# AN OVERVIEW OF THE DATA PROTECTION ACT 2017

Association of Trust and Management Companies (ATMC)

Presented By:
Mrs Drudeishda Madhub
Data Protection Commissioner
31st July 2018

# Agenda

- Aims of the Data Protection Act 2017 (DPA)
- Benefits of the Act
- The Data Protection Office
- Functions of the Data Protection Office (DPO)
- Definitions
- Registration
- Obligations on Controllers and Processors
- Processing operations likely to results in high risk
- Transfer of personal data
- Rights of data subjects
- Offences and penalties
- Certification

# Aims of the DPA
## (came into force on 15 January 2018)

- To strengthen the control and personal autonomy of data subjects (individuals) over their personal data.
- In line with the European Union's General Data Protection Regulation (GDPR).
- To simplify the regulatory environment for business in our digital economy.
- To promote the safe transfer of personal data to and from foreign jurisdictions

# Benefits of the Act

- Increased accountability of controllers
  - Implement better processes
  - Better organisations
  - Better productivity
  - Strengthen customer trust
  - Gain confidence and trust

- Enhanced data subjects' rights of individuals for greater control over their personal data.

- Improve the digital legal landscape to respond to the new EU requirements for adequacy, thereby attracting foreign investors.

- Minimised risk of data breaches

# The Data Protection Office (DPO)

- Public office which acts with complete **independence** and **impartiality.**

- Not subject to the control or direction of any other person or authority in the discharge of its functions

- Head of the Office is the Data Protection Commissioner

# Functions of DPO

| | |
|---|---|
| I | Ensure compliance with DPA 2017 and regulations |
| II | • Registration of controllers and processors |
| III | • Investigation of complaints |
| IV | • Sensitisation/ Training |
| V | • Exercise control on all data protection issues |
| VI | • Conduct data protection compliance audits |
| VII | • Cooperate with supervisory authorities of other countries |
| VIII | • Research on data processing and computer technology |

# Definitions

## Section 2 - Interpretation

# Basic Concepts

**Personal data**

- any information relating to a data subject.

**Data Subject**

- an identified or identifiable individual (any data which can identify an individual),
- in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

# Basic Concepts

**Processing**

- an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as, collection, recording, organisation, structuring, storage, restriction, erasure or destruction, use, etc.

**Controller**

- a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing.

**Processor**

- a person who, or a public body which, processes personal data on behalf of a controller.

# Registration of Controllers and Processors

**Sections 14 to 20**

# Registration

**Should controllers and processors register with the Data Protection Office? → *YES***

- *"... no person shall act as controller or processor unless he or it is registered with the Commissioner...", Part III, Section 14*
- *Validity of Registration Certificate:* ***3 years***
- *Renewal:* ***3 months prior to expiry***
- *Notification of change in particulars within* ***14 days***

# Registration

**Can a management company (MC) register on behalf of global business entity?**

- **YES** provided that:
  - *The management company is keeping all personal data of the global business entity i.e. when all personal data are **centralised** at the management company.*
  - *The MC clearly indicate that it accepts "**total legal responsibility**" under the DPA 2017 as controller of the global business entity.*
  - ***Note:***
    - *MC should provide a list of GBCs under their responsibility at the time of registration.*
    - *Updated list should be provided at the time of renewal.*

- If a single commercial operation is being carried out by the global business entity in Mauritius then it is assumed that personal data are not centralised and the global business entity should thus be registered separately.


# Obligations on controllers and processors

Sections 21 to 33

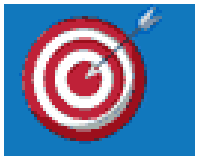
# Obligations on controllers and processors

| | | |
|---|---|---|
| Principles relating to processing of personal data | Duties of Controller (Designate a data protection officer) | Collection of personal data |
| Conditions for consent (bear burden of proof for consent prior to processing) | Notify personal data breach to this office | Communicate personal data breach to data subject |
| Duty to destroy personal data | Ensure lawfulness of processing of personal data | Comply with requirements to process special categories of data |
| Consent for processing personal data for children | Ensure appropriate data security and organizational measures | Keep record of all processing operations |

# Principles relating to processing of personal data – Section 21

**Lawfulness, Fairness and Transparency**

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to any data subject



**Purpose Limitation**

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

**Data Minimisation**

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

**Accuracy**

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

**Storage Limitation**

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

**Rights of data subject**

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

# Duties of Controller – Section 22

Every controller must adopt policies and implement appropriate technical and organisational measures so as to ensure and be able to demonstrate that the processing of personal data is performed in accordance with this Act.


Such measures includes:

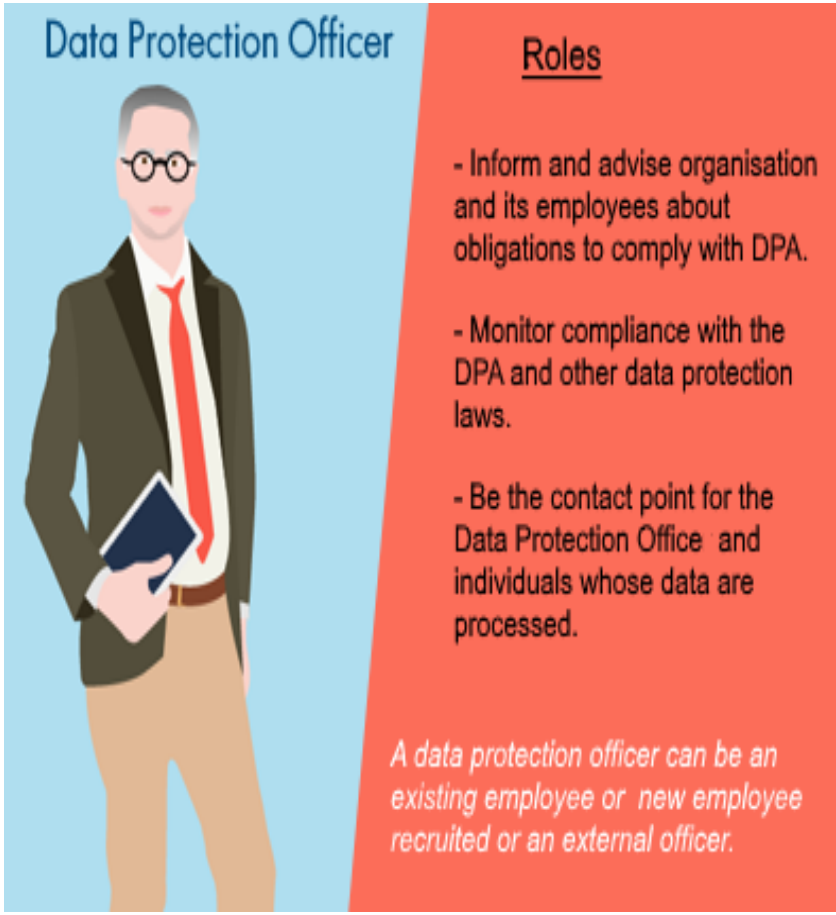
- implementing appropriate data security and organisational measures;
- keeping of documentation;
- Performing data protection impact assessment as per section 34;
- Comply with requirements of prior authorization and consultation as per section 35;
- Designate an officer responsible for data protection.

# Duties of Controller – Section 22

## Should a controller appoint a data protection officer?

**YES** according to section 22 2(e).

- Even though the data protection officer is responsible for assisting the controller or processor in monitoring the internal compliance, the officer is not personally responsible for any non-compliance with the Act by the controller or processor.
- It will be up to the controller or processor to demonstrate compliance, regardless of how much autonomy the data protection officer is granted.




- *It is the responsibility of the controller or processor to determine whether they need to have a single or different data protection officer(s) for their subsidiaries. For example, a single data protection officer may be designated for several subsidiaries, taking account of their organisational structure and size.*

# Collection of personal data – Section 23

- Collect personal data for a lawful purpose.
- Details to be provided to the data subjects
  - The organisation's contact details and where applicable its representative and any data protection officer;
  - Purpose(s) for which you are collecting the data;
  - To whom you intend to disclose the data;
  - Whether the collection is voluntary or mandatory;
  - Right to withdraw consent at any time;
  - Rights of data subjects: Access, Rectification, Erasure, Object to Processing;
  - Automated decision making, and the consequences of such processing;
  - Period for storing the data;
  - Right to lodge a complaint with the Commissioner;
  - To which countries they intend to transfer the data.

# Conditions for Consent - Section 24

- The controller must be able to supply evidence that consent has been obtained(verifiable).
- Consent can be withdrawn at any time.
- When consent is not necessary for a provision of a service, then you should not require consent. It is thus the responsibility of controllers to determine same. Section 28(1)(b) DPA 2017 provides for exceptions regarding consent.

**Definition:**

*Consent means any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed.*

## Notification of personal data breach – Section 25

- As soon as the controller becomes aware that a personal data breach has occurred,
- the latter must notify the Data Protection Office, without undue delay and, where feasible, not later than 72 hours.
- Section 25 (3) of the Act provides details on how the notification should be.

## Communication of personal data breach to data subject – Section 26

- Where a personal data breach is likely to result in a high risk to the rights and freedoms of the individual,
- the controller must communicate that breach to the data subject, without undue delay, in order to allow him / her to take the necessary precautions;
- E.g. by replacing credit cards if the data subject's card details have been leaked

# Duty to destroy personal data - Section 27

- Where the purpose for keeping personal data has lapsed, every controller shall destroy the data as soon as is reasonably practicable; and notify any processor holding the data.

- Retention period has to be defined by the controllers/processors by taking into account other laws.

- Example: Personal data may be removed from marketing list/database if data subject withdraws consent

# Lawful processing – Section 28

- No person shall process personal data unless the data subject **consents to the processing** for one or more specified purposes.

| | |
|---|---|
| Or Exceptions apply (for example) | For the performance of a contract to which the data subject is a party |
| | For compliance with any legal obligation to which the controller is subject to |
| | To protect vital interests of data subject |
| | for the purpose of historical, statistical or scientific research amongst others |

# Special categories of personal data – Section 29

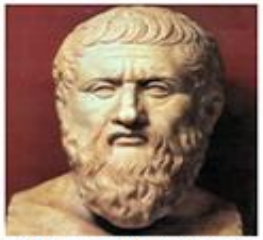
- Previously known as sensitive personal data under the DPA. It now includes “genetic data” and “biometric data” where processed “to uniquely identify a person”.
- Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.


Sexual life


Political views


Religious beliefs


Health status


Philosophical beliefs


Race, nationality

# Personal Data of child– Section 30

- Children have the same rights as adults over their personal data.
- Children merit specific protection with regard to their personal data.
- Children are less aware of the risks, consequences and safeguards and their rights in relation to the processing of personal data.
- Parental consent for children under the age of 16.
- “Reasonable efforts” by the controller to verify consent.

# Security of processing – Section 31

- Appropriate technical and organisational measures must be implemented to prevent unauthorised access to, alteration, disclosure, accidental loss and destruction of personal data.

- These measures include: pseudonymisation and encryption of the personal data; on-going reviews of security measures; redundancy and backup facilities; and regular security testing.

- The Act contains special provisions when a processor is involved such as choosing a processor that provides sufficient guarantees about its security measures and written contracts to be signed

# Security of processing – Section 31(Cntd)

## Case scenario - Pseudonymisation

- The sentence ***"Charles Spencer, born 3 April 1967, is the father of a family of four children, two boys and two girls"*** can, for instance, be pseudonymised as follows:

- "**C.S. 1967** is the father of a family of four children, two boys and two girls"; or

- "**324** is the father of a family of four children, two boys and two girls"; or

- "**YESz320l** is the father of a family of four children, two boys and two girls".

# Prior security check – Section 32

- Provides for the power of the Data Protection Commissioner to perform security checks and inspection of the security measures imposed on the controller or processor.

# Record of processing operations – Section 33

- In order to demonstrate compliance with the Act, controller and processor should maintain records of processing activities under its responsibility. These records should be made available, on request, to the Data Protection Office.

# Data Protection Impact Assessment (DPIA) – Section 34

- **When must a DPIA be performed?**
  - Where processing activities are likely to result in a high risk to the rights and freedoms of individuals by virtue of their nature, scope, context and purposes.

- Nine criteria that may help you determine whether DPIA is required in a specific case:

  (1) evaluation or scoring;
  (2) automated decision-making with legal or similar significant effect;
  (3) systematic monitoring;
  (4) sensitive data;
  (5) data processed on a large scale;
  (6) datasets that have been matched or combined;
  (7) data concerning vulnerable data subjects;
  (8) innovative use or applying technological or organisational solutions;
  (9) when the processing in itself "prevents data subjects from exercising a right or using a service or a contract".

- **It is a good practice to do a DPIA for any other major project which requires the processing of personal data.**

# Data Protection Impact Assessment (DPIA) – Section 34 (Continued)

- Examples:
  - A hospital processing its patients' genetic and health data (hospital information system).
  - The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates. (systematic monitoring and Innovative use or applying technological or organisational solutions)
  - A company monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc. (systematic monitoring)
- An online magazine using a mailing list to send a generic daily digest to its subscribers. DPIA not required in this circumstance.

# Transfer of personal data outside Mauritius – Section 36

- In case the controller or processor cannot provide proof of appropriate safeguards with respect to the protection of the personal data, or

- cannot rely on any of the exceptions provided in section 36(1),
  - (*Consent from data subject, Contract with data subject, Public interest, Legal claim, Vital interest and Legitimate interest)*

- then, according to **Section 35** of the DPA, the controller or processor must seek authorisation and consult the Data Protection Office prior to processing personal data in order to ensure compliance of the intended processing with the DPA and in particular to mitigate the risks involved for data subjects (individuals) where the controller/processor intends to transfer personal information to another country.

# Rights of Data Subjects

Sections 37 to 41

# Rights of Data Subjects

## Right of access – S37

- A data subject has the right to obtain confirmation that his/her personal data is processed and a copy of the data free of charge within one month following a written request.

## Automated individual decision making – S38

- A data subject has the right not to be subject to a measure which is based on profiling by means of automated processing.
- Can be carried out by controller uf it necessary for contract, authorised by law or based on explicit consent of the data subject.

## Rectification –S39

- A data subject has the right to obtain from controller rectification of inaccurate or incomplete personal data concerning him/her.

# Rights of Data Subjects


## Erasure – S39

- Data subject may request that his/her personal data are erasedif the continued processing of those data is not justified


## Restriction of Processing – S39

- A data subject may request that the processing of his/her personal data is restricted where the accuracy of the data is contested.

## Object – S40

- A data subject has the right to object in writing at any time the processing of personal data relating to him/her free of charge.

# Exercise of rights – Section 41

- Where a person is a minor or physically or mentally unfit, a person duly authorised (parents, guardian, legal administrator) can exercise their rights on their behalf under this part.

# Unlawful disclosure of personal data – Section 42

| | |
|---|---|
| Controller | Any controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such data has been collected shall commit an offence. |
| **Processor** | Any processor who, without lawful excuse, discloses personal data processed by him without the prior authority of the controller on whose behalf the data are being or have been processed shall commit an offence |

# Offences and Penalties – Section 43

- There are various offences and criminal penalties under this Act which, in general if committed, are sanctioned by a court of law.

- Where no specific penalty is provided, any person who does not comply or contravenes this Act shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

# Offences and Penalties – Examples

| Offences | Penalties |
|---|---|
| **Section 6:**<br>**Investigation of Complaints**<br>Any person who fails to attend a hearing or to produce a document or other material when required to do so. | Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years. |
| **Section 7:**<br>**Power to require information**<br>Any person who fails or refuses to comply with a requirement specified in a notice, or who furnishes to the Commissioner any information which he knows to be false or misleading in a material particular. | Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years. |

# Offences and Penalties – Examples

| Offences | Penalties |
|---|---|
| **Section 15: Application for registration**<br>Any controller or processor who knowingly supplies any information, during registration, which is false or misleading in a material particular. | Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years. |
| **Section 17: Change in particulars**<br>Any controller or processor who fails to notify a change in particulars. | Liable to a fine not exceeding 50, 000 rupees. |
| **Section 28: Lawful processing**<br>Any person who process personal data unlawfully. | Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years. |

# Exceptions and Restrictions

- Processing of personal data by an individual in the course of a purely personal or household activity.
- For the prevention, investigation, detection or prosecution of an offence, including the execution of a penalty.
- An objective of general public interest, including an economic or financial interest of the State.
- The protection of judicial independence and judicial proceedings.
- The protection of a data subject or the rights and freedoms of others
- Subject to section 44(4):
  - For the protection of national security, defence or public security

*A certificate under the hand of the Prime Minister certifying that the non-application of the provision is required for the purpose of safeguarding national security, defence or public security shall be conclusive evidence of that fact.*

# Certification – Section 48

- To enhance transparency and compliance with the Data Protection Act 2017, certification (Section 48) has been introduced to:
  - help controllers or processors to demonstrate accountability and compliance with the Act
  - build confidence and trust in the organisation with all stakeholders, as well as with the wider public
  - allow data subjects to quickly assess the level of data protection of relevant products and services
  - give legal certainty for cross-border data transfers

# Certification – Section 48

| | |
|---|---|
| Certification body | • **Certification will be issued by the Data Protection Office.** |
| Compulsory and Fee? | • **Certification is voluntary and free.** |
| Validity | • **Certification is valid for three years and is subject to renewal. Controllers or processors may apply for renewal of the certification before the date of its expiry.** |
| Withdrawal | • **Certifications is subject to withdrawal where the conditions for issuing the certification are no longer met.** |

# Thanks!

## Any questions?

Contact us:

Website : http://dataprotection.govmu.org

Email: dpo@govmu.org

Tel: 4600251