



# **A Legal Overview of the Data Protection Act 2017**

**By:  
Mrs D. Madhub  
Data Protection Commissioner  
06.02.2018**

# Overview

- The Data Protection Act 2017
- Aim of the Act
- Major changes brought in the new Act
- Key Definitions
- New Definitions
- The Data Protection Office
- Registration of controllers and processors
- Obligations on controllers and processors
- Rights of Data Subjects
- Offences and penalties
- Exceptions and restrictions
- Certification
- Benefits of the new Act

# The Data Protection Act 2017

- Replaces the Data Protection Act 2004.
- Passed on 8<sup>th</sup> December 2017 at the National Assembly and presidential assented on 23<sup>rd</sup> December 2017.
- Came into force on 15 January 2018.

# Aim of the Act

- To strengthen the control and personal autonomy of data subjects (individuals) over their personal data.
- To be in line with current relevant international standards, in particular the European Union's General Data Protection Regulation (GDPR) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

# Aim of the Act (Continued)

- To simplify the regulatory environment for business in our digital economy.
- To promote the safe transfer of personal data to and from foreign jurisdictions, given the diversification, intensification and globalisation of data processing and personal data flows.

# Major changes brought in the new Act

- Existing data protection principles and key definitions such as consent and personal data have been modernised.
- Introduction of new concepts such as:
  - ✓ Data Protection Impact Assessments (DPIA);
  - ✓ Notification by controllers of personal data breaches to the Data Protection Office and data subjects;
  - ✓ Voluntary certification mechanisms and data protection seals & marks for controllers; and
  - ✓ Rights to object to automated individual decision-making including profiling.

# Major changes brought in the new Act (Continued)

- Simplifying:
  - ✓ the registration / renewal process of controllers and processors;
  - ✓ the complaints' mechanism and the procedures related to hearings conducted by the Data Protection Office;
  - ✓ the ease of business, in particular in terms of free flow of data from EU or other parts of the world to Mauritius.

# Key Definitions

- **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.

- **Data Subject**

An identified or identifiable 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.

# New Definitions

- The following have been defined under the “Interpretation” section of the Data Protection Act 2017:
  - Biometric data
  - Encryption
  - Genetic data
  - Physical or mental health
  - Personal data breach
  - Profiling
  - Pseudonymisation

# The Data Protection Office

- A public office which acts with **complete independence and impartiality.**
- It is not subject to the control or direction of any other person or authority in the discharge of its functions.
- The head of the Office is the Data Protection Commissioner.

# The Data Protection Office

## (Continued)

### **Powers of the Data Protection Commissioner**

- Part II of the Act deals with the powers of the Commissioner to enable her to carry out her functions under the Act.
- For instance, the Commissioner now has enhanced powers with regard to the handling of complaints, namely the amicable resolution of disputes whenever possible.

# Registration of controllers and processors

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

- *PART III of the Act deals with the registration of controllers and processors.*
- *Section 14 provides: “No person shall act as controller or processor unless he or it is registered with the Commissioner”.*
- *The registration will be for a period not exceeding 3 years and on the expiry of such period, the relevant entry will be cancelled unless the registration is renewed.*

# Obligations on controllers and processors

- **Principles relating to processing of personal data (Section 21)**
  - *Controllers/processors need to ensure that processing of personal data is lawful, fair, transparent, adequate, relevant, accurate, kept for as long as required and proportionate to the purposes for which it is being processed.*
- **Duties of Controller (Section 22)**
  - *The controller must ensure all personal data is processed in compliance with the Act, and be able to demonstrate compliance through a series of measures including implementing appropriate data security and organisational measures, keeping of documentation, designating a data protection officer, amongst others.*

# Obligations on controllers and processors (Continued)

## Collection of personal data (Section 23)

- *The principles of fair and transparent processing require the controller to provide information about itself, the purposes of processing and explain to data subjects how their personal data will be processed (e.g. existence of automated decision-making including profiling), the consequences of such processing and their individual rights (e.g. existence of the right to withdraw consent).*

## • Conditions for consent (Section 24)

- *Consent must be freely given, specific, informed and unambiguous.*
- *The controller must be able to supply evidence that consent has been obtained (verifiable).*
- *Consent can be withdrawn at any time.*



Explicit consent and  
lawfulness of processing

# Obligations on controllers and processors (Continued)

- **Notification of a personal data breach to the Commission (Section 25)**  *– As soon as the controller becomes aware that a breach has occurred, the controller must notify the breach to the Data Protection Office without undue delay and, where feasible, not later than 72 hours after having become aware of it.*
- **Communication of a personal data breach to the data subject (Section 26)** *– Controller should communicate to the data subject a personal data breach, without undue delay, where that breach is likely to result in a high risk to the rights and freedoms of the individual in order to allow him or her to take the necessary precautions (e.g., by replacing credit cards if the data subject's card details have been leaked).*

# Obligations on controllers and processors (Continued)

- **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.*
- **Lawful processing(Section 28)**
  - *The Act lays down the conditions for legal basis required for processing such as obtaining the consent of the data subject before any processing.*

# Obligations on controllers and processors (Continued)

- **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.*

# Obligations on controllers and processors (Continued)

- **Personal data of child (Section 30)**

- *Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.*
- *Parental consent must be obtained for children under the age of 16.*
- *The controller is also required to make “reasonable efforts” to verify that consent has been given by the holder of parental responsibility in light of available technology*

# Obligations on controllers and processors (Continued)

- **Security of processing (Section 31)**

- *Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate security (technical) or organisational measures.*
- *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.*

# Obligations on controllers and processors (Continued)

- **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.*

# Obligations on controllers and processors (Continued)

- **Data Protection Impact Assessment (Section 34)**

- *In order to enhance compliance with this Act where processing operations are likely to result in a high risk to the rights and freedoms of individuals, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk.*
- *Such processing operations may include a bank that screens its customers against a credit reference database, or a medical company offering genetic tests directly to consumers in order to assess and predict disease / health risks, or a new data processing technology is being introduced, or a company building behavioural or marketing profiles based on usage or navigation on its website.*

# Obligations on controllers and processors (Continued)

- **Prior authorisation and consultation (Section 35)**

- *Where a controller or processor does not provide for appropriate safeguards for the transfer of personal data to another country, the controller or processor must obtain authorisation from the Office before processing the personal data.*
- *Where a data protection impact assessment indicates that processing operations involve high risks, the controller or processor must consult the Office prior to processing.*
- *Example of when authorisation and consultation should be sought: When processing health data on a large scale as it is considered as likely to result in a high risk.*

# Obligations on controllers and processors (Continued)

- **Transfer of personal data outside Mauritius (Section 36)**



Data transfers

- *Controller or processor must provide proof of appropriate safeguards to the Commissioner before transferring personal data to another country whenever required.*
- *In the absence of appropriate safeguards, the data subject should provide his consent (explicit) after having been informed of the possible risks of the transfer.*
- *Section 36 (1) (c) provides other conditions where transfer can be made for example for the conclusion of contract, public interest requirements amongst others.*

# Rights of Data Subjects

- Part VII of the Act stipulates the rights of data subjects;
- The Act has enhanced the rights to access, rectify, erase and restrict processing of personal data;
- New provisions have been made to cater for decisions which are based on automated processing and the right to object to the processing of personal data by individuals.

# Rights of Data Subjects (Continued)

- **Right of access (Section 37)**

- *The Act obliges controllers to provide free of charge to data subjects with access to their personal data and to be provided a copy of their data within one month following a written request.*

- **Automated individual decision making (Section 38)**

- *Data subjects now have the right not to be subject to a decision based solely on automated processing which produces legal effects concerning him or which significantly affect them (including profiling).*

# Rights of Data Subjects (Continued)

- **Rectification, erasure or restriction of processing (Section 39)**
  - *Data subjects have the right to:*
    - ✓ *rectify inaccurate personal data;*
    - ✓ *delete their personal data if the continued processing of those data is not justified;*
    - ✓ *withdraw their consent;*
    - ✓ *restrict the processing of their personal data (meaning that the data may only be held by the controller, and may only be used for limited purposes).*

# Rights of Data Subjects (Continued)

- **Right to object (Section 40)**

- *Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data.*
- *Following the individual's objection, the burden falls on the controller to establish why it should, nonetheless, be able to process the personal data.*

- **Exercise of rights (Section 41)**

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

# Rights of Data Subjects (Continued)

- Controllers must (on written request):
  - ✓ confirm if they process an individual's personal data;
  - ✓ provide a copy of the data;
  - ✓ provide supporting explanatory materials.
- Access rights are intended to allow individuals to:
  - ✓ check the lawfulness of processing;
  - ✓ have a copy of their personal data.

Note: the rights should not adversely affect the rights of others.

# Offences and Penalties

- There are various offences and criminal penalties under this Act which, in general if committed, is 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 (Continued)

**For e.g.:**

Offences	Penalties
<p><b>Section 6: Investigation of Complaints</b> Any person who fails to attend a hearing or to produce a document or other material when required to do so.</p>	<p>Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.</p>
<p><b>Section 7: Power to require information</b> 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.</p>	<p>Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.</p>

# Offences and Penalties (Continued)

**For e.g.:**

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

# Exceptions and Restrictions

- The processing of personal data by an individual in the course of a purely personal or household activity is exempted from the Data Protection Act.
- Sections 3(4) and 44 depict the types of processing of personal data which are exempted from this Act.
- In general, processing of personal data constitutes a necessary and proportionate measure in a democratic society for the following reasons:
  - ✓ the protection of national security, defence or public security;
  - ✓ the prevention, investigation, detection or prosecution of an offence, including the execution of a penalty;

# Exceptions and Restrictions

## (Continued)

- ..... *necessary and proportionate measure in a democratic society for the following reasons* **(Continued)**:
  - ✓ 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.

# Exceptions and Restrictions

## (Continued)

- The processing of personal data for the purpose of historical, statistical or scientific research is exempted provided that the security and organisational measures are implemented to protect the rights and freedoms of data subjects involved.
- The controller or processor has a duty to secure the data to prevent its unlawful disclosure. For instance, appropriate technology such as pseudonymisation or encryption can be used to secure the data.

# Certification

- 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 (Continued)

- The Data Protection Office encourages the establishment of data protection certification mechanisms, seals and marks.
- Certifications are voluntary but enable controllers and processors to demonstrate compliance with the Data Protection Act.
- Controllers or processors wishing to be certified must apply for certification with the Data Protection Office.
- Certificates will be issued by the Data Protection Office.
- Certifications will be valid for three years and are subject to renewal.

# Benefits of the new Act

- Increased accountability of controllers will make organisations implement controlled business processes resulting in better organisation, greater productivity and efficiency, and higher level of security.
  - ✓ Being compliant will also help organisations to gain and strengthen customer trust, confidence and loyalty.
- Enhanced data subjects' rights will give individuals greater control over their personal data.
- The risk of data breaches will be minimised.

# Benefits of the new Act (Continued)

- The legal and practical certainty for economic operators and public authorities will be reinforced.
- The new data protection framework will significantly improve the digital legal landscape to respond to the new EU requirements for adequacy, thereby attracting foreign investors.
- Certified organisations are recognised as providing adequate privacy protection thus giving legal certainty for cross-border data transfers.

**Thank You**

