Presentation at Ministry of Social Security, National Solidarity and Reform Institutions

BY THE DATA PROTECTION OFFICE

Presenters : Mrs Dodah Pravina
Mr Bhugowon Hemrajsingh

Date : 21.05.13

Aims

- Understand the data protection law in Mauritius
- Recommendations
- Data transfer
- Data Security / Safeguards

Data Protection Act

AN ACT

To provide for the protection of the privacy rights of individuals in view of the developments in the techniques used to capture, transmit, manipulate, record or store data relating to individuals

Some useful definitions

- ✓ **What is data?**

  "data" means information in a form which –

(a) (i) is capable of being processed by means of equipment operating automatically in response to instructions given for that purpose; and

(ii) is recorded with the intent of it being processed by such equipment; or

(b) is recorded as part of a relevant filing system or intended to be part of a relevant filing system;

Some useful definitions

- ✓ **What is personal data ?**
- ● **"personal data" means –**

(a) data which relate to an individual who can be identified from those data; or

(b) data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion;

Some useful definitions - ctd

- ✓ **What does sensitive personal data mean?**

It means personal information of a data subject which consists of information as to his/her -

- **racial or ethnic origin;**
- **political opinion or adherence;**
- **religious belief or other belief of a similar nature;**
- **membership to a trade union;**
- **physical or mental health;**
- **sexual preferences or practices;**
- **the commission or alleged commission of an offence; or**
- **any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.**

Unit	Examples
HR Section	date of birth ;National Identity Number; professional and academic qualifications; bank ac number of all officers
Social Security (National Pensions; Social Aid.)	Name; date of birth ;National Identity Number; residential addresses; bank ac number; medical certificates; marriage certificate of claimants and dependents.
Social Security (Medical Unit)	Name; date of birth;National Identity Number; medical evidence of persons calling on Medical Tribunals and boards.
Finance Section	Name; salary drawn; date of birth ;National Identity Number;bank ac number of all officers
Disability Empowerment Unit	Name; date of birth ;National Identity Number; medical history of disabled persons.

8 Data Protection Principles

- **Personal data shall be processed fairly and lawfully.**
- **Personal data shall be obtained only for any specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose.**
- **Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed**
- **Personal data shall be accurate and, where necessary, kept up to date.**
- **Personal data processed for any purpose shall not be kept longer than is necessary for that purpose or those purposes.**

8 Data Protection Principles, Cont.

- **Personal data shall be processed in accordance with the rights of the data subjects under the Data Protection Act.**
- **Appropriate security and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**
- **Personal data shall not be transferred to another country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.**

- Under the Data Protection Act, **all Ministries, Government Departments and Institutions** have the legal responsibility to implement systems and procedures which will ensure that personal data in their possession is kept safe and secure and in line with the 8 principles of data protection

General Procedures

It is important that each department

- knows what data is held
- where it is held
- knows the purpose of keeping the data
- and what the consequences would be should that data be lost/stolen/misused

How it can be achieved?

- Conduct an audit identifying the types of personal data held within each department, the repositories holding personal data and their location.
- Include the risks associated with the storage, handling and protection of this data in the Department’s risk register.
- Departments can then establish whether the security measures in place are appropriate and proportionate to the data being held

How it can be achieved? - ctd

Access control

- Implement adequate access control mechanisms to protect personal data.

Ideally, users should only have access to data ,which they require in order to perform their duties.

- Examples:
- Passwords to access PC’s ,applications, databases
- Authorisation required when accessing certain files.
- For sensitive data, it is recommended to use multi-level access control, i.e, access is permitted by users with different security clearances

How it can be achieved? - ctd

Implement security measures:

– Computers and databases are password-protected, and encrypted if appropriate. E.g a PC is subject to a password-protected lock-out after a period of inactivity

– Computers, servers, and files are securely locked away from unauthorised people.

– Physical security measures like perimeter security (office locked) are implemented

How it can be achieved? - ctd

- A log book to monitor photocopies of documents / faxes

- In cases where personal data is held on applications and databases, additional measures should be considered to control such data from being copied to external drives, excel sheet formats where no security is in place.

How it can be achieved? - ctd

- Personal, private, sensitive or confidential data should not be stored on portable devices. In cases where this is unavoidable, all devices containing this type of data must be encrypted.

- Internal audits conducted or procedures reviewed on a regular basis to ensure that the security measures in place are up-to-date and effective, e.g. up-to-date antivirus software

How it can be achieved? - ctd

Develop procedures / measures to:

(a) ensure that all disclosures of information are made in compliance with the Act.

(b) ensure that there are defined rules about the use and disclosure of information.

(c) Consider whether the express consent of the individuals should be obtained for these uses and disclosures.

Data Transfer

- Data Transfer should, where possible, only take place via secure on-line channels where the data is encrypted.

- When a data transfer with a third party is required (including to/from other Government Departments), a written agreement (memorandum of understanding) should be put in place between both parties in advance of any data transfer

Data Transfer - ctd

- In order to strengthen data sharing agreements, data sharing protocols can be developed covering:

- The purpose, objectives and scope of the data sharing
- Principles and relevant legislative powers
- Partner undertakings, risk management/indemnity
- DPA compliance (including information security)

Human factor - Training

- It is very important that senior management in departments are aware of the Data Protection Act and its guidelines

- This awareness must also be brought to the attention of all staffs whose work involves handling personal data

Complaint Handling at DPO

- One amongst the functions of the Data Protection Office, is investigation on complaints.

- Any individual or organisation who feels that their privacy rights with regard to their personal data have been infringed can make a complaint to the Data Protection Office

Basic Data Protection Checklist

- 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?

Basic Data Protection Checklist - ctd

- 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?

Publications by DPO

- Data Protection Audit Questionnaire
- Self Assessment Questionnaire
- Guidelines

Available for consultation on our website http://dataprotection.gov.mu

Data Security

Strategies

Appropriate security safeguards and measures for personal information need to be considered by entities across a range of areas. This could include taking steps and implementing strategies to manage the following issues:

- IT security
- Data breaches
- Physical security
- Workplace policies
- Communications security
- Standards

IT security

- Protecting both computer hardware (the physical devices that make up a computer system) and the data that the computer hardware holds from unauthorised use, access, theft or damage.
- Whitelisting describes listing entities, content or applications that are allowed to run on a computer or network. This allows only designated applications to run on a device.

Software Security

- Software security Are the latest versions of software and applications in use?
- What processes are in place to ensure that patches (software that is used to correct a problem with a Software program or a computer system) and security updates to applications and operating systems are installed as they become available?
- Is the anti-virus software up to date?
- Has the operating system been fully patched?

Data Breach

- Procedures and clear lines of authority can assist entities to contain the breach and manage their responses. Ensuring that staff are aware of the plan and understand the importance of reporting breaches is essential for the plan to be effective.
- Is staff educated about the plan and how to respond to data breaches?
- Does the plan enable staff to identify data breaches and require that breaches be reported?
- Does the plan establish clear lines of command and indicate responsible officers? Does the plan outline clearly when affected individuals should be notified of breaches?
- Does the plan include a strategy to identify and address any weaknesses and data handling/data security that contributed to the breach?

Physical security

- Physical security is an important part of ensuring that personal information is not inappropriately accessed
- What measures are used to control access to the workplace?
- Are security and alarm systems used to control entry to the workplace?
- Has privacy and security been considered when designing the workspace?
- On what basis is access to physical files granted?

Workplace Policies

- Privacy protections have the best chance of being effective if they are integrated into workplace policies. Policies should be regularly monitored and reviewed to ensure that they are effective.
- Are all staff, including short term staff and contractors, able to access the policy easily?
- Is there a conflict of interest policy in place that instructs staff members on how to proceed if they handle personal information relating to a person known to them?
- Are new staff members educated how to handle personal data ?
- Is confidential business information segregated from personal user information?

Communications Security

- Personal information can be vulnerable to being improperly accessed or disclosed when it is transmitted. For example, personal information may be disclosed if it is left on a fax machine or printer or discussed over the telephone in an open office.

  -Are there procedures governing the transmission of personal information via fax or email?

  -Are there procedures governing the transmission of personal information to offsite work locations?

  -Does the entity employ encryption when communicating sensitive personal information?

Standards

- ISO 27001:2005 ISMS

  ISMS : Information Security Management System

- The Mauritius Standards Bureau which has been set up under the Mauritius Standards Bureau Act 1993 is responsible for standardization, quality assurance, testing and metrology. MSB operates a certification marking scheme for products and a national management system certification scheme (ISO 9001, ISO 14001, ISO 27001, ISO 22000, HACCP).

Standards

- **MS ISO/IEC 27001 - The Information Security Management System (ISMS)**

  This standard was adopted to address the topic of information security management. The ISMS provides a framework to initiate, implement, maintain and manage information security within any organisation.

- **MS ISO/IEC 27002 - Code of Practice for Information Security Management**

  This is a standard code of practice which contains guidelines to be followed to set up and implement the ISMS. It can be regarded as a comprehensive catalogue of good security things to do.

Questions and Answers