Data Protection Fundamentals

SENSITISATION AT FROID DES MASCAREIGNES

By : Mr. BHUGOWON Hemrajsingh
Mr. DOOKEE Padaruth

Date : 16 Jan 2013

Agenda

1. Data Protection Act
2. The Data Protection Office
3. Data Protection Act – Legal Requirements
4. Froid des Mascareignes
5. Guidelines
6. Technical Requirements
7. Questions and Answers

1. DATA PROTECTION ACT

Data Protection Act 2004

The Data Protection Act 2004 (DPA) gives individuals the right to know what information is held about them.

It provides a framework to ensure that personal information is handled properly.

INDIVIDUALS SHOULD HAVE CONTROL OVER THEIR PERSONAL DATA.

2. THE DATA PROTECTION OFFICE

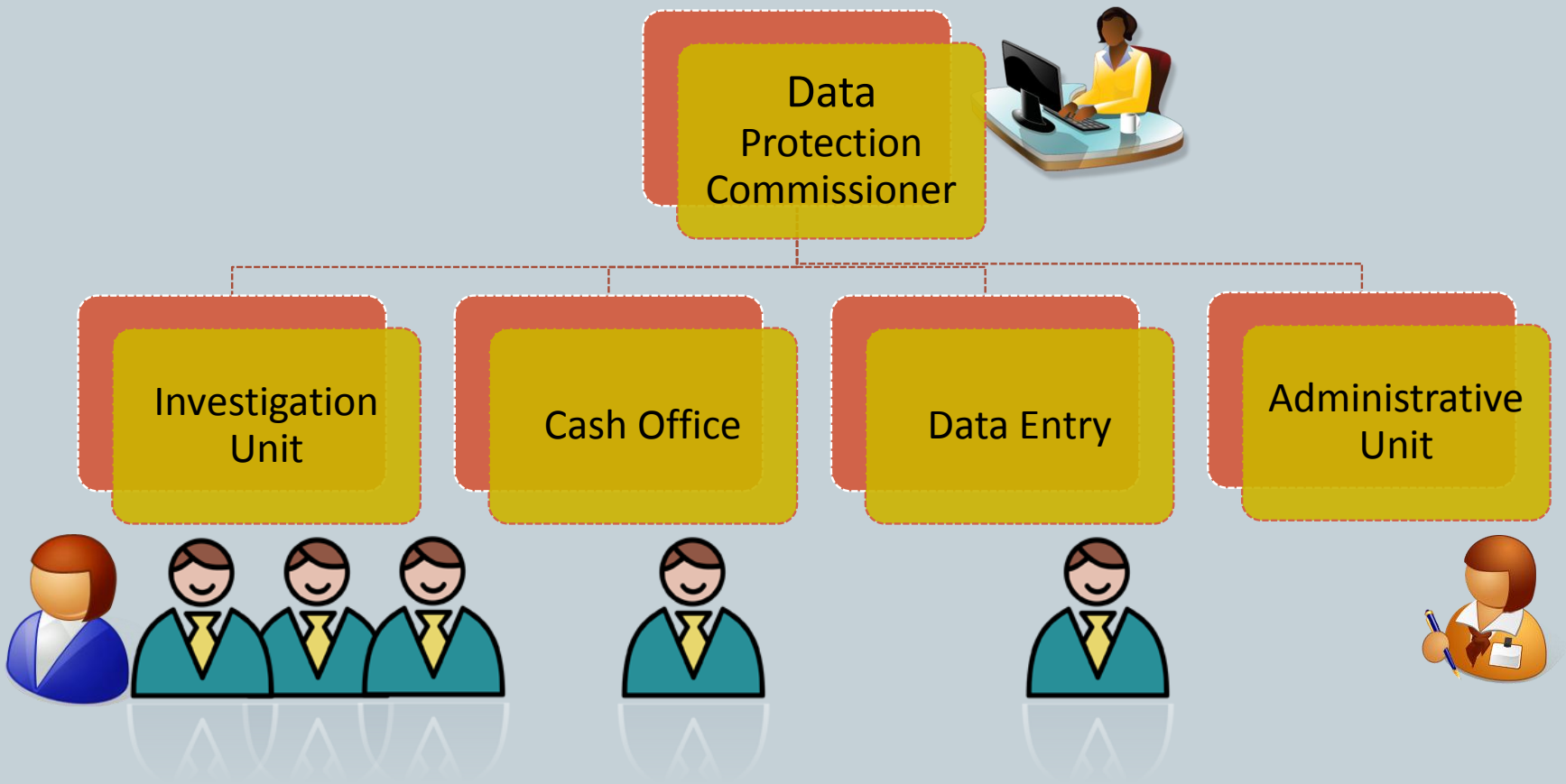
THE DATA PROTECTION OFFICE

The DPO, under the aegis of the Prime Minister's Office, enforces the Data Protection Act

Mission of DPO:

Safeguard the privacy rights of all individuals with regard to the processing of their personal data.

The Data Protection Office



Amongst the Functions of the DPO

- Register all data controllers and data processors in Mauritius
- Investigate complaints w.r.t data protection incidents
- Conduct security checks & data protection compliance audits
- Exercise control on all data protection issues
- Research on data processing & computer technology
- Sensitise the public on their rights and obligations, and the mission of the Data Protection Office

3. Data Protection Act – Legal Requirements

Legal Requirements

What is Personal Data?

Who is a Data Controller?

The 8 Principles of Data Protection

What is Personal Data?

- Definition

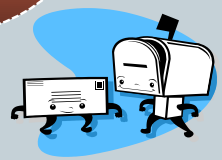
  Data which relate to an individual who can be identified from those data

- Can be on paper, on an IT system, on a CCTV system, etc.

What is Personal Data? – cont'd.

2 types of personal data:

General



- Religious / Similar Belief
- Membership to Trade Union
- Physical / Mental Health
- Political Opinion / Adherence
- Sexual Preferences / Practices
- Racial/Ethnic Origin
- Criminal Convictions

Sensitive

What is Personal Data? – cont'd.

- **What does 'processing' personal data mean?**

"processing" means any operation or set of operations which is performed on the data wholly or partly by automatic means, or otherwise than by automatic means, and includes –

- **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;**

Who is a Data Controller?

An individual or an organisation (either public or private), who decides as to how personal data is to be collected and used.

All Data Controllers are required to register themselves with the Data Protection Office.

It is an offence not to register as a data controller, the penalty of which is a fine not exceeding Rs 100,000 and imprisonment not exceeding 2 years.

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

8 Data Protection Principles – cont'd.

- Personal data processed for any purpose shall not be kept longer than is necessary for that purpose(s)
- Personal data shall be processed in accordance with the rights of the data subjects under this 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

4. FROID DES MASCAREIGNES

FDM

Understand the legal implications of FDM as a data controller:

- Register with DPO
- Educate staff about DPA
- Policies and guidelines within organisation for processing of personal / sensitive and confidential data
- Implement appropriate safeguards
- Apply 8 Principles of DPA

5. GUIDELINES

Guidelines

1). To develop clear procedures on fair collection of data

Make people aware of :

(a) the use of the information being collected, at the time of data collection itself

(b) any disclosure of their data to third parties.

Obtain people's consent for any secondary uses of their personal data, which might not be obvious to them.

Guidelines – cont'd

How ???

- Amend/ design application forms with data protection clauses. E.g:

- All personal data will be processed by …….. in accordance with the Data Protection Act 2004
- This data will be used by …… for … purposes.
- I agree/disagree that……. processes my personal data in the way described above

Guidelines – cont'd

2). To clearly identify the purpose of keeping personal data within the organisation

Assign responsibility to officer(s) for maintaining a list of all data sets and the purpose associated with keeping each data set of personal information

e.g - tax number of employees for calculating taxes

- educational qualifications for career progress

Guidelines – cont'd

3). How to use and disclose information

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) ensure that all staff are aware of these rules.

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

Guidelines – cont'd

4). Ensure Security

Implement a list of security provisions in place in each department to ensure that:

(a) Computers and databases are password-protected, and encrypted if appropriate. E.g PC workstation to be subject to password-protected lock-out after period of inactivity, a firewall to protect systems connected to the internet. For sensitive data, it is recommended to use additional safeguards such as routine encryption of files.

Guidelines – cont'd

(b) Computers, servers, and files are securely locked away from unauthorised people.

(c) 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

Guidelines – cont'd

(d) Access control are put in place and reviewed to control access to data. Ideally, users should only have access to data which they require in order to perform their duties. For sensitive data, it is recommended to use multi-level access control.

(e) Procedures developed so that access to personal information is restricted on a "need-to-know" basis in accordance with a defined policy governing data protection aspects. E.g authorisation required when accessing certain files.

(f) Physical security measures like perimeter security (office locked) are implemented.

Guidelines – cont'd

5). Maintain accurate and up-to-date data

(a) Implement policies to ensure that data is accurate and up-to-date and not excessive to the purpose being collected. E.g existing database should be updated periodically with changes in address, marital status,etc)

Guidelines – cont'd

6). Develop procedures for right of access to personal data

(a) Assign responsibility to officer(s) to handle access requests to personal information. Essentially this means that you as data controller have to supply to the individual the personal data that you hold if a valid request is made to you under Section 41 of the DPA.

6. TECHNICAL REQUIREMENTS

Threats to Data Privacy

- Identity Theft
- Data Breach

Identity Theft

- Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

Data Breach

- A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

Frauds

- **Credit card fraud**

  They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report.

  They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

- **Phone or utilities fraud**

  They may open a new phone or wireless account in your name, or run up charges on your existing account.

  They may use your name to get utility services like electricity, heating, or cable TV.

- **Bank/finance fraud**

  They may create counterfeit cheques using your name or account number.

  They may open a bank account in your name and write bad cheques.

  They may clone your ATM or debit card and make electronic withdrawals your name, draining your accounts.

  They may take out a loan in your name.

Frauds

- **Government documents fraud**

  They may get a driver's license or official ID card issued in your name but with their picture.

  They may use your name and Social Security number to get government benefits.

  They may file a fraudulent tax return using your information.

- **Other frauds**

  They may get a job using your Social Security number.

  They may rent a house or get medical services using your name.

  They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

How do thieves do that ?

- **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
- **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
- **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
- **Changing Your Address.** They divert your billing statements to another location by completing a change of address form.
- **Old-Fashioned Stealing**. They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
- **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources. For more information about pretexting.

Phishing


HSBC
HSBC Bank plc
Customer ID : 000-5432-654386-PSI
Dear Valued HSBC Customer
This e-mail is to inform you that your account will be suspended within 48 hours due to your Account Inactivity. You will have to confirm certain Account Information in order to continue your account subscription :
https://Securityalert.HSBC.co.uk/12/
HSBC Bank Plc
Security Advisor
HSBC Bank PLC
Please do not reply to this e-mail. Mail sent to this address cannot be answered.
For assistance, log in to your HSBC Online Bank account and choose the "Help" link on any page.
HSBC Email ID # 1009

Physical Safeguards

- Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from unauthorized intrusion
- Locked doors and filling cabinet, Security Guards, Surveillance cameras, Alarm System and others.

Technical Safeguards

- Install and use antivirus
- Keep your system patched (updated)
- See well when opening attachment in email
- Install and use firewall
- Make back up of important files and folders
- Use strong password
- Use care when downloading and install free software from the internet. Recommended to use licensed software.
- Install and use file encryption program

Security for Laptop

- Choose a secure operating system and lock it down
- No place is safe so extra vigilance becomes important
- Use strong password
- Use a personal firewall on your laptop
- Use tracking software to have your laptop call home
- Disable the Infrared Port on you laptop

Security over Laptop

- Backup your data
- Record details of equipment serial numbers/identification marks.
- Details need to be readily available in the event of theft
- Beware of email attachments
- Use encryption
- When laptop lost or stolen all these details goes along:
  - Personal details
  - Phone number
  - Credit card numbers
  - Bank details
  - Medical details

Internet Security

- An **Anti-virus** is a software program which helps protect a computer against being infected by a virus
- A **Firewalls** is a system that secures a network, shielding it from access by unauthorized users. Firewalls can be implemented in software or hardware.
- An **Anti-spyware** is a software program which helps protect a computer against the form of Malware. Spyware is one of the most common forms of malware, and often slows the performance of your computer.

Surveillance Camera Systems

- Proper Signage
  - Alert
  - Purpose
  - Name and contact of operator
- Public should be well aware of the presence of the cameras
- Cameras should be focussed and positioned at authorised premises only
- Capturing images outside authorised perimeter constitute an offence under the law

Internet Use and Email Policy

- **Internet usage policy and email policy**
- For many businesses, an internet usage policy and email policy have become increasingly important over recent years.
- In practical terms, the internet use policy and email policy aim to ensure that employees make the most effective use of the internet – but without wasting time on personal chat, social networking and so on. Your internet use policy should include steps to minimise security risks, for example by only allowing authorised employees to download and install software.
- At the same time, your email and internet usage policies should address potential legal risks. Your policies should help ensure that employees do not abuse other people's copyright or use email to harass or defame anyone, including work colleagues. You should aim to ensure that employees understand the potential contractual implications of email and internet use (eg online purchasing) and are aware of any restrictions you impose.

Email disclaimers

- Disclaimer Notice: This e-mail message (including any attachments) is intended for the addressee only, and may contain confidential information. The unauthorised use, disclosure or copying of this e-mail or any information contained within it is strictly prohibited. If you are not the intended recipient, please notify the author and delete this e-mail (including any attachments) immediately in its entirety. This e-mail message has been swept by a virus checker for the presence of known computer viruses. Besides, any opinion or other information in this email (including any attachments) that does not have anything to do with the official business of the **(…)**, is personal to the author, and therefore does not engage any liability whatsoever of the **(…)**, . The above statement does not constitute an acceptance of liability on the part of the (**(…) ,**or its employees in the event of technical or virus issues generated by this e-mail. It is the responsibility of the recipient to take adequate security measures. Further, the **(…) ,**or its employees do not accept liability however arising, including liability for negligence, for any loss resulting from the use of or reliance upon the information contained in the email (including any attachments) and/or reliance or its availability at any time. The recipient must also verify/check any information with the relevant **(…)** and/or other source(s), and to obtain any appropriate professional advice before acting on the contents of this email (including any attachments).

Guidelines by DPO

- Vol. 1 - A Practical Guide for Data Controllers and Data Proccessors
- Vol. 2 - Registration Classification & Guidance Notes for Application
- Vol. 3 - Data Protection - Your Rights
- Vol. 4 - Guidelines for Handling Privacy Breaches

  Part I - Valuable steps for Organisations to circumvent and cure Privacy Breaches

  Part II - Privacy Breach Checklist
- Vol. 5 - Guidelines to regulate The Processing of Personal Data by Video Surveillance Systems Vol. 6 - Guidelines on Privacy Impact Assessments
- Vol. 8 - " Online Behavioural Advertising, Search Engines and Social Networking Sites : What is the connection?"
- Vol. 9 - Practical Notes on Data Sharing Good Practices for the Public and Private Sector

Contact Us

DATA PROTECTION OFFICE

4th Floor, Emmanuel Anquetil Building,

Port Louis

Telephone: 201 3962, 201 2182

Website: http://dataprotection.gov.mu

Email: pmo-dpo@mail.gov.mu

Questions ?