

# AN OVERVIEW OF THE DATA PROTECTION ACT 2017

**Presented By:**

Mrs. J. Haulkhory and Mrs W. Khadun

Data Protection Officer/Senior Data Protection Officer

07 March 2019

# 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)

---

Basic Concepts

---

Application of the Act

---

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**

# Basic Concepts

## Section 2 - Interpretation

# Basic Concepts



## Data Subject

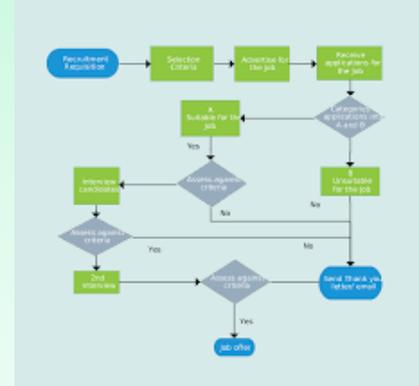
- an identified or identifiable individual (any data which can identify an individual),
- in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic,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

## Personal Data

- any information relating to a data subject



# 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.

# Basic Concepts

## 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.

# Basic Concepts of Data Protection



## Case scenario – Processor – who is he?

- **EverReady** company specialises in data processing for the administration of human resource management for other companies.
- In this function, **EverReady** is a **processor** for the other companies.
- However, **EverReady** is the **controller** of data processing operations for the purpose of fulfilling its obligations as an employer as **EverReady** processes the personal data of its own employees and non-employees.

# Application of the Data Protection Act

## Section 3

# Application of the Act (1)



**For the purposes of this Act, each Ministry or Government department will be treated as separate from any other Ministry or Government department.**

**This Act applies to the processing of personal data, wholly or partly, by automated means and to any processing otherwise than by automated means where the personal data forms part of a filing system or is intended to form part of a filing system.**

# Application of the Act (2)

**The Act applies to a controller / processor who:**



**is established in Mauritius and processes personal data in the context of that establishment; and**



**is not established in Mauritius but uses equipment in Mauritius for processing personal data, other than for the purpose of transit through Mauritius.**

# Non - Application of the Act

## The Act does not apply to:



**the exchange of information between Ministries, Government departments and public sector agencies where such exchange is required on a need-to-know basis;**



**the processing of personal data by an individual in the course of a purely personal or household activity.**

# Registration of Controllers and Processors

**Sections 14 to 20**

# Registration



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

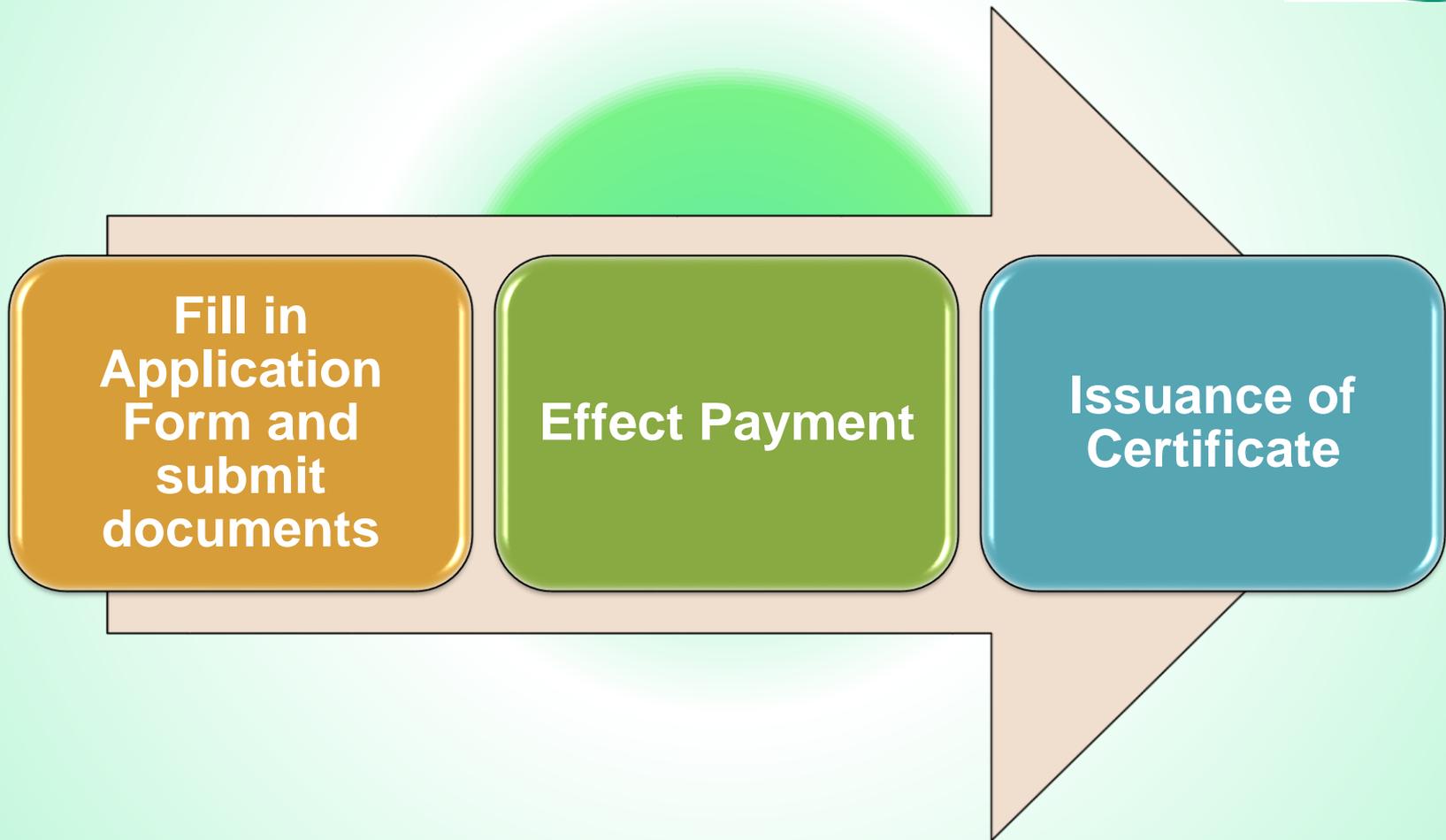
“... no person shall act as controller or processor unless he or it is registered with the Commissioner...”, Part III, Section 14

Validity of Registration Certificate: 3 years

Renewal: 3 months prior to expiry

Notification of change in particulars within 14 days

# Registration Procedure



# Registration



Can a management company (MC) register on behalf of global business entity? **YES**, provided that:

*All personal data of the global business entity 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 entities and provide a list at Registration and Renewal.*

The global business entity must register separately in case other personal data are being processed at its end, outside the control of the management company.

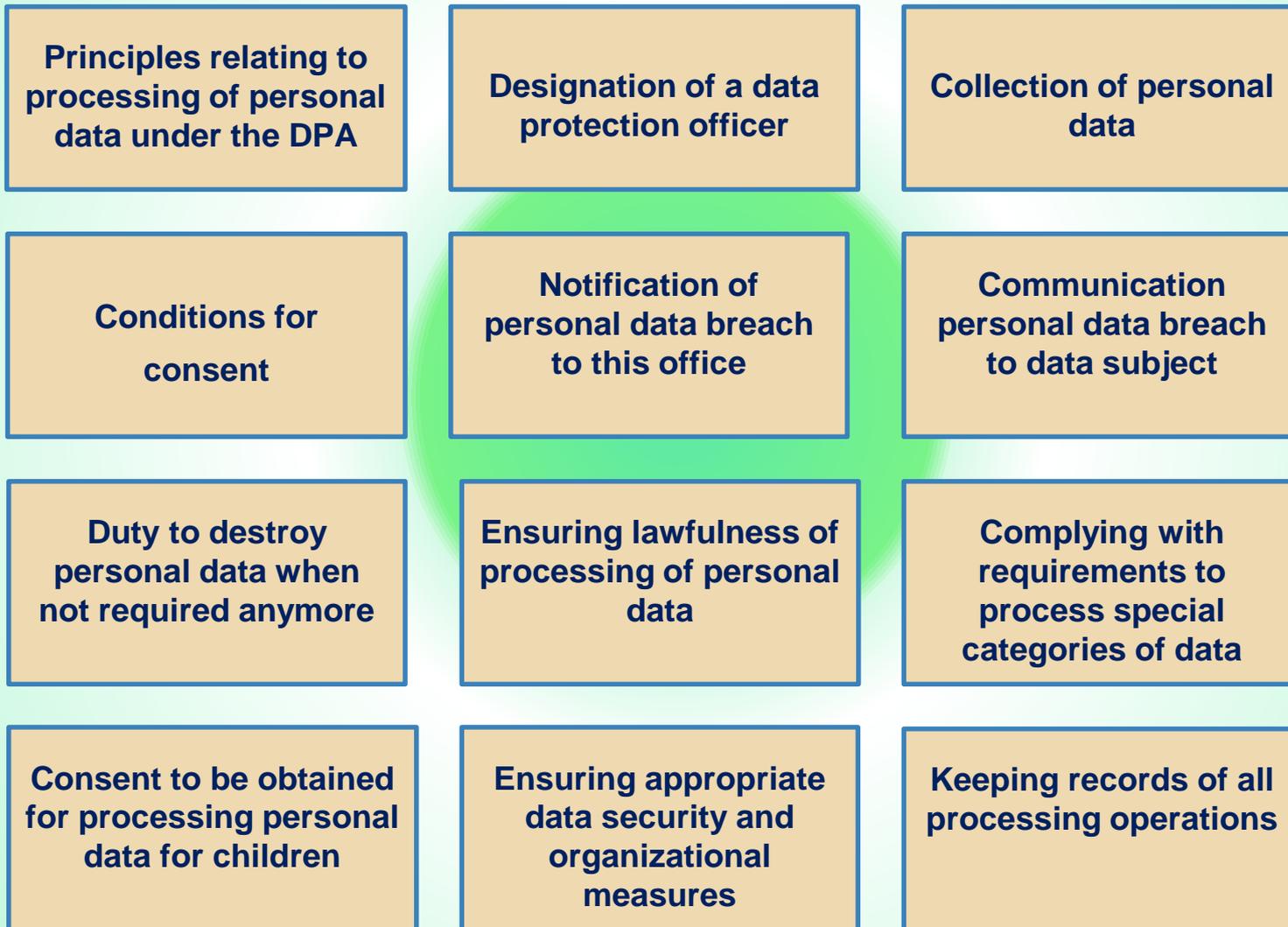


# Obligations on controllers and processors

Sections 21 to 33



# Obligations on controllers and processors are related to:-



# Principles relating to Processing of personal data (1)

## Lawfulness, fairness and transparency

- *Employer can disclose salary details of employees to tax authorities, without consent.*

## Purpose limitation

*Explicit, specified and legitimate purposes and not processed in a way incompatible with the purposes*

- *A General Practitioner cannot disclose patients details to his wife who owns a travel agency.*

## Data minimisation

*Adequate, relevant and limited to what is necessary, in relation to the purposes*

- *Office workers will not be queried about their health conditions compared to a field worker.*

# Principles relating to Processing of personal data (2)

## **Accuracy:**

*Accurate and, where necessary, up-to-date. Erasure and rectification without delay.*

- ***A mis-diagnosis of a medical condition is still kept as it is relevant for the treatment given to the patient or to additional health problems.***

## **Storage limitation:**

*Storage of personal data permitting Identification of data subjects for no longer than necessary*

- ***Deletion of details for staff who have left the organisation.***

## **Data subjects' rights:**

*Processing in accordance with data subject's rights*

- ***Rectification of an incorrect address***

# TO-DO List

**Review internal policies and audit procedures**

```
graph TD; A[Review internal policies and audit procedures] --> B[Update these policies and procedures where necessary to ensure that they are consistent with the revised principles.]; B --> C[Provide appropriate training to ensure that the business is thinking about data protection issues at all levels.];
```

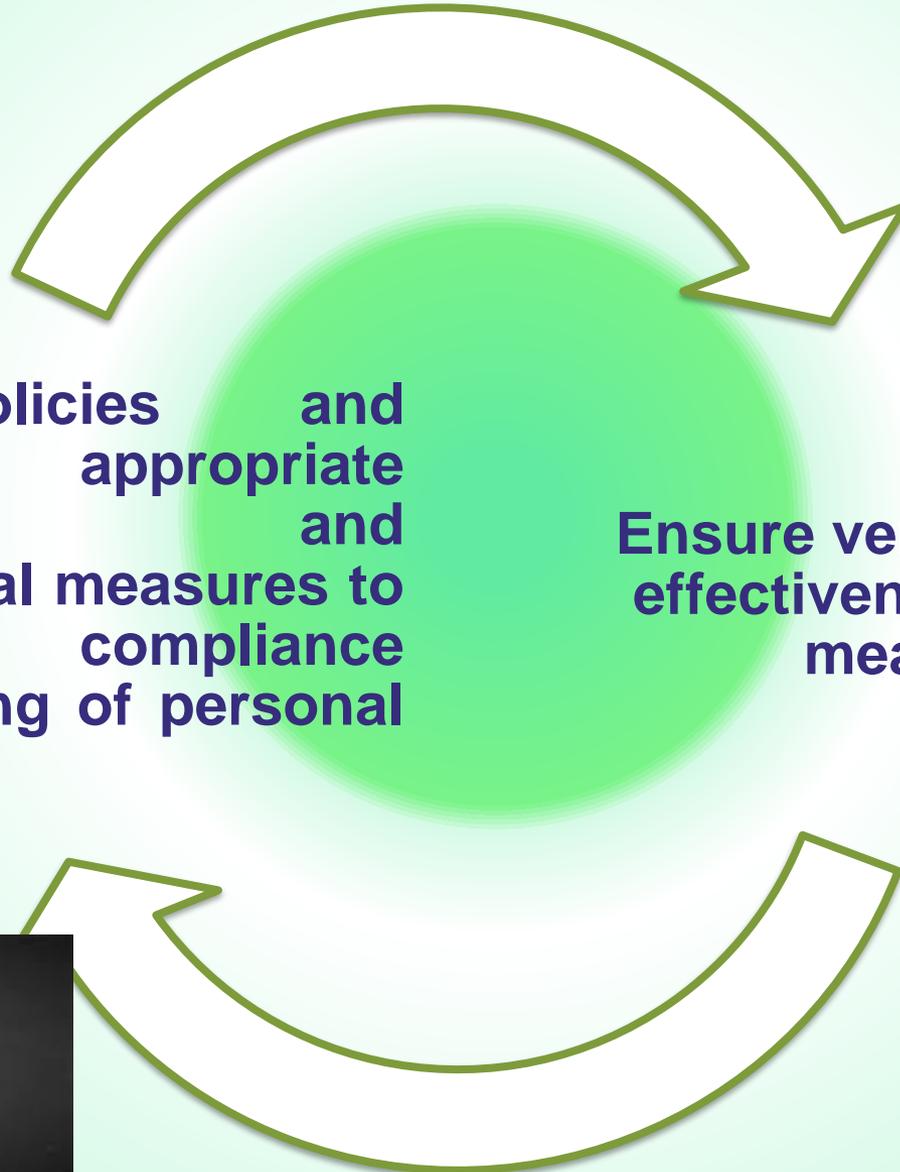
**Update these policies and procedures where necessary to ensure that they are consistent with the revised principles.**

**Provide appropriate training to ensure that the business is thinking about data protection issues at all levels.**

# Duties of Controllers – Section 22

Adopt policies and implement appropriate technical and organisational measures to demonstrate compliance for processing of personal data

Ensure verification and effectiveness of these measures



# Duties of Controllers – Section 22

Measures include:

Implementing appropriate data security and organisational measures

Keeping of documentation as per section 33

Performing data protection impact assessments as per section 34

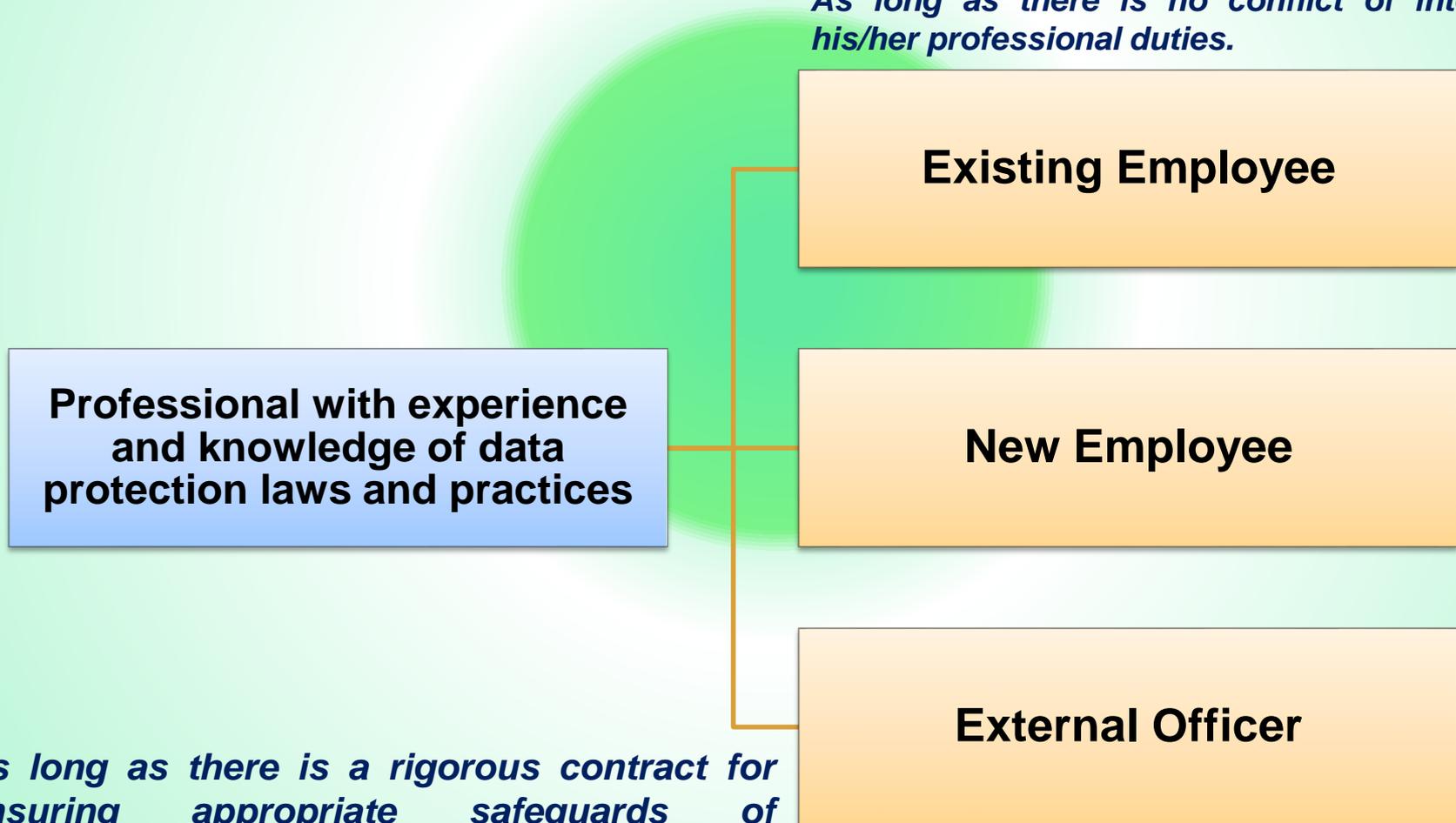
Complying with requirements of prior authorization and consultation as per section 35

Designating an officer responsible for data protection

# Who can be a Data Protection Officer(DPO)?

- **Mandatory appointment of an officer responsible for data protection compliance issues.**

*As long as there is no conflict of interest with his/her professional duties.*



*As long as there is a rigorous contract for ensuring appropriate safeguards of confidentiality*

# Roles of Data Protection Officer (DPO)

**Inform and advise the controller/processor and the employees about the obligations to comply with the DPA 2017**

**Monitor compliance with the DPA 2017**

**Advise on data protection impact assessments**

**Train staff**

**Conduct internal audits**

**Be the point of contact for the Data Protection Office and for individuals whose data are processed**

# Responsibility of Controllers and Processors and the DPO:

## Controller or processor:



**To take responsibility for any non-compliance with the Act.**



**To demonstrate compliance, regardless of how much autonomy the data protection officer is granted.**



**To determine whether to have a single or different data protection officer(s) for subsidiaries.**

# Collection of personal data – Section 23

**It is done for a lawful purpose connected with a function or activity of the controller; and**

**The collection of the data is necessary for that purpose.**



# Collection of personal data – Section 23

## 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 amongst others and the consequences of such processing.

# Example of a Data Protection Information Notification

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 implications 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 to the Commissioner?
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. Where the transfer of personal data abroad is being effected wherever applicable

# 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 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.**

- ▷ **Example: 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 must

- Destroy the data as soon as is reasonably practicable and
- Notify any processor holding the data.

Any processor who receives such a notification from the controller must, as soon as is reasonably practicable,

- Destroy the data specified by the controller.

Retention Period

- Must 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

**Personal data relating to: for e.g**

**physical or mental health, racial or ethnic origin, political opinion, religious or philosophical beliefs, physical or mental health or condition**

**Now includes “genetic data” and “biometric data”.**

**Merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.**



# 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:

**Pseudonymisation and encryption of personal data**

**Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems**

**Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident**

**Process for regularly testing, assessing, and evaluating the effectiveness of TOMs**

# 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.

---

**Template is available on the website.**

# 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.**

---

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 the website.**

# 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”

# 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 the below conditions have been met –

**There are proof of appropriate safeguards**

**Or Explicit consent from data subject**

**Or Contract with data subject**

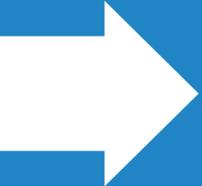
**Or Public interest as provided by law**

**Or Legal claims**

**Or Vital interests of the data subject**

**Or Compelling Legitimate interests of the controllers or processors**

**Or Public register – information contained in which is required to be transfer**



# 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.



## Rectification –S39

- A data subject has the right to obtain from controller rectification of inaccurate or incomplete personal data concerning him/her without undue delay.

# Rights of Data Subjects



## Erasure – S39

- Data subject may request that his/her personal data are erased without undue delay 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 or he/she requires it for a legal claim amongst others.



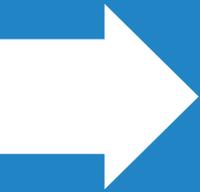
## Object – S40

- 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

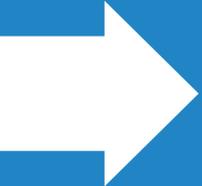
**Any processor who, without lawful excuse, discloses personal data processed by him without the prior authority of the controller on whose behalf the data are being or have been processed shall commit an offence.**

---

# 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.**

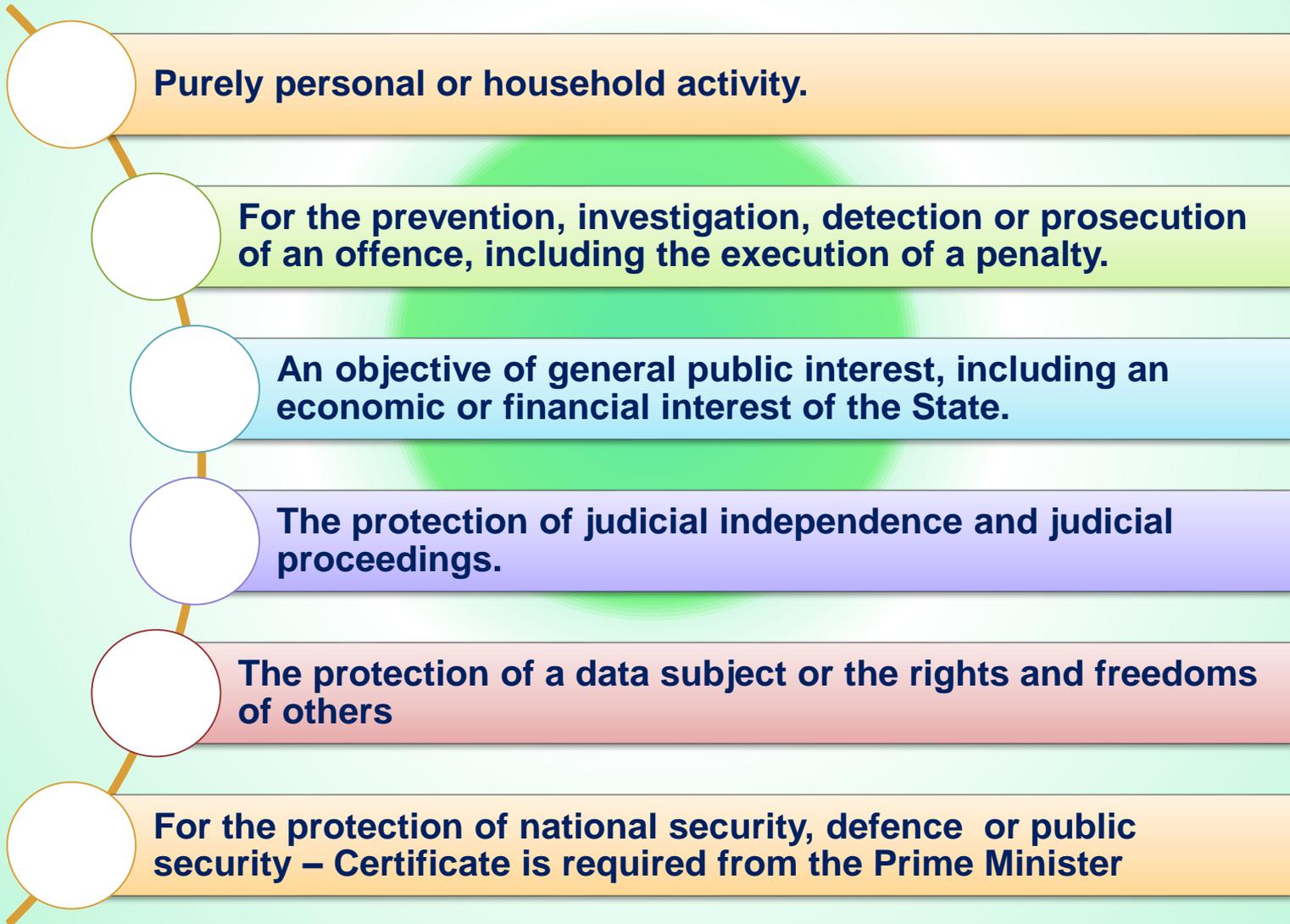
**Where no specific penalty is provided, any person who does not comply or contravenes this Act shall, on conviction, be liable to a fine not exceeding **200,000 rupees** and to imprisonment for a term not exceeding **5 years**.**

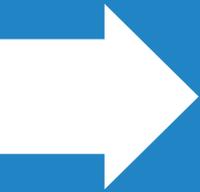


# EXCEPTIONS AND RESTRICTIONS

Sections 44

# Exceptions and Restrictions – S44





# CERTIFICATIONS

Section 48

# Certification – Section 48

- ▷ To enhance transparency and compliance with the Data Protection Act 2017, certification

- **helps controllers or processors to demonstrate accountability and compliance with the Act**

- **builds confidence and trust in the organisation with all stakeholders, as well as with the wider public**

- **allows data subjects to quickly assess the level of data protection of relevant products and services**

- **gives 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

- Certification is subject to withdrawal where the conditions for issuing the certification are no longer met.

# Thank you

## Any questions?

**Contact us:**

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

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

**Tel: 4600251**