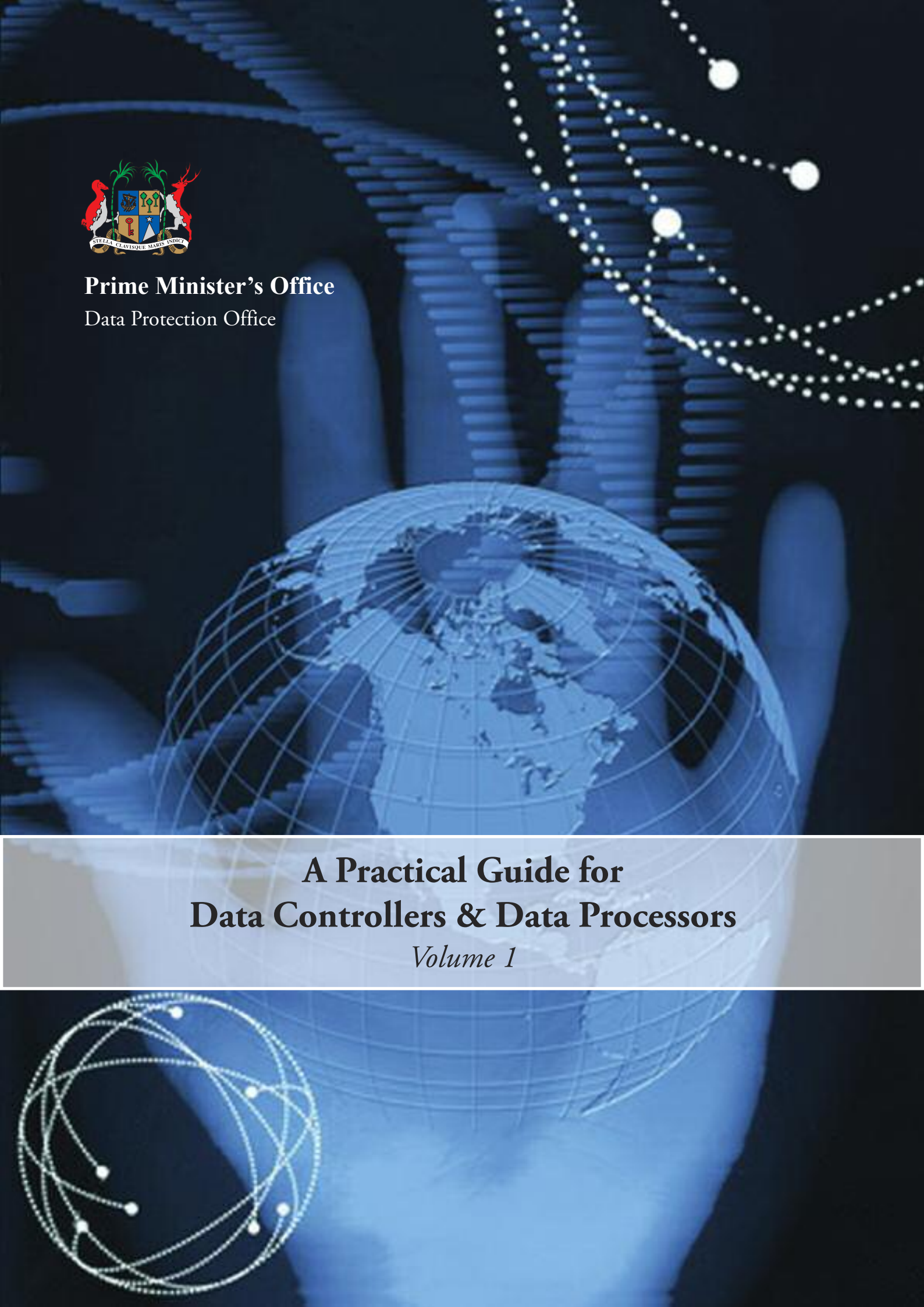


Prime Minister's Office
Data Protection Office

A Practical Guide for Data Controllers & Data Processors

Volume 1

"A Practical Guide for Data Controllers & Data Processors"

Volume I

Mrs Drudeisha Madhub,
Data Protection Commissioner

Contact Details
Tel No.: 201 3604
E-mail: pmo-dpo@mail.gov.mu
Website: http://dataprotection.gov.mu

Table of Contents

Page

INTRODUCTION 5

Definitions 6

(1) Data
(2) Automated data
(3) Manual data
(4) Relevant filing system
(5) Personal data
(6) Processing
(7) Data Subject
(8) Data Controller
(9) Data Processor
(10) Sensitive personal data

OUTLINE 7

Types of Data Controllers
Responsibilities of data controllers
Group companies and subsidiary companies
Data Processors
Responsibilities of data processors
How is the Act enforced?

DATA PROTECTION RULES (13 RULES) 10-42

CONCLUSION 43-48

How to organise yourself to ensure the protection of data within your organisation?
Obligations on retention and security need to be addressed
Dealing with Subject Access Requests
Self Regulation and Codes of Practice
How can the Data Controller initiate a Statutory Code of Practice?

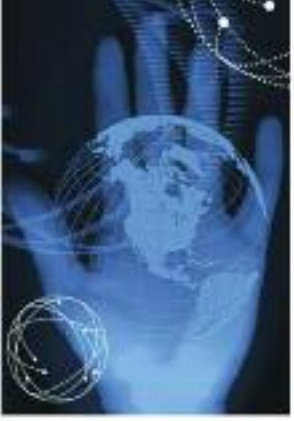
Introduction

No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.

Article 17 of the International Covenant on Civil and Political Rights

Information relating to individuals, called 'personal data', is collected and used in many aspects of everyday life. An individual gives personal data when he/she, for example, registers for a library card, signs up for gym membership, opens a bank account, etc. Personal data can be collected directly from the individual or from existing databases. These data may subsequently be used for other purposes and/or shared with other parties. Personal data can be any data that identifies an individual, such as a name, a telephone number, or a photo. Advancement in computer technology along with new telecommunications networks is allowing personal data to travel across borders with greater ease. Therefore, as personal data is collected and exchanged more frequently, regulation on data transfers becomes necessary. In this context, laws regarding data protection became necessary and they demand good data management practices on the part of the entities who process data, called 'data controllers'. These include the obligation to process data fairly and in a secure manner and to use personal data for explicit and legitimate purposes. The Data Protection Act also guarantees a series of rights for individuals, such as the right to be informed when personal data was processed and the reason for this processing, the right to access the data and if necessary, the right to have the data amended or deleted.

Data protection law reinforces common sense rules of information handling, which most organisations must follow. It is there to ensure that organisations manage the personal information they hold in a sensible way. Organisations must also keep the information accurate and up to date and they must only keep it for as long as they need it and for a specified purpose. Organisations should adopt a good business sense of treating their customers and their information with respect and in compliance with the Data Protection Act 2004.



Definitions

As with any legislation, certain terms have a particular meaning. The following are some important definitions:

Data means information in a form which can be processed. It includes both automated and manual data.

Automated data means, broadly speaking, any information on computer, or information recorded with the intention of putting it on computer.

Manual data means information that is kept as part of a relevant filing system, or intended to form part of a relevant filing system.

Relevant filing system means any set of information that, whilst not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

Personal data means data relating to a living individual who is or can be identified either from the data or other information or opinion likely to come into or is in the possession of the data controller.

Processing means performing any operation or set of operations on data, including:

collecting, organising, or altering the data;

retrieving, consulting , using, storing or adapting the data;

disclosing the data by transmitting, disseminating or otherwise making it available; or

aligning, combining, blocking, erasing or destroying the data.

Data Subject is a living individual who is the subject of personal data.

Data Controller is a person (natural or legal) who, either alone or with others, decides as to the purposes for which and in the manner personal data are to be processed.

Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial or ethnic origin; political opinion or adherence; religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

OUTLINE

What is data protection?

It is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. The Data Protection Act 2004 confers rights on individuals as well as responsibilities on those persons processing personal data.

Are you a "data controller"?

Data controllers are the people or body, 'who determine the purposes and the means of the processing', both in the public and in the private sector. A medical practitioner would usually be the controller of the data processed on his clients; a company would be the controller of the data processed on its clients and employees; a sports club would control the data processed on its members and a public library controls the data processed on its users. Data controllers are required to observe several principles. These principles not only aim to protect the data subjects but also are a statement of good business practices that contribute to reliable and efficient data processing.

Each data controller must adhere to the Data Protection Act when he is established in Mauritius and where he is not established in Mauritius but uses equipment in Mauritius for processing data, other than for the purposes of transit through Mauritius. Where the data controller is not established in Mauritius, he must nominate a representative who resides in Mauritius to carry out his data processing activities through an office in Mauritius.

A data controller is therefore the natural person (the individual) or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files within your organisation. Being a data controller carries with it serious legal responsibilities, so you should be quite clear if these responsibilities apply to you or your organisation. If you are in any doubt, or are unsure about the identity of the data controller in any particular case, you should consult your legal adviser or seek the advice of the Data Protection Commissioner.

In essence, you are a data controller if you can answer **YES** to the following question:-

- ✓ Do you keep or process any information about living people?
- ✓ In practice, to find out who controls the contents and use of personal information kept, you should ask yourself the following questions:-
- ✓ who decides what personal information is going to be kept?
- ✓ who decides the use to which the information will be put?

If your organisation controls and is responsible for the personal data which it holds on its employees, clients, customers, suppliers, etc. then your organisation is a data controller. If, on the other hand, you hold the personal data, but some other organisation decides and is responsible for what happens to the data, then that other organisation is the data contoller, and your organisation is a "data processor".

Types of Data Controllers

Data controllers can be either individuals or "legal persons" such as companies, Government Departments or ministries and voluntary organisations. Examples of cases where the data controller is an individual include general practitioners, pharmacists, politicians and sole traders, where these individuals keep personal information about their patients, clients, constituents etc.

Group Companies and Subsidiary Companies

It is common in the business world for a holding company to own one or more subsidiary companies. If personal data is flowing within the group of companies, who is the data controller? In answering this question, it should be noted that each company, whether it is a parent company or a subsidiary, is a distinct legal person with its own set of legal and data protection responsibilities.

Each company within a group may therefore be a data controller in respect of the personal data which it has obtained and for which it is legally responsible; and it is necessary for each data controller to assess whether disclosures of personal data to other group companies are permissible. It is only in rare cases that two or more companies may properly exercise legal or de facto control and responsibility for a given set of personal data. In such cases, the companies are regarded as joint data controllers.

Responsibilities of Data Controllers

All data controllers must comply with certain important rules about how they collect and use personal information.

Data controllers must register annually with the Data Protection Commissioner, in order to make transparent their data handling practices.

Data Processors

As mentioned above, if you hold or process personal data, but do not exercise responsibility for or control over the personal data, then you are a "data processor". Examples of data processors include payroll companies, accountants and market research companies, all of which could hold or process personal information on behalf of someone else.

It is possible for one company or person to be both a data controller and a data processor, in respect of distinct sets of personal data. For example, a payroll company would be the data controller in respect of the data about its own staff, but would be the data processor in respect of the staff payroll data it is processing for its client companies.

A data processor is distinct from the data controller for whom they are processing the personal data. An employee of a data controller, or a section or unit within a company which is processing personal data for the company as a whole, is not a "data processor". However, someone who is not employed by the data controller, but is contracted to provide a particular data processing service (such as a tax adviser, or a telemarketing company used to manage customer accounts) would be a data processor. A subsidiary company owned by a data controller to process personal data on its behalf (for example to manage the payroll) is a distinct legal person and is a data processor.

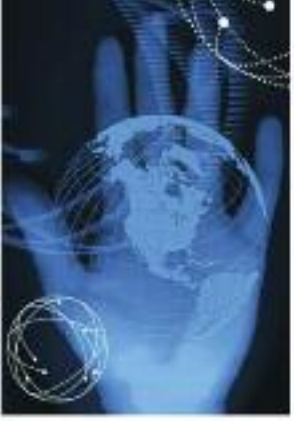
Responsibilities of Data Processors

Unlike data controllers, data processors have a very limited set of responsibilities under the Data Protection Act. These responsibilities concern the necessity to keep personal data secure from unauthorised access, alteration, unlawful disclosure, destruction or accidental loss and the duty to destroy data whenever he receives such a notification from the data controller.

How is the Act enforced?

The Commissioner's role is to ensure that those who keep personal information comply with the provisions of the Act. She has a wide range of enforcement powers to assist her in ensuring that the principles of data protection are being observed. These powers include the serving of legal notices compelling data controllers to provide information needed to assist her enquiries, or compelling a data controller to implement one or more provisions of the Act. She may investigate complaints made by the general public or carry out investigations proactively. She may, for example, authorise officers to enter premises and to inspect the type of personal information kept, how it is processed and the security measures in place. You and your staff must cooperate fully with such officers.

A data controller found guilty of an offence under the Act can be fined to a maximum of Rs 200,000 and imprisoned to a maximum of five years.



Data Protection Rules

Your legal responsibilities as a Data Controller

Data Protection Rule 1:

Fair Collection of personal data
Fair Processing of personal data
Fair processing of sensitive personal data
Comment: The nature of consent
Fair Collection: Test Yourself
Practical steps

Data Protection Rule 2:

Specifying the Purpose for Processing Personal Data
Practical steps

Data Protection Rule 3:

Duty to Destroy Personal Data

Data Protection Rule 4:

Use and Further Processing of Personal Information
Use and Disclosure: Test Yourself
Practical steps

Data Protection Rule 5:

Security of Personal Data
Appropriate Organisational and Security Measures
Dealing with Data Processors
Access Control
Encryption
Anti-Virus Software
Firewalls
Automatic Screen Savers
Logs and Audit Trails
The Human Factor
Remote Access

Wireless Networks
Laptops
Back-up Systems:-
What constitutes lost, destroyed or damaged data?
What is the purpose of backing-up data?
For how long should back-up data be held?
Physical Security
Keeping Personal Data Secure: Test Yourself
Practical steps

Data Protection Rule 6:

Accurate and Up-To-Date Data Processing of Personal Data
Accurate and Up-to-date Data: Test Yourself
Practical steps

Data Protection Rule 7:

Adequate, Relevant and not Excessive
Adequate, Relevant and not Excessive Personal Data: Test Yourself
Practical steps

Data Protection Rule 8:

Retention of Personal Data
Retention of Personal Data: Test Yourself
Practical Steps

Data Protection Rule 9:

Transfers Abroad:-
Adequate Standards of Data Protection
The Four Alternative Measures
Approval of the Data Protection Commissioner

Data Protection Rule 10:

Right of Access to Personal Data
What Must You Do In Response To An Access Request?
Are There Exceptions or Limitations on The Right of Access To Personal Data?

Data Protection Rule 11:

Exempted Forms of Data Processing (Only From Certain Sections Of The DPA):-

Crime and Taxation

National Security

Health and Social Work

Regulatory Activities

Journalism, Literature and Art

Research, History and Statistics

Information available to the public under the law

Legal Professional Privilege

Domestic Purposes

Data Protection Rule 12:

The Direct Marketing Sector

Dealing with Unsolicited Direct Marketing

Postal Marketing

Do I need people's consent before contacting them for direct marketing?

Does consent have to be written, or can it be implied?

Rather than give people an opt-out, can I just notify them that their data will be used for direct marketing?

Is an "opt-out" sufficient, or do I need an "opt-in" consent clause?

Can I make use of personal information obtained in the past for a different purpose?

Can I sell a list of personal data for direct marketing?

How do I obtain consent from children for direct marketing?

Do people have the right to be taken off my company's mailing list?

As a direct marketer, must I register with the Data Protection Commissioner?

Can I put up an advertisement indicating that personal data is or may be for sale in breach of the Act?

The basic rules:-

Residential subscribers - phone calls

Residential subscribers - faxes

Business subscribers - phones & faxes

Business subscribers - phones & faxes

Time factor

Making a complaint

Electronic Mail

Data Protection Rule 13:

Data Matching

What is a Data Matching Procedure?

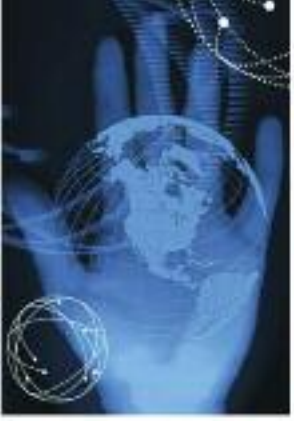
Under What circumstances can a data controller carry out a data matching procedure?

What does adverse action mean?

In what circumstances may the data controller take any adverse action against the data subject?

Data Protection Checklist:-

Assess your own Data Protection Policy



The Data Protection Rules

Your legal responsibilities as a Data Controller

You have certain key responsibilities in relation to the information which you keep on a computer or in a structured manual file about individuals. These may be summarised in terms of Thirteen Rules which you must follow, and which are listed below.

YOU MUST:-

- Collect and process the information fairly
- Keep it only for one or more specified and lawful purposes
- Destroy data where the purpose for keeping it has lapsed
- Process it only in ways compatible with the purposes for which it was given to you initially
- Keep it safe and secure
- Keep it accurate and up-to-date
- Ensure that it is adequate, relevant and not excessive
- Retain it no longer than is necessary for the specified purpose or purposes
- Only transfer personal data to a country if that country ensures an adequate level of protection for data subject rights in relation to the processing of personal data
- Give a copy of his/her personal data to any individual, on request
- Disclose lawfully personal data
- Stop or not to begin processing of personal data for direct marketing upon the request of the individual concerned
- Carry out a data matching procedure only when the individual concerned has given his consent and the Data Protection Commissioner has also consented and imposed any conditions for the carrying out of the procedure or that the procedure is required by law.

These provisions are binding on every data controller. Any failure to observe them would be a breach of the Act.

Data Protection Rule 1

Fair Collection

This is the fundamental principle of data protection. If your organisation wishes to keep personal information about people on computer, then you must collect the information lawfully, and you must process (or use) the information fairly.

This principle requires that -

At the time of collecting personal information, the data controller must ensure that the individuals concerned (the data subjects) are made fully aware of:

- the fact that the data is being collected;
- the name and address of the persons who are collecting it (though this may often be implied);
- to what use the information will be put or what is/are the purposes for which information is being collected;
- the persons or category of persons to whom the information will be disclosed;
- whether or not the supply of data by the individual is voluntary or obligatory;
- the consequences for the individual if the requested information is not provided;
- whether or not the consent of the individual is required for any processing of the information;
- the right of access of the individual to the possibility of correction, destruction of personal data to be provided by him.

Secondary or future uses of the personal data, which do not repeat the prior collection of personal data without any material difference, and where a period of 12 months have elapsed since the prior collection, should be brought to the attention of the individual concerned. Individuals should be given the option of saying whether or not they wish their information to be used in these other ways.

If a data controller has information about people and wishes to use it for a new purpose (which was not disclosed and perhaps not even contemplated at the time the information was collected), he or she is obliged to give an option to individuals to indicate whether or not they wish their information to be used for the new purpose.

Where the data controller cannot inform the individual concerned at the time of collection, he must make available to the individual all the relevant information as soon as practicable.

Where the data subject cannot reasonably expect to be identified from the personal data collected, the data controller does not have to provide the relevant information to the data subject.

These are the ways a data controller achieves transparency and informed consent which are the touchstones of fairness in data protection.

Fair Processing of personal data

First and foremost, section 24 (1) provides that *"no personal data shall be processed, unless the data controller has obtained the express consent of the data subject."*

However, section 24 of the Act further details a number of conditions, at least one of which must be met, in order to demonstrate that personal data are being processed fairly. These include that the data subject has consented to the processing, **or** that the processing is necessary for at least one of the following reasons:

- The performance of a contract to which the data subject is party,
  Or
- In order to take steps required by the data subject prior to entering into a contract,
  Or
- In order to comply with any legal obligation to which the data controller is subject,
  Or
- To protect the vital interests of the data subject ,
  Or
- For the administration of justice,
  Or
- in the public interest.

Fair processing of sensitive personal data

If you are processing sensitive data, you must satisfy the requirements for processing personal data set out above along with at least one of the following conditions, set out in section 25 of the Act:

- The data subject has given express consent, or
- The data subject has made the data public; or
- The processing is necessary in order to exercise or perform a right or obligation which is conferred or imposed by law on the data controller in connection with his employment; or
- The processing is necessary to protect the vital interests of the data subject or of another person in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain such consent; or

- The processing is necessary 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; or
- The processing is necessary for the performance of a contract to which the data subject is a party; or
- The processing is necessary in order to take steps required by the data subject prior to entering into a contract; or
- The processing is necessary for compliance with a legal obligation to which the data controller is subject; or
- The processing is carried out by any entity or any association which exists for political, philosophical, religious or trade union purposes in the course of its legitimate activities and the processing is carried out in accordance with the Act, is related only to individuals who are members of the charitable entity or association and does not involve disclosure of the personal data to a third party without the consent of the data subject; or
- The information being processed has been made public as a result of steps deliberately taken by the data subject; or
- The processing is required by law.

Comment: The nature of consent

Sections 24 and 25 of the Act refer to express consent. Consent means voluntary agreement to some act, practice or purpose. It has two elements: knowledge of the matter agreed to, and voluntary agreement. Express consent is given explicitly, either orally or in writing. Consent is invalid if there is extreme pressure or coercion. Only a competent individual can give consent although an organisation can ordinarily assume capacity unless there is something to alert it otherwise. Competence means that individuals are capable of understanding issues, forming views based on reasoned judgments and communicating their decisions. This means that a data subject must be aware of and understand the purposes for which his/her data are being processed. The general law about competence and incapacity will apply to the issue of consent.

If relying upon consent, the key test will be to demonstrate that consent exists. Express consent need not require a data subject to sign a form in all cases. Consent can be understood to be explicit where a person volunteers personal data after the purposes in processing the data have been clearly explained. Thus a clear explanation on a form, a web page, or the delivery of a script by properly trained telephone staff might be sufficient to demonstrate consent has been explicitly given.

No age limit is associated with consent. However, it is important that the data subject appreciates the nature and effect of such consent. Therefore, different ages might be set for different types of consent. If in doubt, it is advised that you select the common age of majority, 18 years. Where a person is unlikely to be able to appreciate the nature or effect of consent,

by reason of physical or mental incapacity or age, then the person who has parental authority or guardian may give consent on behalf of the data subject. These are the only circumstances in which a third party may give consent on behalf of a data subject.

Fair Collection: Test Yourself

You should be able to answer **YES** to the following questions:-

When people are giving you information,

- ✓ do they know what information you will keep about them?
- ✓ do they know the purpose for which you keep and use it?
- ✓ do they know the people or bodies to whom you disclose or pass it?

If you collect information about an individual from a third party (e.g., from a husband about his wife) you have to consider whether the individual (in this case the wife) needs to be made aware of what is being noted about her as well as the purpose in holding that data. In general, the fair collection principle requires that every individual about whom information is collected for holding will be aware of what is happening.

Practical steps

Where you use application forms or standard documentation in signing up new customers or clients, you should explain your purposes/uses etc. on such forms or documentation.

Where your customers or clients mostly call to your premises, you might consider displaying a notice with such explanations in your reception area for their information.

Data Protection Rule 2

Specifying the Purpose

You must not keep information about people unless it is held for a specific and lawful purpose. It is therefore unlawful to collect information about people routinely and indiscriminately, without having a sound, clear and legitimate purpose for so doing.

The Data Protection Commissioner must include in the public register entry the statement by data controllers of their purpose for holding personal data. If such data controllers keep or use personal data for any purpose other than that specified purpose, they may be found guilty of an offence under the DPA.

Having A Specified Purpose: Test Yourself

You should be able to answer YES to the following questions:-

- ✓ Do you specify the purpose for which you are collecting and keeping personal information?
- ✓ Is that purpose lawful?
- ✓ Can you make a precise statement of that purpose?
- ✓ Has the purpose been made known to those for whom, and about whom, you keep personal data?
- ✓ Have you made out a list of the different sets of data which you keep and the specific purpose of each?

Practical steps

Prepare a statement of the purpose or purposes for which you hold information about others. Any individual has the right to ask you to state the purposes for which you keep such information. If you have not already done so, you should also prepare the list referred to in the final question.

Data Protection Rule 3

Duty to Destroy Personal Data

Where the purpose for keeping personal data has lapsed, the data controller must destroy such data as soon as reasonably practicable and notify the data processor holding such data, if any. The data processor, upon receiving the notification, must as soon as reasonably practicable, destroy the data specified by the data controller. Failure to destroy data is an offence.

Data Protection Rule 4

Use and Further Processing of Personal Information

If you obtain personal information for a particular purpose, you may not use the data for any other purpose, and you may not divulge the personal data to a third party, except in ways that are "compatible" with the specified purpose. A key test of compatibility is whether you use and disclose the data in a way in which those who supplied the information would expect it to be used and disclosed.

Note that transmission of personal data to agents of yours, who are carrying out operations upon the data on your behalf and not retaining it for their own purposes, do not

constitute "disclosures" of data for the purposes of the Act. Examples of such transmissions would include the transmissions of staff data to a separate payroll company for payroll administration purposes, and the transmissions of personal data from a general practitioner to a clinical laboratory for analysis of tissue samples. You should also note that, even though such transmissions would not involve "disclosure" of personal data, the data controller might also have to consider whether the data have been "fairly obtained" for these purposes.

The restriction on processing of personal data (including disclosure to a third party) is lifted in a limited number of circumstances, as they are specified in sections 24 and 25 of the Data Protection Act, where the right to privacy must be balanced against other needs of civil society, or where the processing is in the interests of the individual.

Section 29 of the Data Protection Act provides that a data controller shall not further process personal data (which includes disclosure to a third party), except in ways that are compatible with the purpose for which the data were obtained.

However, this non-disclosure rule is not unqualified.

Part VII of the Act on "Exemptions", particularly section 52 qualify this rule.

Section 52 provides that personal data are exempt from the second, third, fourth and fifth data protection principles as elaborated in the First Schedule, sections 23 to 29 and Part VI in respect of blocking personal data where:-

- the disclosure of such data is required under Mauritian law or by a court order;
- the disclosure of such data is necessary for the purpose of, or in connection with, any on-going or prospective legal proceedings;
- the disclosure of such data is necessary for the purpose of obtaining legal advice;
- the disclosure is otherwise necessary for the purpose of establishing , exercising or defending legal rights.

Use and Disclosure: Test Yourself

You should be able to answer YES to the following questions:-

- ✓ Do you use the data only in ways consistent with the purpose or purposes for which they are kept?
- ✓ Do you disclose the data only in ways consistent with that purpose or purposes?

Practical Steps

Carry out an inventory of all current and proposed disclosures and check each one against the stated purposes.

Data Protection Rule 5

Security of Personal Data

The Data Protection Act 2004 does not detail specific security measures that a Data Controller or Data Processor must have in place. Rather, section 27 of the Act places an obligation on a data controller to have appropriate security and organizational measures in place to prevent "unauthorised access to, alteration of, disclosure of, accidental loss, and destruction of the data in his control."

The security of personal information is all-important. It will be more significant in some situations than in others, depending on such matters as confidentiality and sensitivity. High standards of security are, nevertheless, essential for all personal information. Both data controllers and data processors must meet the requirement to keep data secure.

Appropriate security measures

In determining what security measures should be put in place in order to satisfy the requirements of section 27 a number of factors may be taken into consideration, in particular where the processing involves the transmission of data over an information and communication network;

The state of technological development available - Measures must be reviewed over time. Data controllers may also have regard to the **state of technological development**, and the **cost** of implementing security measures.

Comment: *Security measures need to be reviewed on a regular basis to ensure that they are up-to-date and effective. An obvious example is anti-virus software: such software is a routine safeguard to prevent malicious damage to your computers, but needs to be updated regularly if it is to continue to be effective against newly-emerging computer viruses. Likewise, if sensitive files need to be encrypted, then a data controller should ensure that the standard of encryption is sufficiently robust to withstand attacks from newly-developed decryption software.*

On the other hand, it is reasonable for organisations to weigh up the costs of security measures against the other factors. If the risks of security breaches are low, and the likely harm that would arise is trivial or minor, then a data controller might justifiably decide not to invest a great deal of money in state-of-the-art security measures. Conversely, if the risks of security breaches (or attempted breaches) are high, and/or the likely harm to an individual would be high, then a data controller should invest in robust security measures, and indeed should regard such investment as a budget priority.

The cost of implementing the security measures. - Larger organisations with greater resources can be expected to implement more advanced measures, or update measures more regularly, than smaller bodies.

The special risks that exist in the processing of the data. For instance, data controllers may also have regard to the security measures with regard to **transmission** of personal data over a **network**.

Comment: *Transmission involves particular security risks that must be guarded against. Most obviously, there is the danger that the transmission could be intercepted by a third party. Other risks include corruption or loss of the data, or its accidental disclosure to third parties. Each data controller must make its own judgment, based upon its own particular circumstances, about the most suitable security measures to implement. However, in general terms, the transmission of personal data within an internal network, such as a corporate 'intranet', should at minimum be subject to clear access controls, so that the personal data are available only to those people within the organisation who have a business requirement for such access. Transmission over external networks, such as the internet, should normally be subject to robust encryption. This requirement will be of particular relevance to e-commerce businesses which record customer details on-line, e.g. via on-line booking forms. Similarly, telecommunications service providers, which transmit personal data over their networks, must take whatever technical measures are necessary to keep such data secure from unauthorised interception.*

The nature of the data concerned and the harm that might result from the unauthorised access to, alteration, disclosure, accidental loss, destruction of the data in his control.

There is a greater duty of care relating to the processing of sensitive personal data. In deciding what level of security is appropriate, data controllers must have regard to the **nature of the personal data** in question, and the **harm** that might result from unauthorised use, disclosure or loss of the personal data.

Comment: *Organisations dealing with personal data of a private or sensitive nature – such as people's medical files, personnel files, or private telecommunications – naturally need to have very robust standards of security in place. Organisations that hold personal data with a lower privacy value – such as name, address, or membership of a local drama group – do not need to go to such great lengths, but must still have reasonable security measures in place.*

An organisation should take all reasonable steps to ensure that its **staff are made aware** of the security measures, and comply with them.

This requirement may be satisfied by having appropriate training in place.

This requirement may be satisfied by the automatic generation of audit trails or logs, combined with some form of internal audit or review procedure.

Comment: *There is no point in preparing an elaborate security scheme, which works well in theory, if the measures are not applied in practice. data controllers and data processors to take all reasonable steps (i) to develop an appropriate level of staff awareness, and (ii) to ensure compliance by staff with the security measures. This requirement applies for employees, and for other persons at the place of work.*

Dealing with Data Processors

Sometimes, an organisation will need to engage the services of a sub-contractor or agent to process personal data on its behalf. Such an agent is termed a **'data processor'** under the Data Protection Act. An example would be a payroll company, or a telemarketing company retained by a data controller to conduct a customer-satisfaction survey. Where a data controller engages the services of a data processor, it must take certain steps to ensure that data protection standards are maintained. The key points are as follows:

A data controller can do business with a data processor only on the basis of a **written contract** (or a contract in equivalent form) which includes appropriate security and other data protection safeguards. Informal and ad-hoc arrangements will not be acceptable, where personal data are involved.

In particular, the contract must specifically provide that the data processor will process personal data only on the basis of the **authorisation and instructions** received from the data controller. This provision ensures that personal data passed on to a data processor may not be retained or used by the data processor for its own purposes.

The contract must commit the data processor to apply **appropriate security measures**. This provision ensures that the standard of security must be maintained when the personal data are passed from the data controller to its agent.

Finally, at a practical level, the data controller must satisfy itself that the data processor has suitable and sufficient **technical security measures**, and **organisational measures**, in place. The data controller must also take reasonable steps to ensure that these measures are being **complied with**.

Therefore, when a data controller uses a third party to process data, the processing of such data should be covered by contract. This contract should stipulate at least the following:

- the conditions under which data may be processed;
- the minimum security and organisational measures that the data processors must have in place;
- some mechanism or provision that will enable the data controller to ensure that the data processor is compliant with the security requirement (this might include a right of inspection or independent audit).

Access Control

The obligation to prevent unauthorised access to data can, at the simplest level, be met by placing a password onto a computer. This would certainly be the minimum measure acceptable. However, it is only effective if staff keep the password secure, and is reviewed and changed if necessary. A password is one simple form of authentication. A more advanced form is the use of a token (such as a smart card), or the use of biometrics (such as an iris scan or a finger print scan). Where all three are used in combination, this would offer a high level of authentication.

Network administrators can add a level of security beyond mere authentication. Users tend to develop unique profiles, depending on what they normally do on their computers. This can be a combination of the time and frequency of access; location; nature of data accessed. Where a user seeks to access data in an unusual manner, which conflicts with an established profile, a challenge response question can be asked by the system. This type of authentication prevents a person who has found a password from accessing the system.

In conjunction with authentication, the nature of access allowed to an individual user should be set and reviewed on a regular basis. Ideally, users should only have access to data which they require in order to perform their duties. Regular reviews are necessary in order to increase if necessary as well as to restrict previous access where a user role changes.

A logging and reporting system can be a valuable tool in assisting the network administrator in identifying abuses and developing appropriate responses.

Encryption

There are a variety of tools available with which to encrypt data. These can be useful in closed systems, where all users can have access to the key with which to decrypt data. Providing such a key is held securely, encryption offers a high degree of protection against external attack.

Where encryption currently does not work satisfactorily is in sending data to the outside world. For instance, the use of a Public Key Infrastructure (PKI) requires that both sender and recipient use the same encryption system.

Anti-Virus Software

Anti-Virus software is not only required to prevent infection from the internet (either e-mail or web-sourced). Viruses may also be introduced from diskettes or CD's. No anti-virus package will prevent all infections, as they are only updated in response to infections. It is essential that users update such software on a regular basis, but also keep vigilant for potential threats. A policy of not opening e-mail attachments from unexpected sources can be a useful way of preventing infection.

Firewalls

A firewall is useful where there is any external connectivity, either to other networks or to the internet. It is important that firewalls are properly configured, as they are a key weapon in combating unauthorised access attempts. As firewalls are available for free download from the internet, they should routinely be installed by all data controllers and processors. This will become more important as persons progress to "always-on" internet connections, exposing themselves to a greater possibility of attack.

Automatic Screen Savers

Most systems allow for screensavers to activate after a period of inactivity, on the computer. This automatic activation is useful as the alternative manual locking of a

workstation requires positive action by the user every time he/she leaves the computer unattended. Regardless of which method an organisation employs, computers should be locked when unattended. This not only applies to computers in public areas, but to all computers. It is pointless having an access control system in place if unattended computers may be accessed by any staff member.

Logs and Audit trails

It is of course pointless having an access control system and security policy if the system cannot identify any potential abuses. Consequently, a system should be able to identify the user name that accessed a file, as well as the time of the access. A log of alterations made, along with author/editor, should also be created. Not only can this help in the effective administration of the security system, its existence should also act as a deterrent to those staff tempted to abuse the system.

The Human Factor

No matter what technical or physical controls are placed on a system, the most important security measure is to ensure that staff are aware of their responsibilities. Passwords should not be written down and left in convenient places; passwords should not be shared amongst colleagues; unexpected e-mail attachments should not be opened unless first screened by anti-virus software.

Remote Access

Where a worker is allowed to access the network from a remote location (e.g. from home or from an off-site visit), such access is creating a potential weakness in the system. Therefore, the need for such access should be properly assessed and security measures reassessed before remote access is granted.

Wireless networks

Access to a server by means of a wireless connection (such as infrared or radio signals) can expose the network to novel means of attack. The physical environment in which such systems are used may also be a factor in determining any weakness in the system security. As with remote access, wireless networks should be assessed on security grounds rather than solely on apparent ease of use.

Laptops

Laptops, personal organisers and other form of portable computers are especially vulnerable, as there is not only a higher risk of theft, but also a new risk of accidental loss. It would be a sensible precaution not only to have adequate security measures, but also to limit what data are placed on such machines in the first place. If practical, collected data should be downloaded at an early date with administrators reviewing the nature and quantity of data held.

Where laptops are the personal property of an individual, the data controller should have a contract in place to detail the conditions under which data may be processed on personal computers. A contract might also be advisable to cover all employee use of portable computers, especially concerning use of data where a person leaves the employment of a data controller.

Even where data are not routinely deleted from portable computers, such data should be backed up onto the network. This will assist in keeping the data on the network accurate and up to date, as well as defending against the accidental loss or destruction of data on portable computers.

Back-up systems

A back up system is an essential means of recovering from the loss or destruction of data. While some system should be in place, the frequency and nature of back up will depend, amongst other factors, on the organisation concerned and the nature of data being processed. The security standards for back-up data are the same as for live data.

'Back-up data' cannot be part of a live system nor can they be used for any purpose other than replacing lost, destroyed or damaged data.

What constitutes lost, destroyed or damaged data?

Data that are either accidentally, or deliberately, deleted can be considered to be destroyed. Data that can no longer be found may be considered to be lost. Damaged data may result from files being corrupted. However, a draft of a work in progress which is later overwritten is not considered to have been damaged or destroyed unless there is a clear policy of retaining drafts, in which case the draft should not have been overwritten.

What is the purpose of backing-up data?

There is a requirement in the Data Protection Act that adequate measures be taken to prevent the unauthorised destruction or alteration of data. By backing-up data, a data controller/processor is taking steps to recover from such actions. In general, back-ups are most useful in a disaster recovery situation, where there has been a catastrophic system failure resulting in a large scale, if not total loss or corruption of data.

For how long should back-up data be held?

This depends on how long after an event is it likely to be discovered that data have been lost, destroyed or damaged. This time period will depend both on the nature of the data and the nature of the organisation processing the data. For most situations, it would not be reasonable to keep more than a small number (ten or less) back-up tapes. On a daily back-up regime, this would allow for two working weeks in which to discover that data were lost, destroyed or deleted.

Physical Security

Physical security includes issues like perimeter security (office locked and alarmed when not in use); computer location (so that the screen may not be viewed by members of the public); disposal (so that computer print outs containing sensitive data are securely disposed of).

Keeping Personal Data Secure: Test Yourself

As a minimum standard, you should be able to answer YES to the following questions:-

- Is access to your computers and manual files restricted to authorised staff only?
- Is access to the information restricted on a "need-to-know" basis in accordance with a defined policy?
- Are your computer systems password protected?
- Is information on screens kept hidden from callers to your offices?
- Have you a back-up procedure in operation, including off-site back-up?
- Are all waste papers, printouts, etc. disposed of carefully?

Practical steps

Compile a checklist of security measures for your own systems.

Security measures should be suitable to all of the circumstances involved, including the sensitivity of the personal data, the state of technological development, and the cost of implementing the provisions. In addition, where an agent is being retained to process personal data, there should be a sound contractual basis for this, with appropriate security safeguards in place.

Data Protection Rule 6

Accurate and Up-to-date Data

You must take all reasonable steps to ensure that the personal information you keep is accurate and up-to-date. Apart from ensuring compliance with the Act, this requirement has an additional importance in that you may be liable to an individual for damages if you fail to observe the duty of care provision in the Act applying to the handling of personal data.

A data controller upon being informed as to the inaccurateness of personal data by a data subject must rectify, block, erase or destroy the data as appropriate.

Where he is aware that a third party holds inaccurate personal data, he must as soon as reasonably practicable, require the third party to rectify, block, erase or destroy the data as appropriate. Otherwise, this would amount to the commission of an offence.

If the data controller fails to rectify, block, erase or destroy inaccurate personal data, a data subject may apply to the Commissioner to have such data rectified, blocked, erased or destroyed.

Accurate and Up-to-date Data: Test Yourself

You should be able to answer YES to the following questions:-

- ✓ Are your clerical and computer procedures adequate to ensure high levels of data accuracy?
- ✓ Has the general requirement to keep personal data up-to-date been fully examined?
- ✓ Have appropriate procedures been installed to ensure that each data item is kept up-to-date?

Practical steps

Assign specific responsibility for data accuracy under the Data Protection Act and arrange periodic review and audit. Note that the accuracy requirement does not apply to back-up data, that is, to data kept for the purpose of replacing other data in the event of their being lost, destroyed or damaged.

Data Protection Rule 7

Adequate, relevant and not excessive

The personal data you keep should be enough to enable you to achieve your purpose, and no more. You have no business collecting or keeping personal information that you do not need, "just in case" a use can be found for the data in the future. You should not ask intrusive or personal questions, if the information obtained in this way has no bearing on the specified purpose for which you hold personal data.

Adequate, Relevant and Not Excessive Personal Data: Test Yourself

You should be able to answer YES to the following questions:-

- ✓ Is the personal information I hold really necessary for my business?
- ✓ Am I asking people to provide me with just the information I need, and no more?
- ✓ Do I have a good reason for asking people sensitive or personal questions?

Practical steps

- ✓ Decide on specific criteria by which to decide what is adequate, relevant, and not excessive.
- ✓ Apply those criteria to each information item and the purposes for which it is held.

Data Protection Rule 8

Retention of personal data

Nowadays information can be kept cheaply and effectively on computer. This requirement places a responsibility on data controllers to be clear about the length of time for which data will be kept and the reason why the information is being retained. If there is no good reason for retaining personal information, then that information should be routinely deleted. Information should never be kept "just in case" a use can be found for it in the future.

You should pay particular attention to old information about former customers or clients, which might have been necessary to hold in the past for a particular purpose, but which you do not need to hold any longer. If you would like to retain information about customers to help you provide a better service to them in the future, you must obtain the customers' consent in advance. The same applies to paper records. Good housekeeping would also dictate that you regularly review the need to retain records.

Retention of personal data: Test Yourself

You should be able to answer YES to the following questions:-

- ✓ Is there a defined policy on retention periods for all items of personal data kept?
- ✓ Are there clerical and computer procedures in place to implement such a policy?
- ✓ Is information about old customers routinely purged from our systems?

Practical steps

Assign specific responsibility to someone for ensuring that files are regularly purged and that personal information is not retained any longer than necessary.

Data Protection Rule 9

Transfers Abroad

Section 31 of the Data Protection Act 2004 specify the conditions to be met before personal data is transferred to foreign countries.

Organisations that transfer personal data from Mauritius to these countries will need to ensure that the country in question provides an adequate level of data protection. In certain limited circumstances – especially where the individual data subject has clearly given her or his consent – transfers of personal data may take place even if the level of protection to be afforded to the transferred data cannot be guaranteed in law. The narrow scope of these circumstances is spelled out in Section 31 of the Act.

A best practice approach would be for a data controller planning an international data transfer to consider first whether the country provides an adequate level of protection and to satisfy himself or herself that the exported data will be safeguarded in that country. Only if this is truly not practical and/or feasible should the data controller, consider relying on data subject consent or the other derogations provided for in law. This is particularly so in the case of repeated transfers of personal data, especially where the data involved is sensitive.

The rules regarding transfers to foreign countries can be summarised as follows:-

- The general rule is that personal data cannot be transferred without the written authorisation of the Commissioner to foreign countries.
- If the country does not provide an adequate standard of data protection, then the Mauritian data controller must rely on the use of approved contractual provisions or one of the other alternative measures, provided for in Mauritian Law for transfers to be effected.
- The Data Protection Commissioner retains the power to prohibit transfers of personal data to places outside Mauritius, if she considers that data protection rules are likely to be contravened.

More details on each of the above points are given below.

1. Adequate Standard of Data Protection

As mentioned above, personal data cannot be transferred to foreign countries unless the country ensures an adequate level of data protection and with the authorisation of the Commissioner.

The "adequacy" test relates to all of the circumstances surrounding a proposed transfer of personal data, including the nature of the data, the purpose and duration of the transfer, the country of origin and the country of final destination, the laws in force in that country, and any relevant codes of conduct or other rules and security measures in place.

2. The Four Alternative Measures

If a data controller can point to one or more of the following four alternatives, then the transfer of personal data to another country may proceed:

(i) the data subject (i.e. the individual to whom the personal data relates) has given his or her consent to the transfer.

Comment: *If you wish to transfer a database containing records about many individuals to another country, then – in order to rely on this provision – you need to obtain the consent of each one of these individuals before you can transfer their data. In interpreting what is meant by the word 'consent', the Data Protection Commissioner will have regard to the definition of consent in the Act which refers to freely given, specific and informed consent. Data controllers should therefore be extremely cautious about relying on consent as a basis for data transfer since, in practice, demonstrating that such consent is freely given, specific and informed is likely to be problematic.*

(ii) the transfer is necessary for the performance of a contract to which the data subject is party; or the transfer is necessary for the taking of steps – at the request of the data subject – with a view to his or her entering into a contract with the data controller.

(iii) the transfer is necessary to conclude a contract or to perform a contract between the data controller and someone other than the data subject, in cases where the contract is entered into at the request of the data subject, or where the contract is in the interests of the data subject

Comment: *Data controllers should be cautious about relying on provisions (ii) and (iii) since the "necessity" test rules out use of these provisions other than in very specific circumstances. For example, it would not be prudent to rely solely on these provisions for the transfer of employee data within a multinational company.*

(iv) the transfer is necessary in the public interest, to safeguard public security or national security.

Comment: *this basis is only likely to be relevant to public sector data controllers and only in circumstances where they can show that there is a substantial public interest in the transfer of personal data.*

3. Approval of the Data Protection Commissioner

The transfer is authorised by the Data Protection Commissioner where the data controller can point to adequate data protection safeguards, such as approved contractual provisions. In practice, it is likely that most international transfers will be on the basis of model contracts.

In the case of multinational companies, the use of so-called binding corporate rules – legally enforceable privacy/data protection codes of practice – can offer an alternative or complementary mechanism for approved international transfers within the global corporate entity. A company interested in this option should apply for approval of its rules to the data protection authority where its headquarters or main centre of activity, is based.

Data Protection Rule 10

Right of Access to Personal Data

Under section 41 of the Data Protection Act, on making a written request to you, any individual about whom you keep personal information on computer or in a relevant filing system is entitled to:

- a copy of the data upon payment of the prescribed fee (Rs 75),
- whether the data kept by him include personal data relating to the data subject,
- a description of the purposes for which it is held; and

- a description of those to whom the data may be disclosed unless compliance with such a request would be in breach of the confidentiality obligation of the data controller.

You are also obliged to explain to the data subject the logic used in any automated decision making process where the decision significantly affects the individual and the decision is solely based on the automated process. This "right of access" is subject to a limited number of exceptions, which are listed below.

An individual making an access request must:-

- apply to you in writing by filling in the request for access to data form available on the website http://dataprotection.gov.mu or at the Data Protection Office ,
- give any details which might be needed to help you identify him or her and locate all the information you may keep about him/her.
- The individual must also pay you the access fee.

Every individual about whom a data controller keeps personal information on computer or in a relevant filing system, has a number of other rights under the Act, in addition to the Right of Access. These include the right to have any inaccurate information rectified or erased, to have personal data taken off a direct marketing or direct mailing list and the right to complain to the Data Protection Commissioner.

What must YOU do in response to an access request?

- Supply the information to the individual within 28 days of receiving the request. Note that, having received the access request, you cannot change or delete the personal data which you hold just because you do not wish the data subject to see it.
- Provide the information in a form which will be clear to the ordinary person (e.g., any codes must be explained).
- Ensure that you give personal information only to the individual concerned (or someone acting on his or her behalf and with their authority). For instance, you normally would not provide such information by phone.
- If you do not keep any information on computer or in a relevant filing system about the individual making the request you should tell them so within the 28 days.
- The fee must be refunded if you do not comply with the request.

Are There Exceptions or Limitations on the Right of Access to Personal Data?

Yes, there are. Section 43 of the Data Protection Act provides that the right of access does not apply in a number of cases.

The restrictions upon the right of access fall into five groups:

- The obligation to comply with an access request does not apply where the data controller is not supplied with the information he reasonably requires in order to

satisfy himself as to the identity of the person making the request and to locate the information which the person seeks;

- Where compliance with the request would be in contravention of the confidentiality obligation of the data controller under the Mauritian law;
- The right of access does not include a right to see personal data about another individual, without that other person's consent. This is necessary to protect the privacy rights of the other person. Where personal data consists of expressions of opinion about the data subject by another person, the data subject has a right to that expression of opinion except where that expression of opinion was given in confidence;
- Where the data controller cannot comply with the request without disclosing personal data relating to another person, he may refuse the request unless the other individual has consented to the disclosure of his personal data to the person making the request or he obtains the written approval of the Commissioner;
- The right of access does not include information given in confidence to the data controller for the purposes of the education, training or employment, or prospective education, of the data subject, the appointment or prospective appointment of the data subject to any office, the provision or prospective provision by the data subject of any service, the personal data requested consist of information recorded by candidates during an academic, professional or other examination;
- The right of access does not include the revelation of evidence of the commission of a criminal offence other than an offence under the Act.

Data Protection Rule II

Part VII of the DPA – Exempted Forms of Data Processing

(Some Sections of the Data Protection Act Do Not Apply To All Data Controllers. Please consult the Data Protection Act to ascertain which sections do not apply to you.)

1. Crime and Taxation

The processing of personal data for the purposes of the prevention or detection of crime; the apprehension or prosecution of offenders; or the assessment or collection of any tax, duty or any imposition of a similar nature, are exempt from some sections of the Act.

2. National Security

Personal data are exempt from any provision of the Act where the non application of such provision would, in the opinion of the Prime Minister be required for the purpose of safeguarding national security. A certificate under the hand of the Prime Minister certifying that such is the case will be conclusive evidence of that fact.

3. Health and Social Work

A data controller is exempt from the application of section 41 of the Act where the personal data to which access is being sought by data subject refers to the physical or mental health of the data subject or any other person.

4. Regulatory Activities

The processing of personal data for the purpose of discharging any of the relevant functions designed for protecting members of the public against –

- financial loss due to dishonesty, malpractice or other serious improper conduct, or by 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;
- financial loss due to the conduct of discharged or undischarged bankrupts; or
- dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity;

  - conferred on the Bank of Mauritius, the Financial Services Commission and the Financial Intelligence Unit, by the law;
  - for protecting charitable trusts and other bodies involved in charitable work against misconduct or mismanagement in their administration;
  - for protecting the property of charitable trusts and other bodies involved in charitable work from loss or misapplication;
  - for the recovery of the property of charitable trusts and other bodies involved in charitable work;
  - for securing the health, safety and welfare of persons at work;
  - for 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; or
  - designed for protecting members of the public against conduct which adversely affect their interests by persons carrying on a business;
  - designed for regulating agreements or conduct which have as their object or effect the prevention, restriction or distortion of competition in connection with any commercial activity; or regulating conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market;

  will be exempt from some provisions of the Act to the extent that such an application would be likely to prejudice the proper discharge of such functions.

5. Journalism, Literature and Art

The processing of personal data for journalistic, literary and artistic purposes where -

- such processing is undertaken with a view to the publication of any journalistic, literary or artistic material;
- the data controller involved in such processing reasonably believes that the publication would be in the public interest; and
- the data controller reasonably believes that compliance with any such provisions would be incompatible with such purposes,

will be exempt from certain sections of the Act.

6. Research, History and Statistics

Personal data which are processed only for research, historical or statistical purposes will be exempt from certain sections of the Act.

The exemption provided will not be applicable where –

- such personal data are not processed to support measures or decisions with respect to particular individuals; and
- such personal data are not processed in such a way that such processing would substantially damage or substantially distress any data subject or will likely cause such damage or distress.
- the personal data processed for the purposes specified above will also be exempt from the provisions of Part VI where -
- the conditions above are satisfied; and
- the results of the research or any resulting statistics are not made available in a form which identifies any of the data subjects concerned.

7. Information available to the public under the law

Where personal data consists of information which the data controller is obliged under the law to make available to the public, such data will be exempt form certain sections of the Act.

8. Legal Professional Privilege

Personal data are exempt from certain sections of the Act where the data consist of information in respect of which a claim to legal professional privilege or confidentiality as between client and legal practitioner could be maintained in legal proceedings, including prospective legal proceedings.

9. Domestic Purposes

Personal data processed by an individual are exempt from certain sections of the Act where such processing is only for the purposes of that individual's personal, family or household affairs or for recreational purposes

Data Protection Rule 12

The Direct Marketing Sector

Direct marketing is concerned with identifying and meeting people's needs and preferences. The desire for privacy is one preference that is expressed by many people, and direct marketers should ensure that such privacy choices are respected. Direct marketing that is sent to unwilling recipients is not only wasteful, but is also a violation of people's data protection rights.

Dealing with Unsolicited Direct Marketing

The Data Protection Act takes the sending of unsolicited direct marketing ("junk mail" or "spam") very seriously and offers protection against this practice. The application of data protection law varies depending on the medium through which the marketing is delivered. What follows is a summary of the main types of direct marketing and advice on how to deal with them.

Postal marketing

This is the traditional and oldest form of direct marketing for mail received through a person's letter box. To be considered direct marketing, it must be addressed to a named person and must be promoting a product or service. Unaddressed mail put into a letter box or mail addressed to "the occupant", "the resident" or "the householder" does not necessarily involve the use of personal data and consequently data protection legislation may not apply.

If somebody does not want to receive direct marketing, he/she has a right to notify the sender that he/she is objecting to receiving such material. This request must be made in writing and an organisation that fails to respect the stated preference will be in contravention of the Act. If somebody continues to receive marketing after he/she has objected, he/she can make a complaint to the Data Protection Commissioner.

The provisions of the Data Protection Act 2004 apply to all forms of direct marketing which is defined as the communication of any advertising or marketing material which is directed to any particular individual.

The following questions and answers are designed to shed light on some of the more common queries that may crop up from businesses in the direct mail marketing sector:-

Do I Need People's Consent Before Contacting them with Direct Marketing?

As a general rule, people should not receive unsolicited direct marketing of any nature unless they have indicated that they consent, or at least that they do not object, to such uses of their personal data. This general rule does not apply to unaddressed flyers or letters, where there is no use of an individual's personal data. If direct marketing material is being targeted at someone who does not wish to receive it, that in itself is a warning sign that the direct marketing company, and/or the company from which the personal details were sourced, may have deficient data protection procedures in place.

Does Consent Have to be Written, or Can it be Implied?

No, consent does not have to be in writing for direct marketing purposes, and yes, consent can be implied in certain circumstances. When a person gives clear verbal agreement that his personal data can be used for direct marketing purposes, a direct marketer is entitled to rely on that indication of consent. If a person participates in a special promotion, which clearly involves the use of personal data for certain clearly defined direct marketing purposes, participation might be taken as implicit consent by the individual. The essential point is that the direct marketing company should be clear and up-front about the use of people's personal data, and not be underhanded or cavalier about obtaining people's consent.

Rather than give people an opt-out, can I just notify them that their data will be used for direct marketing?

A person intending to use personal data for direct marketing purposes should offer a cost free opt-out facility.

Is an "opt-out" sufficient, or do I need an "opt-in" consent clause?

An "opt-out" box invites a person to indicate (usually by ticking a box) if they object to receiving direct marketing material. Failure by the person to tick the box, it can be argued, may be taken as an indication of their "passive consent" to receive direct marketing material. An "opt-in" box invites a person to indicate if they would like to receive such material; unless they demonstrate "active consent" by ticking the box, their personal data cannot be used for direct marketing purposes.

Provided an "opt-out" box is clearly visible and explicit in its wording, the Data Protection Commissioner will be prepared to accept that the individual has given their "passive consent" by not ticking the box, provided the personal data in question, and the uses to which the data will be put, are not of a sensitive nature. However, the Commissioner advocates the use of positive "opt-in" boxes as a matter of good practice.

Can I make use of personal information obtained in the past for a different purpose?

No - not unless you have got the consent of all of the individuals affected to this use of their personal data. In theory, it may be open to you to contact all of the people on the old database to ask their permission for the new use of their personal data. Realistically, this will

often be impractical, and the personal data which were originally obtained for one purpose just cannot be used for the new purpose. The best advice is that, if you anticipate a future, secondary use of personal data, you should seek the consent of the individuals at the time of collecting their data.

Can I sell a list of personal data for direct marketing?

No - not unless you have got the consent of all of the individuals affected to this use of their personal data.

How do I obtain consent from children for direct marketing?

When dealing with personal data relating to children, the standards of fairness in the obtaining and use of data are much more onerous than when dealing with adults. The apparent consent of minors to the use of their details for direct marketing purposes cannot be relied upon as the standard of "fair collection", and the Commissioner considers that use of minors' personal data cannot be legitimate unless accompanied by the clear consent of the child's parent or guardian.

Can I target direct marketing at people referred by my existing customers?

You should be careful about soliciting your customers to provide the names of friends, who will be targeted by you for direct marketing. Unless an individual has, in their own right, given their clear consent to receive direct marketing, it is difficult to see how your company could meet the "fair collection" requirement of the Data Protection Act. Alternative mechanisms should be found whereby potential customers may be encouraged to contact you directly, before receiving any direct marketing material from you.

Do people have the right to be taken off my company's mailing list?

Yes. Under section 30 of the Data Protection Act, if you are holding personal data for direct marketing purposes, people may write to you requesting that you stop or not to begin using their data for this purpose. You must comply within 28 days, in principle, by erasing the data, unless you still need to retain the data for some purpose other than direct marketing. You are also required under this section to notify the individual concerned, in writing, of any action taken on your side and inform him of the other purposes for which you are processing his personal data.

As a direct marketer, must I register with the Data Protection Commissioner?

If you are a data controller, yes.

Can I put up an advertisement indicating that personal data is or may be for sale but which is in breach of the Act?

No. This constitutes an offer to sell personal data and is an offence.

What are the basic rules?

Residential subscribers phone calls.

A phone call for the purpose of direct marketing may not be made to an individual's phone number if the individual has his/her preference not to receive marketing calls unless the caller has consent to make such a call, such as from an existing business-customer relationship or as a result of the subscriber entering competitions or promotions. An individual who applies or subscribes to or utilises the Service provided by the Mauritius Telecom Limited (MT), may at any time request MT, by notice in writing, to stop the processing of data provided for the purposes of marketing.

A phone call for the purpose of direct marketing may not be made to an individual's phone number if the individual has previously instructed the caller that he/she does not wish to receive such calls.

It is to be noted that the Commissioner has no role to play in situations where somebody signs up to a service (such as ring tones, jokes or games) and later have difficulty in unsubscribing.

Residential subscribers faxes.

A fax for the purpose of direct marketing may not be sent to the line of an individual subscriber unless that individual has previously consented to the receipt of such a communication. The line of the subscriber on which the fax operates must solely be used for domestic/personal purposes. If the line is used (in any part) to run a business, that line will be treated as a business, not a residential line.

Business subscribers phones & faxes

A phone call or fax for the purpose of direct marketing may not be made to a business phone number if that business has its preference not to receive marketing calls unless the caller has consent to make such a call/send such a fax, such as from an existing commercial relationship.

A fax for the purpose of direct marketing may not be made to a business phone number if the business has previously instructed the caller that it does not wish to receive such calls.

Time factor

When a person issues a specific instruction not to be contacted in the future, before that person may complain he/she must give the other party a reasonable time period in which to record that instruction and update calling lists accordingly. This time period is likely to differ from organisation to organisation, depending upon its size, the size of its database, its structure, its resources and whether it uses outsourced call centres.

Electronic Mail

Marketers may send an individual electronic mail for direct marketing purposes where:

An individual has given them consent to do so, or

they have obtained his personal contact details in the course of a sale to him of a product or service, they informed him of their identity, the purpose in collecting his contact details, the persons or categories of persons to whom his personal data may be disclosed and any other information which is necessary so that processing may be fair, and

the direct marketing they are sending is in respect of their similar* products and services only, and

he was given a simple cost-free means of refusing the use of their contact details for direct marketing purposes at the time his details were initially collected, and where he did not initially refuse the use of those details, he was given a similar option at the time of each subsequent communication **(If the individual concerned fails to unsubscribe using the cost-free means provided to him by the direct marketer, he will be deemed to have remained opted-in to the receipt of such electronic mail)**.

Marketers may not send him any electronic mail for direct marketing purposes in the following circumstances:

if he has not given his prior consent to receiving such mail in accordance with the options set out above,

if the identity of the sender has been disguised or concealed or a valid address to which he can send an opt-out request has not been provided, and additionally, where the electronic mail is an email communication, a valid address at which the sender may be contacted has not been provided.

if he has joined a club to which he pays a subscription for text, multimedia or email message services, unless the direct marketing is directly related to a similar* product or service to the subscription club of which he is a member,

*Similar: is defined in the Oxford English Dictionary as like, alike, of the same kind, nature or amount, having a resemblance.

The Data Protection Commissioner expects persons engaged in direct marketing activity to pay close attention to the limitations which this definition sets down. It is the Commissioner's view that the term 'similar products' referred to above is strictly limited and that direct marketing undertaken on that basis must not breach those parameters.

If you wish to discuss any issue surrounding unsolicited commercial communications, you may phone the Commissioner's office. Please read section 30 of the DPA as well.

Data Protection Rule 13

Data Matching

Data matching is an important tool for the detection and deterrence of fraud and other irregularities, for example fraudulent or multiple claims, unreported income or assets, impersonation; verification of information supplied; verification of eligibility, for example for a benefit programme; identification of corruption or mismanagement, for example conflict of interest; unusual payments; excessive withdrawals; construction of comprehensive databases for research purposes; identification of suspects through searching on the basis of the characteristics of potential offenders; improved efficiency, for example in identifying and concentrating on genuine beneficiaries; locating and rectifying discrepancies and errors; cost-effectiveness.

What is the data matching procedure?

It means any procedure whether manually or by means of any electronic or other device, where personal data collected for one or more purposes in respect of 10 or more data subjects are compared with personal data collected for any other purpose in respect of those data subjects where the comparison is for the purpose of producing or verifying data in respect of which it is reasonable to believe that the data may be used , whether immediately or at any subsequent time, for the purpose of taking any adverse action against any of those data subjects.

Under what circumstances can a data controller carry out a data matching procedure?

A data controller cannot carry out a data matching procedure unless the data subject consents to the procedure being carried out and the Commissioner has consented to the procedure being carried out who may impose such conditions as she wishes or is required by law.

What does adverse action mean?

It means any action that may adversely affect the data subject's rights, benefits, privileges, obligations or interests.

In what circumstances may the data controller take any adverse action against the data subject?

A data controller must not take any adverse action against any data subject as a consequence of the carrying out of a data matching procedure unless the data controller serves a notice in writing on the data subject specifying the adverse action it proposes to take and the reasons for so doing and further stating that the data controller has 7 days after the receipt of the notice to say why the adverse action should not be taken.

However, a data controller is not bound under the Act with the requirements of a notice where such compliance will prejudice the investigation into the commission of any offence.

Data Protection Checklist

Assess your own Data Protection Policy

- ✓ Are the individuals whose data you collect aware of your identity?
- ✓ Have you told the data subject what use you make of his/her data?
- ✓ Are the disclosures you make of that data legitimate ones?
- ✓ Do you have appropriate security measures in place?
- ✓ Do you have appropriate procedures in place to ensure that each data item is kept up-to-date?
- ✓ Do you have a defined policy on retention periods for all items of personal data?
- ✓ Do you have a data protection policy in place?
- ✓ Do you have procedures for handling access requests from individuals?
- ✓ Are you clear on whether or not you should be registered?
- ✓ Are your staff appropriately trained in data protection?
- ✓ Do you regularly review and audit the data which you hold and the manner in which they are processed?

CONCLUSION

Main Responsibilities of Data Controllers

Rule 1: Fair collection:

- At the time when we collect information about individuals, are they made aware of the uses for that information?
- Are people made aware of any disclosures of their data to third parties?
- Have we obtained people's consent for any secondary uses of their personal data, which might not be obvious to them?
- Can we describe our data-collection practices as open, transparent and up-front?

Rule 2: Purpose specification

- Are we clear about the purpose (or purposes) for which we keep personal information?
- Are the individuals on our database also clear about this purpose?
- If we are required to register with the Data Protection Commissioner, does our register entry include a proper, comprehensive statement of our purpose? [Remember, if you are using personal data for a purpose not listed on your register entry, you may be committing an offence.]
- Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each?

Rule 3: Duty to destroy personal data

Have we checked whether the purpose for keeping personal data has lapsed?

Have we notified the data processor holding any such data to destroy it?

Rule 4: Use and disclosure of information

Do we ensure that all disclosures of information are made in compliance with the Act?

Are there defined rules about the use and disclosure of information?

Are all staff aware of these rules?

Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.

If we are required to register with the Data Protection Commissioner, does our register entry include a full list of persons to whom we may need to disclose personal data? [Remember, if you disclose personal data to someone not listed on your register entry, you may be committing an offence.]

Rule 5: Security

Is there a list of security provisions in place for each data set?

- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data we keep?
- Are our computers and our databases password-protected, and encrypted if appropriate?
- Are our computers, servers, and files securely locked away from unauthorised people?

Rule 6: Adequate, relevant and not excessive

- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?
- Does a policy exist in this regard?

Rule 7: Accurate and up-to-date

Do we check our data for accuracy?

- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure our databases are kept up-to-date?

Rule 8: Retention time

Is there a clear statement on how long items of information are to be retained?

Are we clear about any legal requirements on us to retain data for a certain period?

Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?

Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

Rule 9: The Right of Access

- Is a named individual responsible for handling access requests?
- Are there clear procedures in place for dealing with such requests?
- Do these procedures guarantee compliance with the Act's requirements?

Rule 10: Transfers Abroad

Are we clear on what are the adequate data protection safeguards which need to be put in place by us before effecting international transfers?

Are we adequately equipped to make provision for model contracts or codes of practice in order to effect international data transfers?

Rule 11: Exemptions

Are we aware of all the exempted forms of data processing?

Rule 12: Direct Marketing

Are we clear on the parameters of direct marketing?

Are we aware of all the procedures to be followed and safeguards that have to be put in place for the protection of the data subject against unsolicited direct marketing?

Rule 13: Data Matching

Are we aware of the circumstances in which adverse action may be taken against the data subject?

Registration

- Are we clear about whether or not we need to be registered with the Data Protection Commissioner?
- If registration is required, is the registration kept up to date? Does the registration accurately reflect our practices for handling personal data?

  [Remember, if your data-handling practices are out of line with the details set out in your register entry, you may be committing an offence.]
- Is a named individual responsible for meeting our registration requirements?

Training & Education

- Do we know about the levels of awareness of data protection in our organisation?
- Are our staff aware of their data protection responsibilities - including the need for confidentiality?
- Is data protection included as part of the training programme for our staff?

Co-ordination and Compliance

- Has a data protection co-ordinator and compliance person been appointed?
- Are all staff aware of his or her role?
- Are there mechanisms in place for formal review by the co-ordinator of data protection activities within our organisation?

How to organize yourself to ensure the protection of data within your organisation?

The right of access is the most important right that an individual has and you need to organise yourself for handling access requests. Dealing with access requests is not your only obligation. Staff should also be made aware of the obligations imposed by the Data Protection Act. To comply you should:

Ensure that the basic principles of data protection are explained to staff;

Ensure that there are regular updates to guidance material and staff training and awareness, so that data protection is a "living" process aligned to the way the organisation conducts its business;

Document procedures, for example with regard to accuracy and have regular security reviews;

Allocate responsibility for compliance and set-out what in-house sanctions may be imposed if correct procedures are not followed;

Set out the circumstances in which personal data may be disclosed to third parties.

Obligations on retention and security need to be addressed

Adhere to the 'need to know principle' – only personal data necessary for the purpose should be collected and staff should only be able to access the personal data that they need to carry out their functions;

Have adequate access controls, firewalls and virus protection and do not forget manual files;

There should be retention policies for the various categories of data.

The organisation should provide for:-

Periodic audit checks and reviews;

A procedure for complaints handling;

Plans for remedial steps if things go wrong;

Privacy /Data Protection Statements on Forms and Websites and an internal e-mail and internet use policy.

Dealing with Subject Access Requests

The key right for the individual is the right of access. Essentially this means that you have to supply to the individual the personal data that you hold if a valid request is made under Section 41. The time limit for complying with an access request is 28 days. In order to ensure your compliance with the time limit and your other access obligations the following organisational and procedural steps may be effected:

1. Appoint a Co-ordinator or a Data Protection Officer who will be responsible for the response to the access request. A description of the functions and responsibilities of the Co-ordinator should be circulated within the organisation and staff should be advised of the necessity for co-operation with the Co-ordinator.
2. All subject access matters should be submitted to the Co-ordinator.
3. Check the validity of the access request. Ensure that it is in writing, that the appropriate fee is included.
4. Check that sufficient material has been supplied to definitively identify the individual. This is most important as a third party may provide false material to lodge a false access request.
5. Check that sufficient information to locate the data has been supplied. If it is not clear what kind of data is being requested you should ask the data subject for more information. This could involve identifying the databases, locations or files to be searched or giving a description of the interactions the individual has had with the organisation.
6. Log the date of receipt of the valid request.
7. Keep note of all steps taken to locate and collate data – if different divisions of the organisation are involved, have the steps "signed off" by the appropriate person.
8. Check each item of data to establish whether any of the restrictions on or denial of access provided by section 43 will apply.
9. If data relating to a third party is involved, do not disclose without the consent of the third party such data. An opinion given by a third party may be disclosed unless it is an opinion which was given in confidence on the clear understanding that it would be treated as confidential.

10. Monitor process of responding to the request – observing time limit of 28 days.

11. Supply the data in an intelligible form (include an explanation of terms if necessary). Also provide description of purposes, discloses and source of data (unless revealing the source would be contrary to the public interest). Number the documents supplied. Have the response "signed-off" by an appropriate person.

12. Regularly review your procedures and processes.

Self Regulation and Codes of Practice

The requirements of data protection law are quite clear, and applying the rules and principles of data protection to your business activities is often a matter of common sense. However, for some businesses and professions, interpreting and applying data protection law is not so straightforward, and sometimes requires a fine appreciation of the ethical norms and standards, and the traditional expectations of good practice, associated with that sector. For that reason, Section 56 of the Data Protection Act 2004 provides that the Commissioner may approve codes of practice elaborated by data controllers which should have a direct input into the establishment of data protection standards within their sector.

It is a matter for the data controller to devise a code of practice that is appropriate to his sector. If the Commissioner agrees that the code provides adequate data protection for individuals, then the code of practice may be approved by her and incorporated through regulations to be enacted under the Act. The code will then have the force of law, and will be binding upon all data controllers in that sector.

The Commissioner will keep a register of approved codes and guidelines which will be available for public inspection. Upon the payment of the prescribed fee, provide copies or extracts from the register.

How can the Data Controller initiate a statutory Code of Practice?

If you would like to initiate a code of practice, to clarify how data protection rules are to be applied for your sector, then we suggest that you contact the Data Protection Commissioner, with a view to arranging discussions to progress the matter. The Commissioner will be glad to provide you with practical advice on what should be covered in your code of practice, and on how circumstances specific to your sector might be handled.

Designed and Printed by the Government Printing Department - March 2010