AN OVERVIEW OF THE DATA PROTECTION ACT 2017

Presented By:
Mrs. R. Goburdhun and Mrs. J. Haulkhory
Data Protection Officer/ Senior Data Protection Officer
29 November 2018

Agenda

- Aims of the Data Protection Act 2017 (DPA)
- Benefits of the Act
- Mapping between DPA and GDPR
- 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

Mapping between DPA and GDPR

DPA (Section)	GDPR (Article)
6 - Investigation of complaints Amicable settlement of disputes and conduct of hearings has been included.	40 - Codes of conduct (2)(k)
21- Principles relating to processing of personal data	5 - Principles relating to processing of personal data
22 - Duties of controller	24 - Responsibility of the controller
23 – Collection of personal data	13 - Information to be provided where personal data are collected from the data subject
24 - Conditions for consent	7 - Conditions for consent
25 - Notification of personal data breach	33 - Notification of a personal data breach to the supervisory authority
26 - Communication of personal data breach to data subject	34 - Communication of a personal data breach to the data subject

DPA (Section)	GDPR (Article)
28 - Lawful processing	6 - Lawfulness of processing
29 - Special categories of personal data	9 - Processing of special categories of personal data
30 - Personal data of child	8 - Conditions applicable to child's consent in relation to information society services
31 - Security of processing	28 - Processor 29 - Processing under the authority of the controller or processor 32 - Security of processing
33 - Record of processing operations	30 - Records of processing activities
34 - Data protection impact assessment	35 - Data protection impact assessment
35. Prior authorisation and consultation	36 - Prior consultation

DPA (Section)	GDPR (Article)
36 - Transfer of personal data outside Mauritius	46 - Transfers subject to appropriate safeguards 49 - Derogations for specific situations
37 - Right of access	15 - Right of access by the data subject
38 - Automated individual decision making	22- Automated individual decision-making, including profiling
39 - Rectification, erasure or restriction of processing	16 - Right to rectification 17 - Right to erasure (‘right to be forgotten’) 18 - Right to restriction of processing
40 - Right to object	21 - Right to object
44 – Exceptions and Restrictions	23 - Restrictions
48 - Certification	42 - Certification

The Data Protection Office

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 protection

Some Definitions

Section 2 - Interpretation

Basic Concepts

Personal Data

- **Names of staff, customers**
- **Dates of birth**
- **Addresses**
- **National Identity numbers**
- **Assessments data**
- **School marks**
- **Exam results**
- **Staff development reviews**

Basic Concepts

Data Subject

- **An identified or identifiable individual**
- **In particular by reference to an identifier such as a name, ID, location data, an online identifier or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity**

Basic Concepts

Processing

- **Operations performed on personal data, including by automated means.**
- **For e.g collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination**

Controller

- **A person who or public body which, alone or jointly with others**
- **Determines the purposes and means of the processing of personal data**
- **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***

Obligations on controllers and processors

Sections 21 to 33

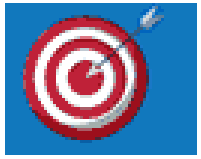
Obligations on controllers and processors

Principles relating to processing of personal data	Designate a data protection officer	Collection of personal data
Conditions for consent	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 (1)

Lawfulness, Fairness and Transparency

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



Data Minimisation

Personal data shall be adequate, relevant and not excessive in relation to the purpose.

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.

Principles relating to processing of personal data – Section 21 (2)

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

Duties of Controller – Section 22

- Must adopt policies and implement appropriate technical and organisational measures ensure and to demonstrate compliance.

Such measures includes:

- implementing appropriate data security and organisational measures;
- keeping of documentation as per section 33;
- 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).

- Data protection officer is responsible for assisting the controller or processor in monitoring the internal compliance.
- Data protection officer is not personally responsible for any non-compliance with the Act by the controller or processor.
- Responsibility of controller or processor to demonstrate compliance, regardless of how much autonomy the data protection officer is granted.
- Responsibility of the controller or processor to determine whether to have a single or different data protection officer(s) for their subsidiaries.

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.

Example of Data Protection Policy

1. About Us
2. Collection of Personal Information
3. Purpose/s of processing
4. Where do we collect personal information from?
5. Who we share your personal information with?
6. How long do we keep your personal information?
7. What are the implication if you choose not to give your personal information?
8. What automated decisions take place?
9. Use of Cookies
10. How to make a complaint?
11. How to withdraw your consent?
12. Your responsibility to let us know if your personal information is incorrect
13. What are your rights?
14. How to get a copy of your personal information?
15. What if you want us to stop using your personal information?

Conditions for Consent - Section 24

- **Consent must be freely given, specific, informed and unambiguous.**
  - *either by a statement or a clear affirmative action to signify agreement to personal data being processed*

- **Consent must be able verifiable.**

- **Consent can be withdrawn at any time.**

  Consent can be withdrawn at any time.

- When consent is not necessary for a provision of a service, it is the responsibility of controllers to determine the exceptions that apply under Section 28(1)(b).

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

Notification & Communication of personal data breach- Sections 25 & 26

- Notify the personal data breach to the Commissioner without undue delay.

- Where feasible, not later than 72 hours of becoming aware of the breach

- The controller must communicate that breach to the data subject where a personal data breach is likely to result in a high risk to the rights and freedoms of the individual,

- For e.g An officer has disclosed personal details of patients to a marketing company.

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

Special categories of personal data – Section 29

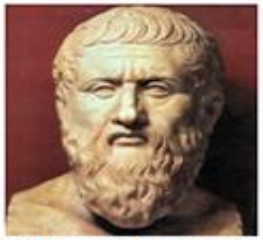
- Previously known as sensitive personal data under the DPA. It now includes “genetic data” and “biometric data” where processed “to uniquely identify a person”.
- Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection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

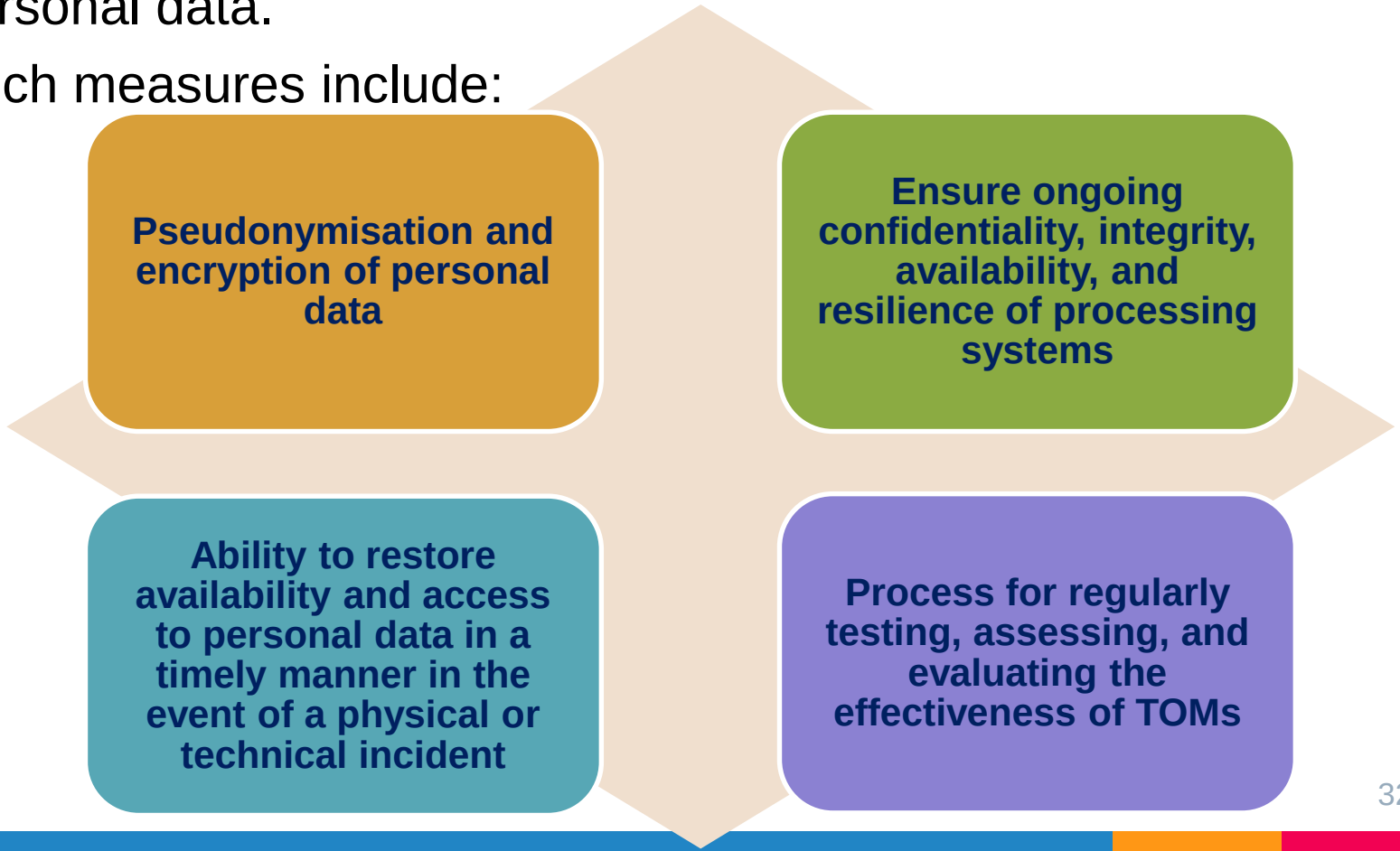

Race, nationality

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.
- Such measures include:



Security of processing – Examples

- An employee of an insurance company receives a telephone call at her workplace from someone who says he is a client, requiring information concerning his insurance contract.

- The duty to keep clients' data confidential requires that the employee apply at least minimum security measures before disclosing personal data. This could be done, for example, by offering to return the call to a telephone number documented in the client's file.

Security of processing – Section 31(Cntd)

If the controller is using the services of a processor, the controller is still responsible under the DPA for data protection and so must ensure through a written contract that the processor

acts only on instructions received from the controller and

implements appropriate security measures for protecting any personal data processed

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

The new Act requires the controller and processor to keep records of processing activities under its responsibility.

Such records must include:	
	Name and contact details of controller or processor or any representative
	Purpose of processing
	Description of categories of data subjects and personal data
	Description of categories of recipients
	Details of transfers to third countries including documenting the transfer mechanism safeguards in place.
	Retention schedules
	Description of technical and organisational security measures.

A Template is available on this office website which can be used by controller and processor to comply with this section . These records must be made available, on request, to the Data Protection Office.

Data Protection Impact Assessment (DPIA) – Section 34

A DPIA is a process that help you identify and mitigate the data protection risks of a project.

DPIA is mandatory when the processing is likely to result in a high risk for the rights and freedom of individuals, including some specified types of processing such as:	**Use systematic and extensive profiling or automated decision-making to make significant decisions about people**
	Process special category data on a large scale.
	Systematically monitor a publicly accessible place on a large scale.

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

A form and a list of criteria to evaluate high risk processing are available on this office website
http://dataprotection.govmu.org/English/Pages/default.aspx

Data Protection Impact Assessment (DPIA)

This office has developed nine criteria to help controllers and processors determine whether their processing operations are likely to present high risks.

1) Evaluation or scoring personal aspects/behaviour of people including profiling

2) Automated decision-making producing legal or similar significant effects

3) Systematic monitoring by observing, monitoring or controlling data subjects

4) Sensitive data (special categories of personal data) or data of a highly personal nature

5) Data processed on a large scale

6) Matching or combining data sets

7) Data on vulnerable persons to whom the data relates (e.g. people with mental illness, asylum seekers or elderly people, patients, children, etc.)

8) Innovative use or application of new technological or organisational solutions

9) When the processing "prevents data subjects from exercising a right or using a service or a contract"

Examples of DPIA

Example 1: An intelligent video analysis system that recognise car number plates and matches them with the national database to monitor the driving behaviour in the city

Possible relevant criteria:

1) Innovative use or application of new technological or organisational solutions
2) Data processed on a large scale
3) Systematic monitoring by observing, monitoring or controlling data subjects

Since the processing meets 3 criteria, it is considered as high risk. Therefore it is necessary to carry out a DPIA.

Example 2:

An editorial magazine which uses its mailing list to send daily newspapers to its subscribers

Possible relevant criteria: Data processed on a large scale

Since the processing meets only 1 criterion, it is considered as low risk. It is therefore not necessary to carry out a DPIA

Prior authorisation and consultation – Section 35

According to Section 35, 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 or processor cannot provide for the appropriate safeguards required for the transfer of personal data to another country.

Transfer of personal data outside Mauritius – Section 36

A controller or a processor may transfer personal data to another country where –

- **Proof of appropriate safeguards**
- **Consent from data subject**
- **Contract with data subject**
- **Public interest**
- **Legal claim**
- **Vital interest**
- **Compelling Legitimate interest**

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 if 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 erased if 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.

OTHER OFFENCES AND PENALTIES

Sections 42 and 43

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.

EXCEPTIONS AND RESTRICTIONS

Sections 44

Exceptions and Restrictions – S44

- 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

Sections 44

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