



DATA PROTECTION IN AN ORGANISATION

Presented by:

- **Mr Padaruth Dookee (Data Protection Officer/ Senior Data Protection Officer)**
- **Mrs Rushda Goburdhun (Data Protection Officer/Senior Data Protection Officer)**

Date: Friday 13 January 2017 at 10:00

Venue: MITCO, EBENE SKIES

Today's Agenda

1

- Our Vision

2

- Data Protection Office

3

- Data Protection Act 2004 (DPA)

4

- Definitions

5

- 8 Principles of Data Protection Act

6

- Functions of Data Protection Office

7

- Managing Data Protection

8

- Offences and Penalties

9

- Resources

OUR VISION

- **A society where Data Protection is understood and practiced by all.**
- **The right to privacy and data protection is primordial to the sanctity of any modern democracy.**
- **The adoption of clear procedures for the collection and use of personal data in a responsible, secure, fair and lawful manner, by all data controllers and data processors.**



DATA PROTECTION OFFICE

The DPO is under the aegis of the Ministry of Technology, Communication and Innovation enforces the **Data Protection Act**.

Mission of DPO

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

DATA PROTECTION ACT 2004

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.

THE MAIN ELEMENTS IN THE ACT

PART I

- PRELIMINARY - Definitions etc.

PART II

- DATA PROTECTION OFFICE

PART III

- POWERS OF COMMISSIONER

PART IV

OBLIGATION ON DATA CONTROLLERS : SECTIONS 22 – 32

PART V

- THE DATA PROTECTION REGISTER : SECTIONS 33 – 40

PART VI

- RIGHTS OF DATA SUBJECT : SECTIONS 41 – 44

PART VII

- EXEMPTIONS: SECTIONS 45 – 54

PART VIII

- MISCELLANEOUS

DEFINITIONS

Personal Data means –

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

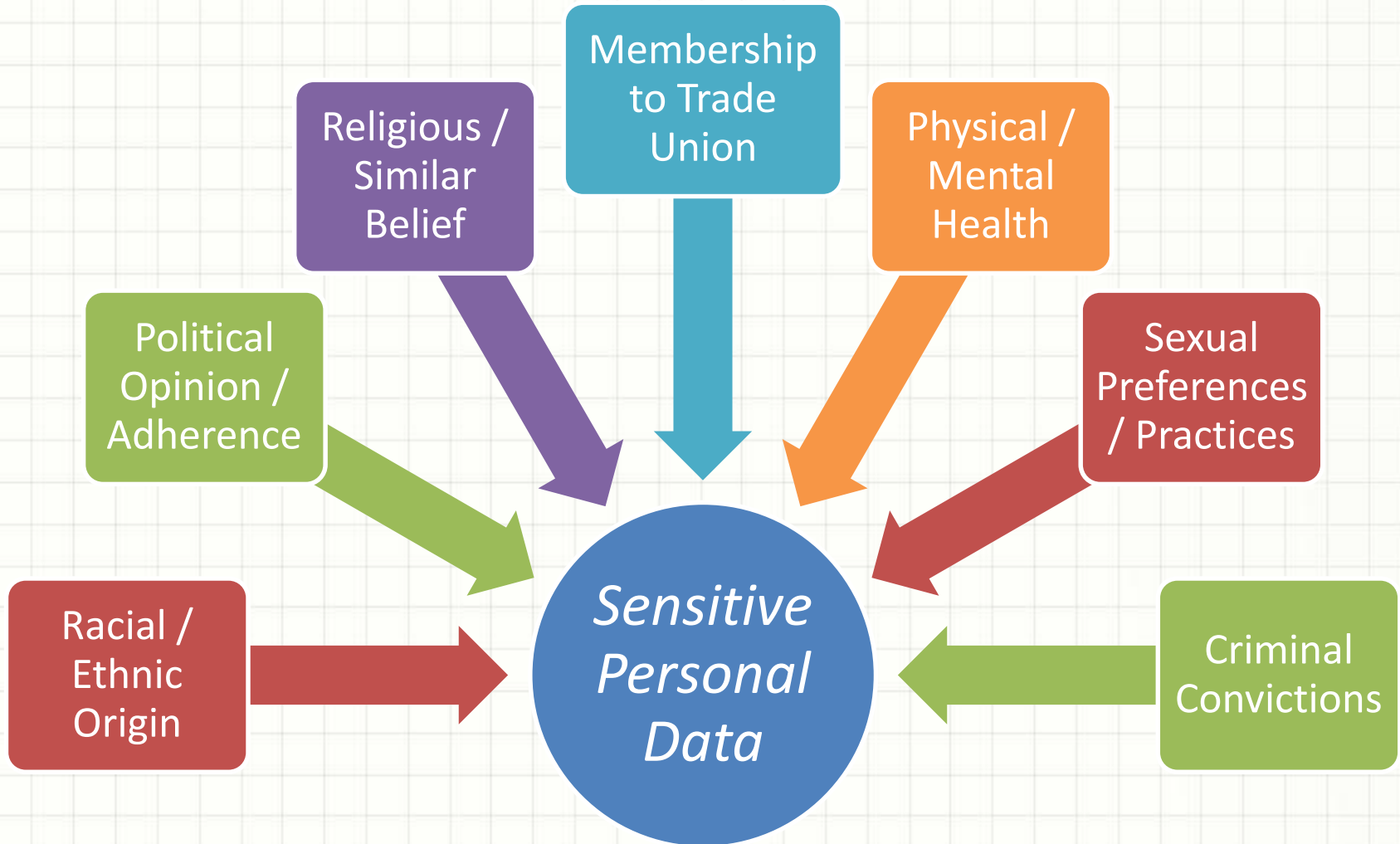
- a) data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion;

EXAMPLES OF PERSONAL DATA

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

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;

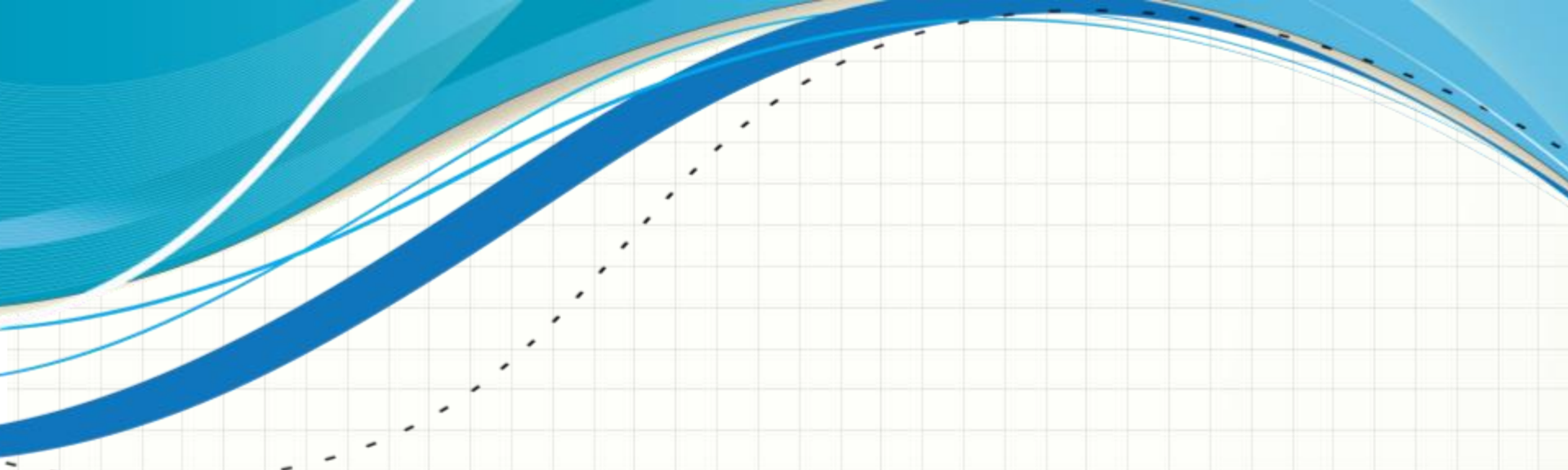
DEFINITIONS (Cont.)

Data Controller means a person who,

- either alone or jointly with any other person,
- makes a decision with regard to the purposes for which and
- in the manner in which any personal data are, or are to be, processed;

The data controller can be the organisation,

- or can also be an individual if that individual is acting on his/her own initiative
- for example, doctors, lawyers or sole traders.



8 DATA PROTECTION PRINCIPLES

8 DATA PROTECTION PRINCIPLES

The DPA is based around 8 principles, which are flexible enough to accommodate most every day situations.

- **Principle 1: Fairness**

Personal data must be collected and used fairly and lawfully.

- **Principle 2: Transparency**

Personal data must be obtained only for any specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose.

- **Principle 3: Quantity**

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

- **Principle 4: Accuracy**

Personal data must be accurate and, where necessary, up to date.

8 DATA PROTECTION PRINCIPLES (Cont.)

- **Principle 5: Time limit**

Personal data must not be kept for longer than necessary.

- **Principle 6: Individuals' rights**

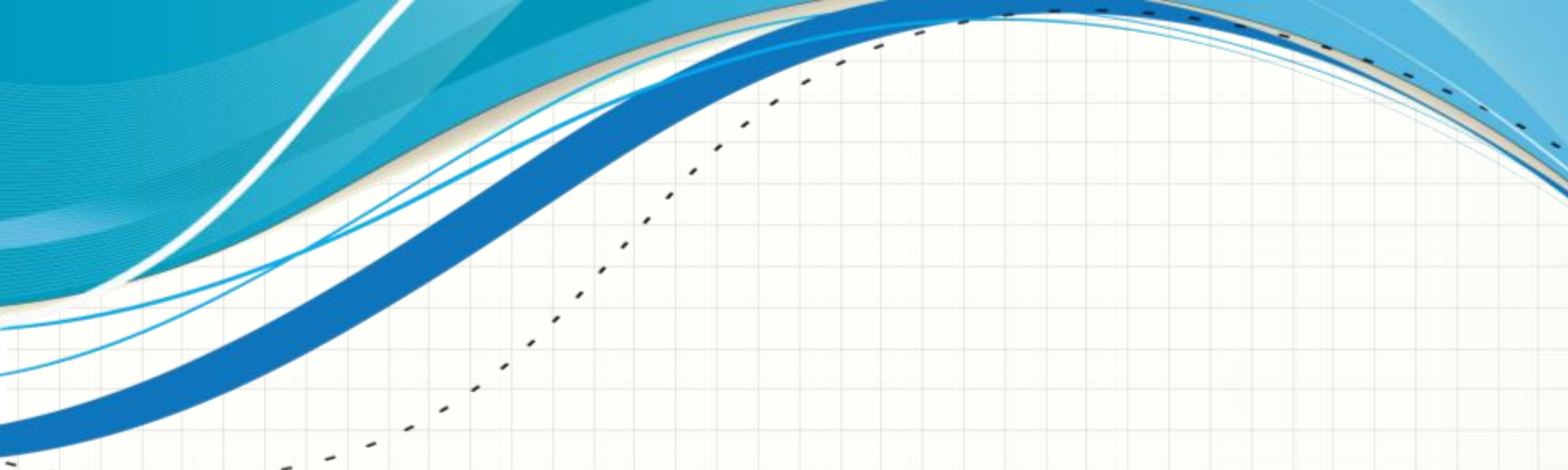
Personal data shall be processed in accordance with the rights of data subjects.

- **Principle 7: Security**

Appropriate security measures must be implemented to prevent personal data being accidentally or deliberately compromised.

- **Principle 8: International transfers**

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 processing of personal data.



FUNCTIONS OF THE DATA PROTECTION OFFICE

FUNCTIONS OF THE DATA PROTECTION OFFICE

I

- REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS IN MAURITIUS

II

- INVESTIGATION OF COMPLAINTS

III

- CONDUCT DATA PROTECTION COMPLIANCE AUDITS

IV

- SENSITISATION

V

- EXERCISE CONTROL ON ALL DATA PROTECTION ISSUES

VI

- RESEARCH ON DATA PROCESSING AND COMPUTER TECHNOLOGY

REGISTRATION OF DATA CONTROLLERS

- Under **section 33** of the Data Protection Act, every data controller and data processor shall, before keeping or processing personal data or sensitive personal data, register himself with the Data Protection Commissioner.
- The provisions for making registration & renewals have been made under **sections 34 to 39** of the Data Protection Act respectively.

INVESTIGATION OF COMPLAINTS

- The Data Protection Commissioner has the power to investigate any complaint or information which gives rise to a suspicion that an offence may have been, is being or is about to be committed under the Data Protection Act.
- All investigations on complaints are carried out as per **section 11** of the Data Protection Act.
- All complaints are investigated effectively, fairly and in a timely manner with all the concerned parties and upon finalisation of the enquiry, the Commissioner gives a decision.

COMPLIANCE AUDIT

- The Commissioner may carry out periodical audits of the systems of data controllers or data processors to ensure compliance with data protection principles and to adopt best practices.
- All compliance audits are carried out as per **section 15** of the Data Protection Act.

SENSITISATION

- **To promote and simplify the understanding of the legal provisions of the Data Protection Act, extensive sensitisation campaigns have been accomplished:**
 - **Presentation sessions at data controllers' site**
 - **Trainings provided to data controllers**
 - **This office was benchmarked by officials of the Tanzanian government**
 - **Participation in international workshops**
 - **Organisation of capacity building sessions for senior public officers**
 - **Organisation of workshop for both private and public sector audiences**
 - **Organisation of the 36th International Conference in Mauritius**
 - **Publication of guidelines**
 - **24th hour helpdesk service for our customer service**

24 HOUR HELPDESK

- The Data Protection Office has set up an automated 24 hour helpdesk facility on
 - **230-2039076**
 - **138**
- The helpdesk became operational as from August 2012 and assists anyone seeking information on the role and mission of the office, and their respective obligations and rights under the Data Protection Act.



MANAGING DATA PROTECTION

MANAGING DATA PROTECTION

Establish an appropriate policy on data protection

- **At organisational level, a policy will help an organisation to address data protection in a consistent manner.**
- **The policy should clearly set out the business's approach to data protection together with responsibilities for implementing the policy and monitoring compliance.**
- **The policy should be approved by management, published and communicated to all staff.**
- **The policy should also be reviewed and updated as and when required.**

MANAGING DATA PROTECTION

Identify a data protection lead

- **It is good practice to identify a person or department responsible for developing, implementing and monitoring the data protection policy.**

MANAGING DATA PROTECTION

Awareness

- **An organisation must take all reasonable steps to ensure that its employees are aware on matters related to data protection and to raise their concerns with the appropriate person/department responsible for data protection compliance in the organisation.**

MANAGING DATA PROTECTION

Registration as Data Controller

- **A data controller must register with the Data Protection Office for all personal data being processed (Part V of the DPA).**
- **Registration should be renewed annually.**

MANAGING DATA PROTECTION

Privacy Notices

To ensure that the processing of data is fair, it is a good practice to include privacy notices on an organisation's website and any forms that is used to collect data. These notices should clearly explain the reasons for using the data, including any disclosures.

It is good to mention here that in case an organisation wants to use personal data in a manner different to its privacy notice, then prior consent to use or disclose personal data is required from the data subject unless the exceptions listed under section 24(2) of the DPA applies where an organisation can proceed without prior consent.

EXCEPTION OF CONSENT

Section 24(2) of DPA

(2) 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;**
- (e) for the administration of justice; or**
- (f) in the public interest.**

MANAGING DATA PROTECTION

Access request rights

The sixth principle of the DPA requires that personal data is processed in accordance with individual rights. Under section 41 of the DPA, a data subject has the rights of access to information that the organisation holds about him/her.

An individual can make a written request to see and obtain a copy of his/her information being held upon payment of the prescribed fee to the organisation.

You should therefore have a process in place to recognise and respond to requests within statutory timescales.

MANAGING DATA PROTECTION

Data quality & accuracy

An organisation should regularly review information to identify when to correct inaccurate records and remove irrelevant ones.

MANAGING DATA PROTECTION

Retention and disposal

- The fifth principle of the DPA requires that personal data should not be kept for longer than necessary. It is important to note that the DPA does not set any time limit to retain data.
- The onus lies on the data controller to determine the time retention based on the purpose for which data is being kept and in accordance with other laws such as Employment Rights Act, Income Tax Act, Banking Act, etc..

MANAGING DATA PROTECTION

Security policy

The seventh principle of the DPA requires that personal data is protected by appropriate security measures.

Before you can decide what level of security is right for your business you will need to assess the risks to the personal data you hold and choose the security measures that are appropriate to your needs.

MANAGING DATA PROTECTION

Transfer of Data Abroad

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

PRIVACY IMPACT ASSESSMENTS

Build in privacy considerations at the start of projects or initiatives that involve the processing of personal data.

- **Thinking about privacy early on will reduce risks and avoid costly changes at a later date.**

http://dataprotection.govmu.org/English/Documents/Publications/Guidelines/DPO_Vol6_PrivacyImpactAssessment.pdf

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.

The principle is that the prior consent from the concerned data subject should be obtained before any disclosure is made, unless you fall under the exceptions of **section 24(2)** of the DPA.

OFFENCES AND PENALTIES

- Subject to **Section 61** of the DPA, any person who contravenes this ACT shall commit an offence.
- Where no specific penalty is provided for an offence, the person shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

RESOURCES

- The Data Protection website
 - <http://dataprotection.govmu.org/English/Pages/default.asp>

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

THANK YOU

