJECT** means an individual who is the subject of personal data

**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** 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

**RELEVANT FILING SYSTEM** means

any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

**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.

**THE SPECIAL PURPOSES** means any one or more of the following:

- (a) the purposes of journalism,
- (b) artistic purposes, and
- (c) literary purposes.