Data Protection Office

Data Controllers' Sensitisation Workshop

Presented by (DPO/SDPO):

1) **Mr R. Mukoon**
2) **Mr V. Bhantoo**
3) **Mrs R. Goburdhun**
4) **Mrs W. Khadun**
5) **Mr P. Dookee**

MSB REGISTERED FIRM
RF 153
MS ISO 9001

Date: Thursday 31 March 2016

Venue: Lunch Room, National Assembly

MAURITAS ACCREDITATION

Data Protection Office

Agenda

- Cloud Computing
- Privacy Impact Assessment
- Smart Device Apps
- Biometric Data
- Data Sharing
- Security of Personal Data

Data Protection Office

Cloud Computing

Cloud Computing in Organisations

- Organisations are increasingly moving to cloud across all application areas as well as platform and infrastructure investments.
- Cloud deployments are growing in size, and more mission-critical areas of their business are being run out of the cloud.
- Cloud is also becoming a new way to engage directly with customers and partners.

Various Types of Cloud

- On Premise
- Out of Premise (Public Cloud)
- Hybrid

Two major issues

- Cloud sourcing is an underdeveloped capability and requires newer skills and experiences.
- Contract requirements negotiation checklist which organisations have to work out with all their stakeholders to support their business strategy

Data Protection issues

- You will have to seek authorisation from the Data Protection Commissioner for the transfer of data abroad.
- Retention period depends on the purpose of the processing of the personal data as per section 28 of DPA.
- The duration which has to be determined by you must be reasonably justified.

Data Protection issues

- Section 27 of DPA explains the shared legal responsibilities between a data controller (Organisation) and a data processor (the cloud provider).

- Hence, the data controller must ensure that any selected cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organisation.

Data Protection issues

- Encryption is recommended during the transit of data from your company to the cloud provider.
- The country where the cloud provider is operating should have data protection principles in force.
- In other cases, there is a need to have data protection clauses in your contract.

Data Protection issues-Contract

- You will need to have a written contract with the cloud provider that covers the following points amongst others.
  - Continuity of service, backups and integrity.
  - Certification such as ISO 27001 compliant.
  - Auditing of the cloud provider by third party.
  - Appropriate access rights are provided to officers of your company for creation, amendment and deletion of data with audit trails.
  - Termination of contract: Ensure that all personal data are returned to you and no copies are kept at the cloud provider.

Guideline

- Consult our guideline titled **Vol. 7- "*Privacy Enhancing Technologies* An Absolute Necessity for Effective Compliance with Data Protection Laws"** which covers cloud computing technology and which is available on our website address

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

Other Useful reference

- “Brief: Cloud Contract Negotiations Checklist"
- Forrester report for an overview of the key areas you need to consider when negotiating a cloud contract and advice for negotiating with cloud vendors.

Data Protection Office

Privacy Impact Assessment (PIA)

PIA Tool or Questionnaire

- Privacy Assessment is seen as a valuable tool for businesses and governments which take privacy seriously.

- 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 here dealing with the human right to privacy.

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 and Privacy Compliance Assessments are new techniques which are increasingly being used internationally to better manage privacy risks. 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.

PIA

Privacy Assessment

- 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.

PIA

Privacy Assessment

- Demo of application
- The questionnaire from website

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 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

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 Data Protection Act.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

PIA

Benefits of taking a ‘privacy by design’ approach

- 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 Data Protection Act.
  - ✓ Actions are less likely to be privacy intrusive and have a negative impact on individuals.

Data Protection Office

Smart Device 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 the end user
  - E.g.: data stored on the device by the user and data from different sensors, including location

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.

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;

a) carries out data processing activities through an office, branch or agency in Mauritius,

shall be treated as being established in Mauritius

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**.

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.

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.

Personal Data (Cont.)

- Examples of such personal data that can have a significant impact on the private lives of the users and other individuals are:
  - ✓ 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.

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.

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.

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,

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**,**

Consent (Cont.)

3) **“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).

Consent (Cont.)

3) **“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.

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.

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.

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.**

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.

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.

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.

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.

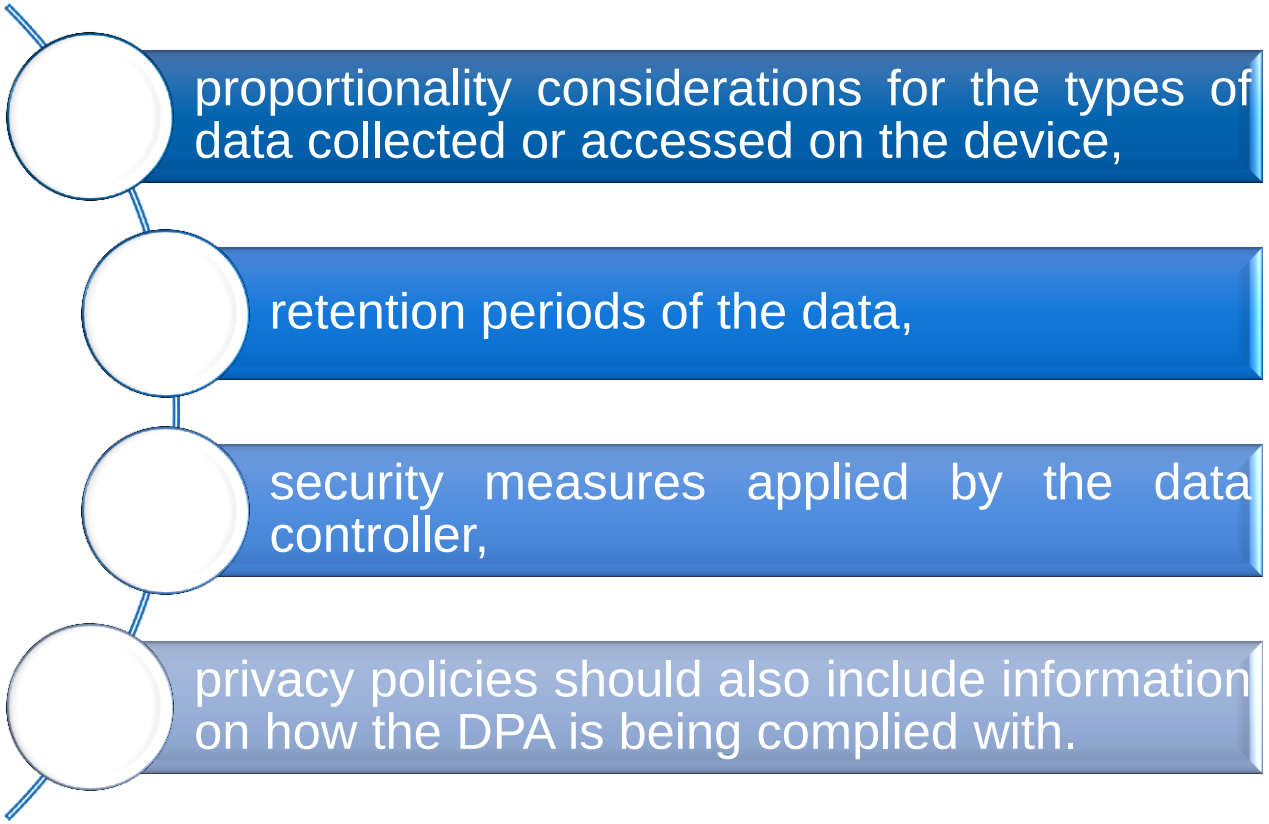
The obligation to inform and the content required (Cont.)

- 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:



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**.

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.

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.

Recommendations

- **Third parties** must:

✓ comply with their obligations as data controllers **when they process personal data about users**;

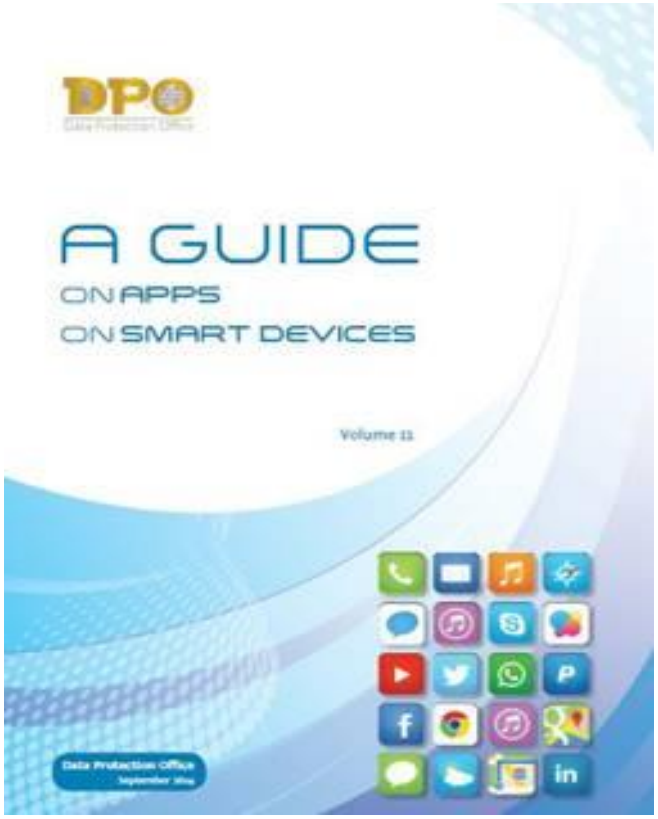
✓ **comply with the consent requirement determined in section 2 of the DPA** when they read or write data on mobile devices, in cooperation with the app developers and/or app stores, which essentially provide user with the information on the purposes of data processing;

✓ 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/

Data Protection Office

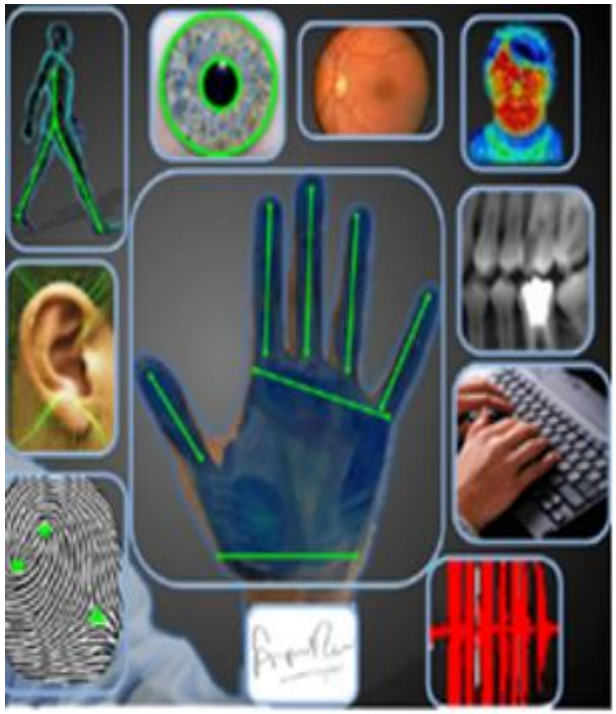
Biometric Data

BIOMETRIC DATA

What is Biometric Data?

- Biometric Data refers to your physical characteristics such as your fingerprints, iris, retina, outline of a hand, an ear shape, voice pattern, DNA amongst others.

- In today's evolving society, biometric is becoming a more popular means for identification and verification of people.



Uses of Biometric Data

- **Identification** confirms the identity of the person. It involves taking the measured characteristic and trying to find a match in a database containing records of people and their characteristics.

- **Verification** is determining if a person is who they say they are. It involves taking the measured characteristic and comparing it to the previously recorded data for that person.

Types of Biometric Data- Description

- There are two types of biometrics: behavioral and physical.
  - Examples of physical biometrics include:
    - **Fingerprint** - analyzing fingertip patterns
    - **Facial Recognition** - measuring facial characteristics
    - **Hand Geometry** - measuring the shape of the hand
    - **Iris Scan** - analyzing features of colored ring of the eye
    - **Retinal Scan** - analyzing blood vessels in the eye
    - **Vascular Patterns** - analyzing vein patterns
    - **DNA** - analyzing genetic makeup
  - Examples of behavioral biometrics include:
    - **Speaker Recognition** - analyzing vocal behavior
    - **Signature** - analyzing signature dynamics
    - **Keystroke** - measuring the time spacing of typed words

Biometric Data under DPA

- All biometric data pertaining to a living individual are “personal data” within the DPA.
- The Data Protection Act applies when use or processing of all personal data are being made.

Applicability of DPA (relevant sections)

- Section 22: Collection of Personal data
  - Processing for lawful and necessary purpose
  - Transparency (e.g. Purpose/purposes for which data is being collected; the identity of the data controller, intended recipients amongst others)

- Section 23: Accuracy of data has to be ensured
  - Any biometric system must accurately identify the person whose data are processed by the system. If changes in physical or physiological characteristics result in a template becoming outdated, a procedure must be put in place by the Data Controller to ensure that the data is kept up to date.

BIOMETRIC DATA

Applicability of DPA (relevant sections)

- Section 24: Processing of Personal Data
  - The express consent of the data subject is required for processing personal data
- Section 25: Processing of sensitive data
  - Biometric data reveal sensitive information about us; our health, genetic background, age and it is unique to each of us. So again ,express consent of the person is required before processing of the data.

Applicability of DPA (relevant sections)

- Section 26: Use of Personal Data
  - Keeping for specified purpose(s) & ensuring that the data is adequate, relevant and not excessive
    - The key word here is "excessive". Questions to be asked when considering the installation of a biometric system:
      - What is the need for it? Is there a need for a particular system?
      - What is wrong with current systems?
      - Do we have less invasive alternatives?
    - A data controller must conduct an assessment of the need for a biometric system and an evaluation of the different types of system before the introduction of any particular system.

BIOMETRIC DATA

Applicability of DPA (relevant sections)

- Section 27: Security of personal data
  - The organisation as data controller has the responsibility to ensure that the data is safe and secure.

- Section 28: Data is kept only for a justified duration.
  - In the context of a biometric system in a workplace, the data controller should devise a retention policy in advance of the deployment of the system which clearly sets out the retention period which would apply to biometric data.

- Section 29: Unlawful disclosure is not allowed
  - Any data controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purposes for which such data has been collected shall commit an offence.

Exemption from DPA

- Section 24 (2) and Section 25(2): Provides some exemptions where the consent of data subject is not required.
- Section 45: Exemption from DPA application allowed for national security
- Section 46: Exemption to certain sections of the DPA allowed for the prevention or detection of crime by relevant authorities

Biometric Data

Biometric fingerprint for attendance purposes

- Requires consent of individuals unless explicitly provided in the contract of employment and the employee is agreeable, or is required by law or relates to information made public by the employee. In case no consent is received, alternative methods for recording attendance must be provided.
- Appropriate security and organisational measures must be implemented to secure the data and counteract the 3 main risks associated with the use of fingerprints namely identity fraud, purpose diversion and data breach occurrence.

- Appropriate retention policies must be established e.g what will happen to the data when an employee leaves the organisation?

BIOMETRIC DATA

Best Practices - The Four Part Test

Case to case analysis using the following principles to show that collection is required:

- Necessity
  - Is the measure demonstrably necessary to meet a specific need?
- Effectiveness
  - Is it likely to be effective in meeting that need?
- Proportionality
  - Would the loss of privacy be proportionate to the benefit gained?
- Alternatives
  - Is there a less privacy-invasive way of achieving the same end?

BIOMETRIC DATA

Best Practices - Privacy Impact Assessments

- A Privacy Impact Assessment is a process intended to help organisations consider the impact that a new or substantially modified initiative can have on people's privacy, especially when personal information is being collected. The process is useful for any organisation.

- Guideline titled Vol. 6 – "**Guidelines on Privacy Impact Assessments"** on http://dataprotection.govmu.org

Data Protection Office

Data Sharing

DATA SHARING

Definition

- ‘Data sharing’ refers to the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation.

- ‘Data sharing’ does not only mean sharing data between organisations but also apply to the sharing of information within an organisation.

DATA SHARING

Sharing with a ’data processor’

- A form of data sharing where a data controller shares data with another party that processes personal data on its behalf.

- The DPA (Section 27) requires that a data controller using a data processor must ensure, in a written contract, that:
  - the processor only acts on instructions from the data controller; and
  - it has appropriate security and organisational measures in place that is equivalent to those imposed on the data controller by the seventh data protection principle.

Main types of data sharing

- **'Systematic' data sharing**
  - Involves routine sharing of data sets between organisations for an agreed purpose or a group of organisations making an arrangement to 'pool' their data for specific purposes.

- **Ad hoc or 'one-off' data sharing**
  - Involves a decision about sharing being made in conditions of real urgency, for example in an emergency situation, not covered by any routine agreement.

DATA SHARING

Personal data and Sensitive personal data

- **Personal data** means data which relate to a living individual who can be identified from those data.
- **Sensitive personal data** means personal data consisting of information such as:
  - the racial or ethnic origin of the data subject,
  - his political opinions,
  - his religious beliefs or other beliefs of a similar nature,
  - whether he is a member of a trade union

Personal data and Sensitive personal data (2)

- **Sensitive personal data** means personal data consisting of information such as:
  - his physical or mental health or condition,
  - his sexual life,
  - the commission or alleged commission by him of any offence, or
  - any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

DATA SHARING

Questions to ask before sharing personal data

- Is the sharing justified?
  - Have you assessed the potential benefits and risks to the individuals and/or society of sharing or not sharing?
  - Is the sharing proportionate to the issue you are addressing?
  - Could the objective be achieved without sharing personal data

Questions to ask before sharing personal data (2)

- Do you have the legal power to share?
  - The nature of the information you have been asked to share?(for example is it confidential?)
  - Any legal obligation to share information (for example a statutory requirement or a court order)

DATA SHARING

Importance of personal express consent

- One of the conditions the DPA provides to legitimise processing of personal data.

- If you are going to rely on consent as legal justification for sharing you must be sure that individuals know precisely what data sharing they are consenting to and understand its implications for them. They must also have genuine control over their data after the sharing takes place through their right of access.

Importance of personal express consent (2)

- Consent for data sharing is most likely to be needed where:
  - confidential or particularly sensitive information is going to be shared without a clear legal basis for doing so;
  - the individual would be likely to object should the data be shared without his or her consent; or
  - the sharing is likely to have a significant impact on an individual or group of individuals.

Disclosure under DPA

- Section 29 of the DPA highlights the criminalisation of unlawful disclosure of personal data where any data controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purposes for which such data has been collected shall commit an offence.

- Section 52 of the DPA provides an exempt from the listed principles in the section for disclosure of personal data required by law and in connection with legal proceedings

Data sharing agreements

- A good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

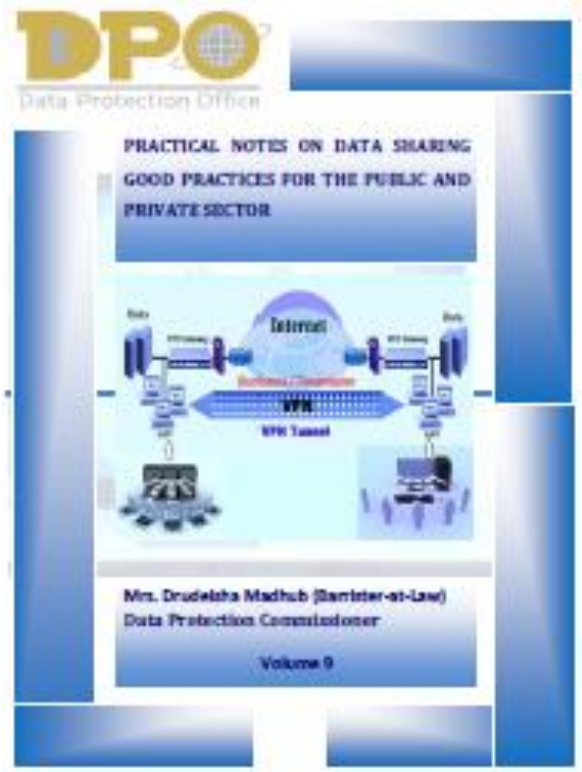
- A data sharing agreement should, at least, document the following issues:
  - the purpose, or purposes, of the sharing;
  - the potential recipients or types of recipient and the circumstances in which they will have access;
  - the data to be shared;
  - data quality – accuracy, relevance, usability etc;

Data sharing agreements

- A data sharing agreement should, at least, document the following issues:
  - retention of shared data;
  - individuals' rights – procedures for dealing with access requests, queries and complaints;
  - review of effectiveness/termination of the sharing agreement; and
  - sanctions for failure to comply with the agreement or breaches by individual staff.

Guideline

Further information may be obtained in our guideline Vol. 9 – “**Practical Notes on Data Sharing Good Practices for the Public and Private Sector”** available on our website address http://dataprotection.govmu.org



Data Protection Office

Security of Personal Data

Security – CIA Triad

- Confidentiality
- Integrity
- Availability

- **Confidentiality, integrity and availability**,
  - also known as the **CIA triad**,
    - is a model designed to guide policies for information security within an organization.

Elements of Security

- The elements of the triad are considered
  - the three most crucial components of security.

- In this context,
  - confidentiality is a set of rules that limits access to information,
  - integrity is the assurance that the information is trustworthy and accurate, and
  - availability is a guarantee of reliable access to the information by authorized people.

Confidentiality

- Confidentiality is roughly equivalent to privacy.
- Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it:
  - Access must be restricted to only those authorized parties to view or maintain the data in question as per their designated role.
  - It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands.
  - More or less stringent measures can then be implemented according to those categories.

Safeguarding data confidentiality

Sometimes safeguarding data confidentiality may involve

- strong passwords and password-related best practices and
- information about social engineering methods,
  - to prevent them from data-handling rules with good intentions and potentially disastrous results.
- Extra measures must be taken in the case of extremely sensitive documents,
  - precautions such as storing only on very secured computers,
  - Protected disconnected storage devices or, for highly sensitive information, in hard copy form only.

Data Integrity

- Integrity involves maintaining
  - the consistency, accuracy, and trustworthiness of data over its entire life cycle.
- Data must not be changed in transit, and
  - steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

Data Integrity

- These measures include file permissions and user access controls.

Version control maybe used to prevent erroneous changes or accidental deletion by authorized users becoming a problem.

- In addition, some means must be in place
  - to detect any changes in data that might occur as a result of non-human-caused events such as strong electromagnetic pulse (EMP) or file/ computer/server crash.

Availability

- Availability is best ensured by
  - rigorously maintaining all hardware,
  - performing hardware repairs immediately when needed and
  - maintaining a correctly functioning operating system environment that is free of software conflicts.
- It's also important to keep current with
  - all necessary system upgrades.
- Safeguards against data loss or interruptions in connections must include
  - unpredictable events such as natural disasters and fire.

Availability

- To prevent data loss from such occurrences,
  - a backup copy may be stored in a geographically-isolated location,
    - perhaps even in a fireproof, waterproof safe.
- Extra security equipment or software such as
  - firewalls and proxy servers can guard against downtime and unreachable data due
    - to malicious actions such as denial-of-service (DoS) attacks and network intrusions.

DPO
Data Protection Office

Thank You