



# TRAINING ON DATA PROTECTION

**Presented by:**

- 1) Mrs Jasbir Haulkhory (DPO/SDPO)**
- 2) Mr Vivekanand Bantoo (DPO/SDPO)**

**Date: Thursday 17 August 2017**

**Venue: Emtel, Ebene**

# Today's Overview

**1**

- Familiarize yourself with the Data Protection Act

**2**

- Understand some key definitions

**3**

- Be aware of the Data Protection Principles

**4**

- Privacy Impact Assessment (PIA)

**5**

- Smart Device Apps

**6**

- Disclosure of information

**7**

- Data Sharing

**8**

- Data Security

**9**

- Best Practices

**10**

- Case Study

# Contact Us

**Website:** <http://dataprotection.govmu.org>

**Email:** [pmo-dpo@govmu.org](mailto:pmo-dpo@govmu.org)

**Telephone:** 4600253

**Address:**

**5th Floor, Sicom Tower, Wall Street, Ebene**

# DATA PROTECTION ACT (DPA)



# THE ACT IN A NUTSHELL

## PART I

- PRELIMINARY - Definitions etc.

## PART II

- DATA PROTECTION OFFICE

## PART III

- POWERS OF COMMISSIONER

## PART IV

- OBLIGATION ON DATA CONTROLLERS : S22 – S32

## PART V

- THE DATA PROTECTION REGISTER : S33 – S40

## PART VI

- RIGHTS OF DATA SUBJECT : S41 – S44

## PART VII

- EXEMPTIONS: S45 – S54

## PART VIII

- MISCELLANEOUS



# 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.



# DEFINITIONS

**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;



## DEFINITIONS (Cont.)

**Personal Data means –**

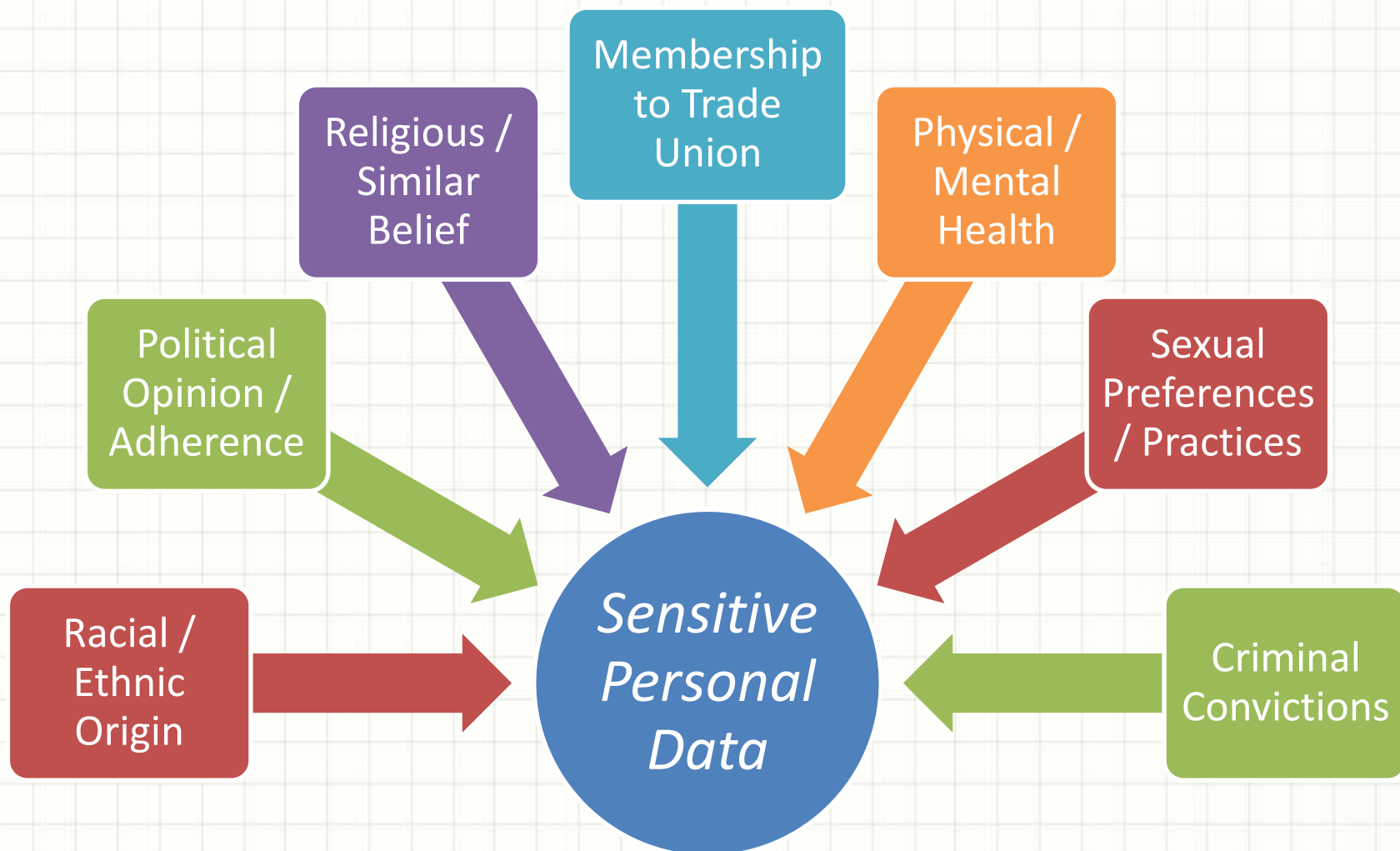
- a) data which relate to an individual who can be identified from those data;**
- a) data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion;**

# EXAMPLES OF PERSONAL DATA

- ❖ Name of individual
- ❖ Address
- ❖ Car Registration No.
- ❖ Telephone No.
- ❖ Bank Account No.
- ❖ Email

# DEFINITIONS (Cont.)

## Sensitive Personal Data



## DEFINITIONS (Cont.)

**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;

# 8 PRINCIPLES OF DATA PROTECTION ACT





# DATA PROTECTION PRINCIPLES

## First Principle

**Personal data shall be processed fairly and lawfully.**

# DATA PROTECTION PRINCIPLES

## *Practical Steps*

For example, if an organisation is collecting personal data using application forms, the organisation is advised to explain the purposes/uses etc. on such forms such as:

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

# DATA PROTECTION PRINCIPLES

## Second Principle

**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.**

# DATA PROTECTION PRINCIPLES

## *Practical Steps*

Prepare a statement of the purpose/purposes for which the organisation holds information about others.

### Remember:

Any individual has the right to ask the organisation to state the purpose/s for which such information is kept.

# DATA PROTECTION PRINCIPLES

## Third Principle

**Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.**



# DATA PROTECTION PRINCIPLES

## *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 PRINCIPLES

## Fourth Principle

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

# DATA PROTECTION PRINCIPLES

## *Practical Steps*

Assign specific responsibility for data accuracy under the Data Protection Act and arrange periodic review and audit.

# DATA PROTECTION PRINCIPLES

## Fifth Principle

**Personal data processed for any purpose shall not be kept longer than is necessary for that purpose or those purposes.**

# DATA PROTECTION PRINCIPLES

## *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 PRINCIPLES

## Sixth Principle

**Personal data shall be processed in accordance with the rights of the data subjects under this Act.**

# DATA PROTECTION PRINCIPLES

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

- a copy of his/her 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;

# DATA PROTECTION PRINCIPLES

## Seventh Principle

**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.**

# DATA PROTECTION PRINCIPLES

## *Practical Steps*

Compile a checklist of security measures for your own systems.

In addition, where an agent is being retained to process personal data on behalf of the organisation, there should be a sound contractual basis for this, with appropriate security safeguards in place.

# DATA PROTECTION PRINCIPLES

## Eighth Principle

**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.**



# DATA PROTECTION PRINCIPLES

- Authorisation is required from the Data Protection Commissioner to transfer data abroad.
- Organisation must fill and submit to this office the 'Transfer of Personal Data Form' available on <http://dataprotection.govmu.org>



# PRIVACY IMPACT ASSESSMENT (PIA)

## *PIA Tool or Questionnaire*

- Privacy Assessment is seen as a valuable tool for businesses & governments.
- This application will enable public and private bodies to make informed choices.
- It will often be the case that a privacy enhancing solution will be no more difficult or more costly to implement than an intrusive one, if the option is identified sufficiently.
- However, this should not be the motivation since we are dealing with the human right to privacy.

# PRIVACY IMPACT ASSESSMENT (PIA)

## *Privacy Assessment*

- Protection of privacy is more than simply avoiding a breach of the law. It involves striving for something better.
- Privacy Impact Assessments & Privacy Compliance Assessments are new techniques which are increasingly being used internationally to better manage privacy risks.

# PRIVACY IMPACT ASSESSMENT (PIA)

## *Privacy Assessment (Cont.)*

- Others include audits, privacy seals and associated self-regulatory initiatives and privacy enhancing technologies.
- Each builds on the bedrock of the enforceable privacy rights for citizens and consumers enshrined in law.

# PRIVACY IMPACT ASSESSMENT (PIA)

## *Privacy Assessment (Cont.)*

- These assessments are being encouraged as a means by which business and government can proactively identify and avoid privacy problems.
- Internationally, these assessments play an important part of a policy approach to build trust and confidence in business and these processes are recommended as part of any new Project such as the HRMIS in the public sector.

# PRIVACY IMPACT ASSESSMENT (PIA)

## *Privacy Assessment (Cont.)*

- Demo of application.
- The questionnaire from the Data Protection Office website.



# PRIVACY IMPACT ASSESSMENT (PIA)



## *Privacy Assessment (Cont.)*

**The questionnaire from DPO website**  
*(highlighted in red).*

- ❖ ***“Self Assessment - Questionnaire on Data Protection for Data Controllers and Processors”***  
**(available in pdf and word version)**

# PRIVACY IMPACT ASSESSMENT (PIA)

## *Privacy By Design*

- Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start.
- Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.
- It helps organisations comply with their obligations under the legislation.

# PRIVACY IMPACT ASSESSMENT (PIA)

## *Privacy By Design*

- The Data Protection Office encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle.
- For example when:
  - building new IT systems for storing or accessing personal data;
  - developing legislation, policy or strategies that have privacy implications;
  - embarking on a data sharing initiative; or using data for new purposes.

# PRIVACY IMPACT ASSESSMENT (PIA)

## *Benefits of taking a 'Privacy By Design' Approach*

- Increased awareness of privacy and data protection across an organisation.
- Organisations are more likely to meet their legal obligations and less likely to breach the DPA.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

# PRIVACY IMPACT ASSESSMENT (PIA)

## *Benefits of taking a 'Privacy By Design' Approach (Cont.)*

- Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust.
- Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:
  - ✓ Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
  - ✓ Increased awareness of privacy and data protection across an organisation.
  - ✓ Organisations are more likely to meet their legal obligations and less likely to breach the DPA.
  - ✓ Actions are less likely to be privacy intrusive and have a negative impact on individuals.



# SMART DEVICE APPS



# SMART DEVICES APPS

## *About Apps on Smart Devices*

- **Apps include activities such as:**
  - ✓ Web browsing;
  - ✓ Communication (e-mail, telephony & internet messaging);
  - ✓ Entertainment (games, video / movies & music);
  - ✓ Social Networking;
  - ✓ Banking;
  - ✓ Location based services.
- **Apps can collect large quantities of data & process them in order to provide services to end user.**
  - ✓ E.g. data stored on the device by end user and data from different sensors, including location.



# SMART DEVICES APPS

## *Data Protection Principles*

- **Identifying potential data controllers**
  - Sections 3(3), 3(4) & 3(5) of the **Data Protection Act (DPA)** are relevant.
- **Section 3(3):**

**Subject to Part VII, this Act shall apply to a data controller –**

  - a) who is established in Mauritius and processes data in the context of that establishment; and
  - b) who is not established in Mauritius but uses equipment in Mauritius for processing data, other than for the purpose of transit through Mauritius.

# SMART DEVICES APPS

## *Data Protection Principles (Cont.)*

- **Section 3(4):**

A data controller, falling within subsection (3)(b) shall nominate for the purposes of this Act, a representative established in Mauritius.

- **Section 3(5):**

For the purposes of subsection (3)(a) any person who –

- a) is ordinarily resident in Mauritius;
- b) carries out data processing activities through an office, branch or agency in Mauritius,

shall be treated as being established in Mauritius.

# SMART DEVICES APPS

## *Data Protection Principles (Cont.)*

- The concept of “**establishment**” is crucial in determining whether the DPA is applicable.
- An **organisation XYZ** is involved in the development of apps for **Country A**.
- **XYZ** is geographically located outside **Country A**.
- **XYZ** should consider that all the requirements of apps must comply with **data protection laws of Country A**.

# SMART DEVICES APPS

## *Personal Data*

- Many types of data on smart mobile device are **personal data**.
- They are personal data whenever they relate to:
  - a living individual, who is directly or indirectly identifiable to the controller,
  - a third party,
  - the owner of the device,
  - any other individual.



# SMART DEVICES APPS

## *Personal Data (Cont.)*

- **Data can be:**
  - collected and processed on the device or,
  - once transferred, elsewhere, on app developers' or third parties' infrastructure, via connection to an external API,
  - in real-time without the knowledge of the end user.

# SMART DEVICES APPS

## *Personal Data (Cont.)*

- **Examples of such personal data that can have a significant impact on the private lives of the users and other individuals:**
  - ✓ Location,
  - ✓ Contacts,
  - ✓ Unique device and customer identifiers (such as IMEI, IMSI, UDID & mobile phone number),
  - ✓ Identity of data subject,
  - ✓ Identity of the phone (i.e. name of the phone),
  - ✓ Credit card & payment data,
  - ✓ Phone call logs, SMS or instant messaging,
  - ✓ Browsing history,
  - ✓ Email,
  - ✓ Information society service authentication credentials (services with social features),
  - ✓ Pictures & videos,
  - ✓ Biometrics.

# SMART DEVICES APPS

## *Consent*

- As per section 2 of the DPA, consent to process personal data must have 3 characteristics:
  - 1) a “freely given” consent:
    - ✓ a user must have the choice to accept or refuse the processing of his personal data,
    - ✓ if an app needs to process personal data, a user must be free to accept or refuse,
    - ✓ option to ‘Cancel’ or otherwise stop installation of app must be available.



# SMART DEVICES APPS

## *Consent (Cont.)*

### 2) “informed”:

- ✓ the data subject must have the necessary information at his end in order to form an accurate judgment,
- ✓ such information must be made available before any personal data is processed,
- ✓ includes data processing that could take place during installation of app.

# SMART DEVICES APPS

## *Consent (Cont.)*

### 3) “specific”:

- ✓ the expression of consent must relate to the processing of a particular data item or a limited category of data processing,
- ✓ it is for this reason that simply clicking an “install” button cannot be regarded as valid consent for the processing of personal data **due to the fact that consent cannot be a blanket authorisation**,
- ✓ in some cases users are able to give a granular consent, where consent is sought for each type of data the app intends to access,

# SMART DEVICES APPS

## *Consent (Cont.)*

### 3) “specific”:

- ✓ the alternative approach for an app developer asking its users to accept a lengthy set of terms and conditions and / or privacy policy **does not constitute specific consent**,
- ✓ specific means that the **consent must be limited to the specific purpose** of advising the user about a particular product.

# SMART DEVICES APPS

## *Consent (Cont.)*

### 3) (i) “specific” - e.g. location app

- ✓ the location data from the device may therefore only be accessed when the user is using the app for that purpose,
- ✓ the user’s consent to process geolocation data does not allow the app to continuously collect location data from the device (Note: additional information and separate consent may be required).

# SMART DEVICES APPS

## *Consent (Cont.)*

### 3) (ii) “specific” - e.g. communication app

- ✓ to access the contact list, the user must be able to select contacts that the user wishes to communicate with,
- ✓ instead of having to grant access to the entire address book (including contact details of non-users of that service that cannot have consented to the processing of data relating to them).
- ✓ also relates to the practice of tracking user behaviour by advertisers and any other third party.

# SMART DEVICES APPS

## *Consent (Cont.)*

- **Note:** Even if the consent meets the three elements described above, it is not a license for unfair and unlawful processing to take place.
- If the purpose of the data processing is excessive and/or disproportionate, even if the user has consented, the app developer will not have a valid legal ground and would be in violation of the DPA.

# SMART DEVICES APPS

## *Contractual legal ground*

- **An exception under section 24 or 25 of the DPA:-**
- E.g.: a user consents to the installation of a mobile banking app.
  - In order to fulfill a request to make a payment, the bank does not have to ask for the separate consent of the user to disclose his name and bank account number to the recipient of the payment.
  - **This disclosure is strictly necessary in order to perform the contract with this specific user,**
  - the bank has a legal ground under section 24(2)(a) or section 25(2)(a)(iv) of the Data Protection Act concerning sensitive personal data.



# SMART DEVICES APPS

## *Contractual legal ground (Cont.)*

- **An exception under section 24 or 25 of the DPA:-**
- The same reasoning applies to communication apps.
  - when they provide essential information such as an account name, e-mail address or phone number to another individual that the user wishes to communicate with,
  - **the disclosure is obviously necessary to perform the contract.**

# SMART DEVICES APPS

## *Purpose limitation & data minimisation*

- **Purpose limitation:-**
  - enables users to make a deliberate choice to trust a party with their personal data as they:
    - ✓ will learn how their data are being used, and
    - ✓ will be able to rely on the limitative purpose description to understand for what purposes their data will be used.
- The purposes of the data processing therefore need to be well-defined and comprehensible for an average user without expert legal or technical knowledge.

# SMART DEVICES APPS

## *Purpose limitation & data minimisation (Cont.)*

- Purpose limitation goes hand-in-hand with the principle of data minimisation.
- To prevent unnecessary and potentially unlawful data processing, app developers must carefully consider which data are strictly necessary to perform the desired functionality.
- Third parties obtaining access to the user data through the apps must respect the principles of purpose limitation and data minimisation.
- Information and user controls are the key features to ensure the respect of the principles of data minimisation and purpose limitation.

# SMART DEVICES APPS

## *Security*

- App developers must:
  - **take measures to prevent unauthorised access to personal data** by ensuring that data are protected both in transit and when stored,
  - carefully consider their methods of user identification and authentication.
- The goal of compliance with the security obligation is twofold:
  - it will empower users to more stringently control their data,
  - enhance the level of trust in the entities that actually handle users' data.
- App stores are an important intermediary between end users & app developers and should include a number of robust and effective checks on apps.

# SMART DEVICES APPS

## *The obligation to inform and the content required*

- According to section 22 of the DPA, each data subject has a right to know the identity of the data controller who is processing their personal data.
- In the context of apps, **the end user has the right to know what type of personal data is being processed and for what purpose/s the data is/are intended to be used.**
- If the personal data of the user are collected from other actors in the app ecosystem, the end user has the right to be informed about such data processing.

# SMART DEVICES APPS

## *The obligation to inform and the content required (Cont.)*

- Therefore, if processing personal data, the relevant data controller must inform potential users at the minimum about:
  - who they are (identity and contact detail),
  - the precise categories of personal data the app developer will collect and process,
  - why (for what precise purposes),
  - whether data will be disclosed to third parties,
  - how users may exercise their rights, in terms of withdrawal of consent and deletion of data.

# SMART DEVICES APPS

## *The obligation to inform and the content required (Cont.)*

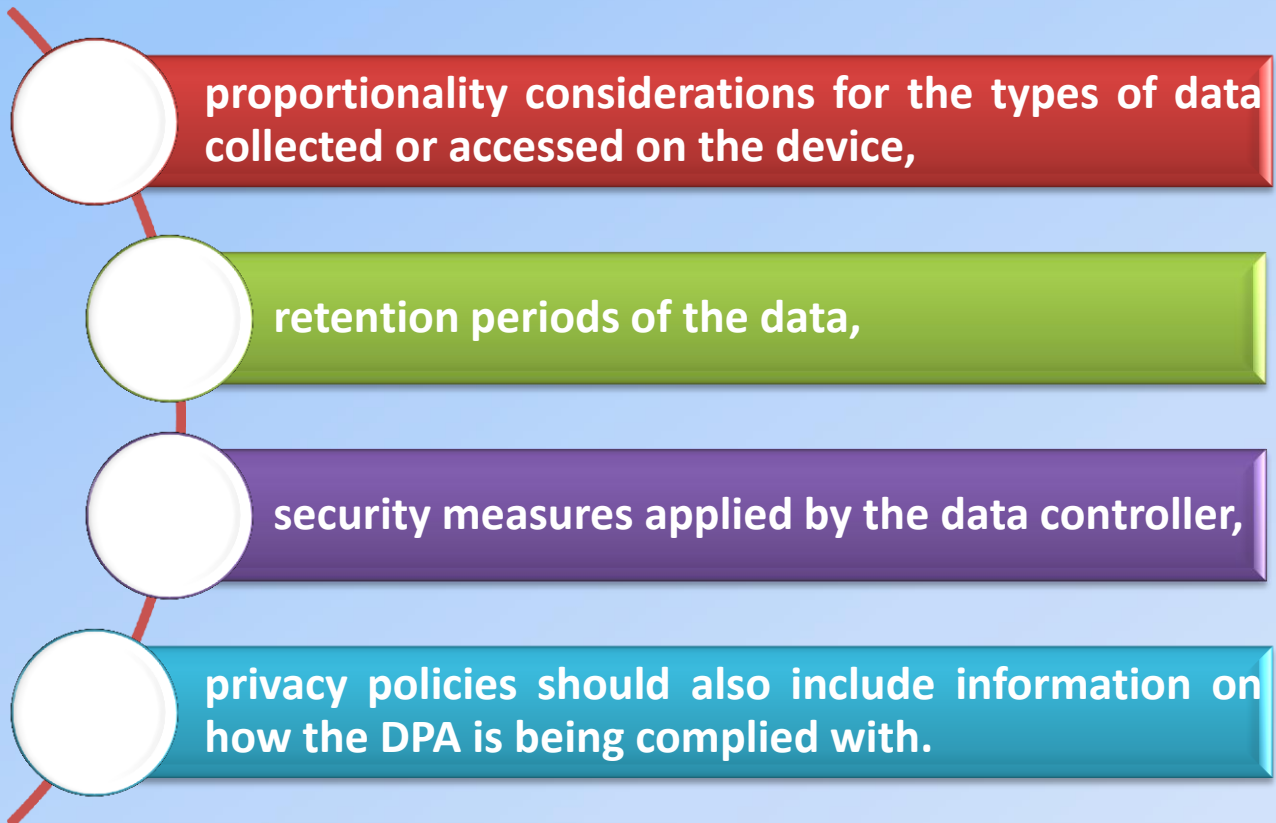
- Availability of this information on personal data processing is critical in order to obtain consent from the user for the data processing.
- Users need to know who is legally responsible for the processing of their personal data and how that controller can be contacted.
- End users must be adequately informed which data are collected about them and why.



# SMART DEVICES APPS

## *The obligation to inform and the content required (Cont.)*

- Data controllers should be able to provide to the users information on:



# SMART DEVICES APPS

## *Recommendations*

- **App developers must:**
  - ✓ comply with their obligations as data controllers **when they process data from and about users;**
  - ✓ comply with their obligations as data controllers **when they contract with data processors** such as if they outsource the collection and processing of personal data to developers, programmers and for example cloud storage providers;
  - ✓ take the necessary organisational and technical measures **to ensure the protection of the personal data they process**, at all stages of the design and implementation of the app (privacy by design);
  - ✓ be aware that **consent does not legitimise excessive or disproportionate data processing.**

# SMART DEVICES APPS

## *Recommendations*

- **App stores must:**
  - ✓ comply with their obligations as data controllers **when they process data from and about users;**
  - ✓ **enforce the information obligation of the app developer,** including the types of data the app is able to access and for what purposes, as well as whether the data is shared with third parties;
  - ✓ implement a **privacy friendly remote uninstall mechanism;**
  - ✓ provide detailed information on the **app submission checks** they actually perform, including those aimed to assess privacy and data protection issues;
  - ✓ **warn app developers about the specificities of the DPA** before submitting the application in Mauritius.

# SMART DEVICES APPS

## *Recommendations*

- **OS and device manufacturers must:**
  - ✓ **employ privacy by design principles** to prevent secret monitoring of the user;
  - ✓ **ensure security of processing;**
  - ✓ **ensure** (the default settings of) **pre-installed apps are compliant** with data protection laws;
  - ✓ Ensure the availability of appropriate mechanisms to inform and educate the end user about what the apps can do and what data they are able to access;
  - ✓ Implement consent collection mechanisms in their OS at the first launch of the app or the first time the app attempts to access one of the categories of data that have significant impact on privacy.

# SMART DEVICES APPS

## *Recommendations*

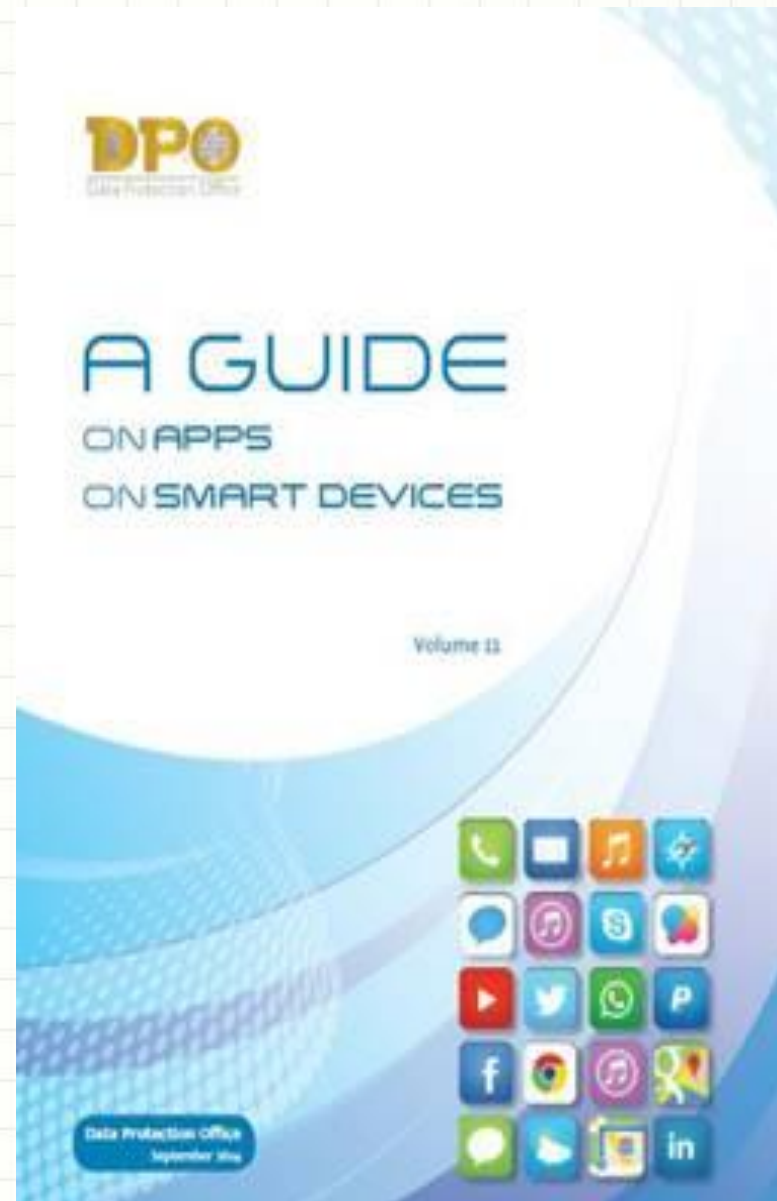
- **Third parties must:**
  - ✓ comply with their obligations as data controllers **when they process personal data about users;**
  - ✓ **comply with the consent requirement determined in section 2 of the DPA** when they read or write data on mobile devices, in cooperation with the app developers and/or app stores, which essentially provide user with the information on the purposes of data processing;
  - ✓ develop and implement simple but secure online access tools for users, **without collecting additional excessive personal data;**
  - ✓ **only collect and process data that are consistent with the context where the user provides the data.**

# SMART DEVICES APPS

## *Guideline*

Further information may be obtained in the guideline: *Vol. 11*  
*“A guide on Apps on Smart Devices”*, which is available on our website:

<http://dataprotection.govmu.org>  
under publications.





# DISCLOSURE





# DISCLOSURE OF INFORMATION

**An organisation must ensure that personal information in its possession is not disclosed in any manner incompatible with the purposes for which such data has been collected, which is an offence under section 29 of the Data Protection Act.**

# DISCLOSURE OF INFORMATION

**The principle is that the prior consent from the concerned data subject should be obtained before any disclosure is made, unless the exceptions under section 24(2) of the DPA are applicable in the circumstances as follows:**

- ☐ **For the performance of a contract to which the data subject is a party and/or;**
- ☐ **For compliance with any legal obligation to which the organisation is subject.**



# DATA SHARING

**The organisation who owns the personal data, i.e. the data controller, is responsible for the personal data in his custody.**

**As per section 24(1) of the Data Protection Act, the express consent of the data subject is required before sharing can be done and the data subject should be informed of that at the time of collection of the personal data according to section 22 of DPA.**

# DATA SHARING

However, as per section 24(2) of the Data Protection Act, personal data may be processed without obtaining the express consent of the data subject where the processing is necessary:

- a. for the performance of a contract to which the data subject is a party;
- b. in order to take steps required by the data subject prior to entering into a contract;
- c. in order to protect the vital interests of the data subject;
- d. for compliance with any legal obligation to which the data controller is subject;
  - (da) for the purpose of making use of unique identification number to facilitate sharing information and avoid multiple registrations among public sector agencies.
- e. for the administration of justice; or
- f. in the public interest.

# DATA SHARING

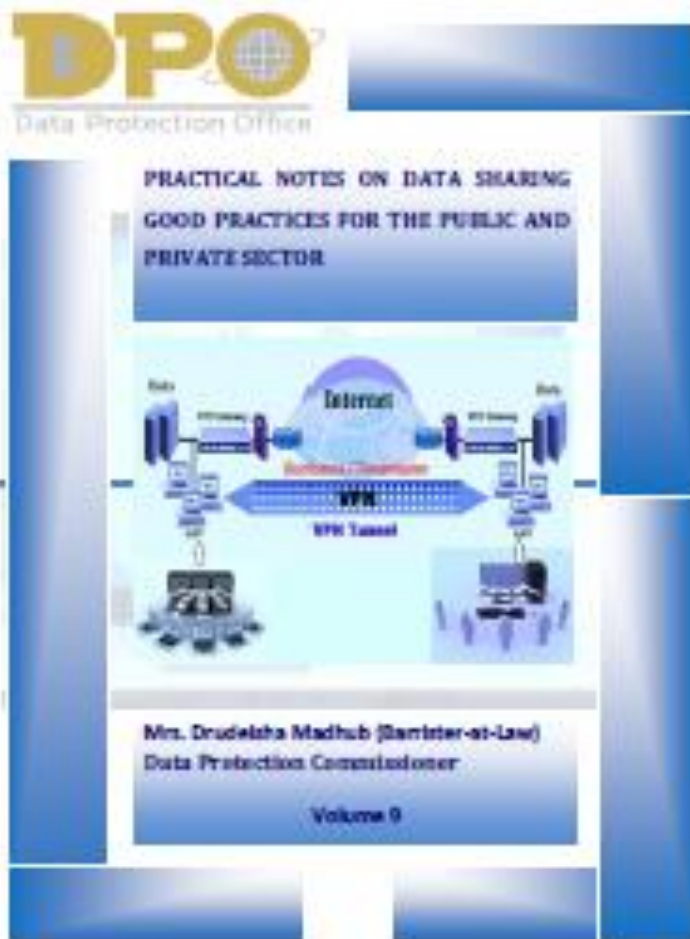
**In the absence of the application of sections 24(1) and 24(2) of the Data Protection Act and any legislation/act which authorises the data to be shared, amendment to existing legislation/act is required to allow the sharing to be done.**

# DATA SHARING

**Whenever data sharing is taking place, the data controller (i.e. the organisation who owns the data) has to ensure that organisational and technical measures are in place to protect the data being shared.**



# DATA SHARING



Further information may be obtained in the guideline: “*Vol. 9 - Practical Notes on Data Sharing Good Practices for the Public and Private Sector*”, which is available on our website at

[http://dataprotection.govmu.org/English/Documents/Publications/Guidelines/Data\\_Sharing.pdf](http://dataprotection.govmu.org/English/Documents/Publications/Guidelines/Data_Sharing.pdf)

# DATA SECURITY



# RISK



Image Source: Office of Privacy Commissioner (OPC)

# 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 unauthorised to do so.**

# BEST PRACTICES





# EMPLOYEE OR END USER EDUCATION

- All relevant security policies must be clearly explained to staff.
- A clear explanation of the consequences for violating these policies must also be explained.
- The end user needs to sign a document acknowledging that they understand the policies and consequences for violating these policies.

# STANDARDS

- **Data Security is subject to several types of audit standards and verification.**

**Example - ISO 27001/27002 : ISMS**

- **Security Administrators are responsible for creating and enforcing a policy that meets the standards that apply to their organisation's business.**

# DATA CLASSIFICATION

- Data needs to be classified in the security policy according to its sensitivity.
- Once this has taken place, the most sensitive data requires extra measures in place to safeguard and ensure its integrity and availability.
- All access to personal data must be logged using audit trail.

# PHYSICAL / TECHNICAL CONTROLS

- **Physical access must be controlled to the data center or area where the data is stored.**
- **Fine Grained Access control must be implemented to define which user needs what type of access / no access on which data.**
- **Encryption of data is recommended for transmission of data across networks.**

# SYSTEM AND NETWORK SECURITY

- The use of firewalls to protect against intrusions.
- Disconnect unused data points.
- If wireless is deployed, use authentication servers to verify and log the identity of those logging on.
- Anti-Virus and malicious software protection on all systems.

# CASE STUDY



# CASE STUDY - BIOMETRIC

**Does management have the right to demand the collection of my biometric data?**

**All employees use a magnetic key to access their workplace.**

**The management decided to change the magnetic access control with a biometric control (iris scanner or hand geometry and fingerprints).**

**They announced this change to the personnel.**



## **CASE STUDY - BIOMETRIC (Cont.)**

**Does management have the right to demand the collection of my biometric data?**

**An employee then phoned a trade union who explained that it is "completely illegal" and that the staff should "refuse to partake" and that dismissal on this ground would be "highly abusive."**

**The employee informed his superior that he did not intend to be subjected to the collection of fingerprints.**

## **CASE STUDY - BIOMETRIC (Cont.)**

**Does management have the right to demand the collection of my biometric data?**

**Informed of the intention of the employee, the management let it be understood that they would consider this lack of collaboration as an unacceptable violation of the employment contract.**

**The supervisor, now worried about this situation, called the Data Protection Office.**

# CASE STUDY - BIOMETRIC (Cont.)

Does management have the right to demand the collection of my biometric data?

## Answer

The Data Protection Office found that the proposed data collection was not proportionate to the actual aim and it would therefore be necessary to obtain the consent of each employee.

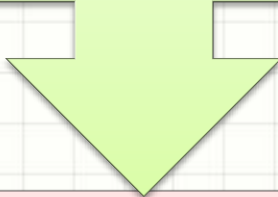
The management postponed the project and promised to study a less intrusive solution.

The employee was pleased that his fears had been heard and that he has the right to oppose such collection.

# **CASE STUDY - VIDEO SURVEILLANCE**

**Does my employer have the right to monitor me by filming me?**

**Being a heavy smoker, an employee makes a dozen times trips to the toilet during the day, where it is forbidden to smoke.**



**About a month after joining the company, he was summoned by the head of service which explained that this going to and from the toilet, the smell of smoke, may be grounds for his dismissal.**

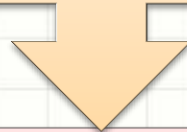
# **CASE STUDY - VIDEO SURVEILLANCE (Cont.)**

**Does my employer have the right to monitor me by filming me?**

**The employee was astounded when he learned that there were cameras hidden in the corridors.**



**Outraged, he informed the office that he would enter a complaint before the Data Protection Office.**



**Anxious to calm his anger, the employer explained why the cameras were installed.**

# CASE STUDY - VIDEO SURVEILLANCE (Cont.)

Does my employer have the right to monitor me by filming me?

## Answer

Video surveillance is very intrusive. The express consent of the persons concerned cannot always be collected.



We may monitor the service provided by a worker, it is however illegal to monitor his behaviour.

# CASE STUDY - PROFESSIONAL EMAIL

**Can my employer have access to my email?**



**An employee is on vacation and didn't divert his mail or put an absence message on his email.**



**Upon his return, the service was disturbed because an urgent file could not be dealt with without access to his email.**



**His head of department issued a warning. The employee denied any fault, insofar as his colleague mistakenly sent the email to him when he was not responsible for this file.**



# CASE STUDY - PROFESSIONAL EMAIL (Cont.)

Can my employer have access to my email?

## Answer



The employee should have received specific instructions on the use of his mail in his absence. Holiday dates must be anticipated.



The professional inbox of an employee may be accessible according to the conditions defined in advance and acknowledged by the employee.

# SUMMARY

PRIVACY

SECURITY

PROTECTION

SAFETY



# RESOURCES


## The Data Protection website

-  Web Links
-  Documents / Forms
-  <http://dataprotection.govmu.org/English/Pages/default.asp>

## The Law

-  <http://dataprotection.govmu.org/English/Legislation/Pages/default.aspx>

## Guidelines

-  <http://dataprotection.govmu.org/English/Pages/Guidelines/Publications---Guidelines.aspx>

**THANK YOU**





# APPENDIX



# USEFUL REFERENCE & LINKS

## The National Computer Board

- + Useful for any relevant documentation in ICT
  - Legislations (Computer Misuse & Cybercrime Act 2003, etc.)
  - Knowledge Bank (Guidelines, e-Security Bulletin, etc.)
- + <http://www.ncb.mu/>

## ICTA

- + ICT Laws
- + <https://www.icta.mu>