Data Protection in Mauritius:

Challenges and Opportunities for law practitioners

Presented By:

Mrs Drudeisha MADHUB

Data Protection Commissioner

26 July 2018

Institute for Judicial and Legal Studies

OVERVIEW

- INTRODUCTION
- VISION & MISSION
- THE DATA PROTECTION ACT 2017 (DPA)
- AIMS OF THE ACT
- MAJOR CHANGES
- BENEFITS
- KEY DEFINITIONS
- NEW DEFINITIONS
- DATA PROTECTION OFFICE
- FUNCTIONS OF THE DATA PROTECTION OFFICE
- REGISTRATION OF CONTROLLERS AND PROCESSORS
- PRINCIPLES OF THE DPA
- OBLIGATIONS ON CONTROLLERS AND PROCESSORS
- PROCESSING OPERATIONS LIKELY TO PRESENT RISK
- TRANSFER OF PERSONAL DATA ABROAD
- RIGHTS OF DATA SUBJECTS
- OFFENCES AND PENALTIES
- EXCEPTIONS AND RESTRICTIONS
- CERTIFICATION

Introduction

- Privacy is a fundamental right, essential to autonomy and protection of human dignity.
- Data protection concerns the protection of the personal data of living individuals.
- Links between data protection and privacy indicate that data protection is linked to private life and the right to decide on whom the data related to private life are shared with and how they are shared.
- Data protection's importance has certainly increased due to technology.

Vision & Mission

Vision

- A society where Data Protection is understood and practiced by all.

- The right to privacy and data protection is primordial to the sanctity of any modern democracy.

- The adoption of clear procedures for the collection and use of personal data in a responsible, secure, fair and lawful manner by all data controllers and data processors.

Mission

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

AIMS OF THE ACT

- 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.

MAJOR CHANGES

- Existing data protection principles
- Key definitions such as consent and personal data have been modernised
- Introduction of new concepts such as:
  - Data Protection Impact Assessments (DPIA);
  - Notification and Communication of personal data breaches to the Data Protection Office and data subjects respectively
  - Voluntary certification mechanisms
  - Rights to object to automated individual decision-making, including profiling

MAJOR CHANGES

Simplifying:

- the registration / renewal process
- the complaints' mechanism and the procedures of the 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.

BENEFITS

- Increased accountability of controllers
- 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

DPO

- 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.

FUNCTIONS OF DPO

I • Ensure compliance with the 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 OTHER supervisory authorities

VIII Research on data processing and computer technology

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.

- **Personal Data**

  Any data that refers to a data subject.

Example: Personal Data

A supervisor's assessment of an employee's work performance, stored in the employee's personnel file, is personal data about the employee. This is the case even though it may just reflect, in part or whole, the superior's personal opinion, such as: "the employee is not dedicated to their work" – and not hard facts, such as: "the employee has been absent from work for five weeks during the last six months".

Case: Controller

Google Spain was brought by a Spanish citizen who wanted to have an old newspaper report on his financial history removed from Google. The CJEU was asked whether Google, as the operator of a search engine, was the 'controller' of the data within the meaning of Article 2 (d) of the Data Protection Directive.

The CJEU considered a broad definition of the notion 'controller' to ensure "effective and complete protection of data subjects".

The CJEU found that the search engine operator determined the purposes and means of the activity and that it rendered data loaded on internet pages by publishers of websites accessible to any internet user who carries out a search on the basis of the data subject's name. Therefore, the CJEU determined that Google can be regarded as the 'controller'.

CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014

Example: Processor

The Everready company specialises in data processing for the administration of human resource data for other companies.

In this function, Everready is a processor. Where Everready processes the data of its own employees.

However, it is the controller of data processing operations for the purpose of fulfilling its obligations as an employer.

Case: Personal Data

In Breyer v. Bundesrepublik Deutschland, the CJEU considered the notion of indirect identifiability of data subjects. The case dealt with dynamic IP addresses, which change every time a new connection is made to the internet. The websites run by federal German institutions registered and stored dynamic IP addresses to prevent cyber-attacks and to initiate criminal proceedings where needed.

Only the internet service provider that Mr Breyer used had the additional information needed to identify him. The CJEU considered that a dynamic IP address, which an online media services provider registers when a person accesses a website that the provider has made accessible to the public, constitutes personal data where only a third party – the internet service provider in this case – has the additional data necessary to identify the person. It held that "it is not required that all information enabling the identification of the data subject must be held in the hands of one person" for information to constitute personal data. Users of a dynamic IP address registered by an internet service provider may be identified in certain situations, for instance within the framework of criminal proceedings in the event of cyber-attacks, with the assistance of other persons. According to the CJEU, when the provider "has the legal means which enable it to identify the data subject with additional data which the internet provider has about that person", this constitutes "a means likely reasonable to be used to identify the data subject". Therefore, such data are considered personal data.

CJEU, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, 19 October 2016, para. 43

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
  - Additional information is required to identify the data subject.
  - The additional information must be kept separately and subjected to security measures.

Example: Pseudonym

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".

REGISTRATION

"... 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**
- **Cancellation or variation of terms of Registration Certificate.**
- ***Section 19,***
    i. **False and Misleading**
    ii. **In Breach of DPA or the certificate**

OBLIGATIONS OF PROCESSORS AND CONTROLLERS

- Collection of personal data for lawful purpose(s)
- Bear the burden of proof for consent prior to processing
- Notify and communicate personal data breach
- Ensure appropriate data security and organisational measures
- Duty to destroy personal data
- Ensure lawfulness of processing of personal data
- Keep record of all processing operations
- Comply with requirements to process special category of data
- Consent for processing personal data for children
- Perform a data protection impact assessment
- Comply with req. of prior authorisation or consultation from DPO
- Designate a data protection officer

PRINCIPLES OF THE DPA

Lawfulness, Fairness, Transparency
Explicit, Specified, Legitimate Purpose(s)
Adequate, Relevant, Limited to what is necessary
Accurate, Up-to-date
Storage Limitation – Data Subjects identified for no longer than necessary
In accordance with the rights of the data subjects

Example: Fair Processing

A university research department conducts an experiment analysing changes of mood on 50 subjects. These are required to register in an electronic file their thoughts every hour, at a given time.

The 50 persons gave their consent for this particular project, and this specific use of the data by the university. The research department soon discovers that electronically logging thoughts would be very useful for another project focused on mental health, under the coordination of another team.

Even though the university, as controller, could have used the same data for the work of another team without further steps to ensure lawfulness of processing that data, given that the purposes are compatible, the university informed the subjects and asked for new consent, following its research ethics code and the principle of fair processing.

Case: Transparency

In the case of Haralambie v. Romania, the applicant was only granted access to the information held on him by the secret service organisation five years after his request.

The ECtHR reiterated that individuals who were the subject of personal files held by public authorities had a vital interest in being able to access them.

The authorities had a duty to provide an effective procedure for obtaining access to such information. The ECtHR considered that neither the quantity of the files transmitted nor shortcomings in the archive system justified a delay of five years in granting the applicant's request for access to his files. The authorities had not provided the applicant with an effective and accessible procedure to enable him to obtain access to his personal files within a reasonable time. The Court concluded that there had been a violation of Article 8 of the ECHR.

ECtHR, Haralambie v. Romania, No. 21737/03, 27 October 2009

Example: Purpose Limitation

An airline collects data from its passengers to make bookings to operate the flight properly. The airline will need data on: passengers' seat numbers; special physical limitations, such as wheelchair needs; and special food requirements, such as kosher or halal food.

If airlines are asked to transmit these data, which are contained in the Passenger Name Record, to the immigration authorities at the port of landing, these data are then being used for immigration control purposes, which differ from the initial data collection purpose.

Transmission of these data to an immigration authority will therefore require a new and separate legal basis.

Case: Storage Limitation

In S. and Marper,304 the ECtHR ruled that indefinite retention of the fingerprints, cell samples and DNA profiles of the two applicants was disproportionate and unnecessary in a democratic society, considering that the criminal proceedings against both applicants had been terminated by an acquittal and a discontinuance, respectively.

ECtHR, S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 4 December 2008

DUTIES OF CONTROLLER

Adopt policies

Implement appropriate technical and organisational measures

Demonstrate compliance with the DPA

CONDITIONS FOR CONSENT

Freely given, specific, informed, unambiguous verifiable

Consent can be withdrawn at any time.

To take into account whether, inter alia, the performance of a contract, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract

Example: Consent

A customer agrees to receivie promotional mail to an address that he or she provides to a controller.

Should the customer withdraw consent, the controller must immediately stop sending promotional mail.

No punitive consequences such as fees should be imposed. The withdrawal however is exercised for the future, and does not have retroactive effect.

The period in which the customer's personal data was processed lawfully – because of the customer's consent – had been legitimate. The withdrawal prevents any further processing of these data, unless such processing is in accordance with the right to erasure.

NOTIFICATION & COMMUNICATION OF PERSONAL DATA BREACH

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 the breach to the data subject.

DUTY TO DESTROY PERSONAL DATA

Every controller must destroy the data as soon as is reasonably practicable.

Notify any processor holding the data, who must destroy the data specified by the controller as soon as is reasonably practicable.

LAWFUL PROCESSING

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 protect the vital interests, amongst others

Example: Lawful Processing

Employers collect and process data about their employees, including information relating to their salaries. Their employment agreements provide the legal ground for legitimately doing so. Employers will have to forward their staff's salary data to the tax authorities. This transmission of data will also be 'processing' under the meaning of this term in Modernised Convention 108 and in the GDPR and the DPA.

The legal ground for such disclosure, however, is not the employment agreements. There must be an additional legal basis for the processing operations which result in employer's transmitting salary data to the tax authorities. This legal basis is usually to be found in the provisions of national tax laws. Without such provisions – and in the absence of any other legitimate ground for processing – this transmission of personal data would be unlawful processing.

SPECIAL CATEGORIES OF PERSONAL DATA

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

Case: Special Category of personal data

Bodil Lindqvist concerned the reference to different persons by name or by other means, such as their telephone number or information on their hobbies, on an internet page.

The CJEU stated that "reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health".

CJEU, C-101/01, Criminal proceedings against Bodil Lindqvist, 6 November 2003

PERSONAL DATA OF CHILD

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.

"Reasonable efforts" to verify that consent has been given by the holder of parental responsibility in light of available technology

SECURITY OF PROCESSING

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

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

Example: Security

Social networking sites and email providers make it possible for users to add an extra layer of data security to the services they provide through the introduction of two-tier authentication. In addition to entering a personal password, users must complete a second sign-in to enter their personal account.

The latter could be, for instance, the entry of a security code sent to the mobile number connected to the personal account. In this way, two-step verification provides better protection of personal information against unauthorised access to personal accounts via hacking.

PRIOR SECURITY CHECK

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

Controller and processor should maintain records of processing activities under its responsibility.

Records to be made available, on request, to the Data Protection Office.

RECORD OF PROCESSING OPERATIONS

Controller and processor should maintain records of processing activities under its responsibility.

Records to be made available, on request, to the Data Protection Office.

DATA PROTECTION IMPACT ASSESSMENT:

Process to help identify and mitigate the data protection risks of a project

Mandatory when the processing is likely to result in a high risk for the rights and freedom of individuals, including :

- Use systematic and extensive profiling or automated decision-making
- 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.

DATA PROTECTION IMPACT ASSESSMENT MUST:

- Describe the nature, scope, context and purposes of the processing
- Check that the processing is necessary for and proportionate to the purposes
- Identify and assess risks to individuals (by considering their likelihood and severity)
- Identify any measures to address(eliminate or reduce) those risks

PRIOR AUTHORISATION AND CONSULTATION

To ensure compliance of the intended processing with the DPA

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

If one of the conditions are met:

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

RIGHTS OF DATA SUBJECT

Right of Access

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

A data subject has the right not to be subject to a measure which is based on profiling by means of automated processing.

Rectification

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

RIGHTS OF DATA SUBJECT

Where a person is a minor or a physically or mentally unfit, a person duly authorised (parent, guardian, legal administrator) can exercise his/her rights under the DPA

Erasure

Data subject may request that his/her personal data are erased if the continued processing of those data is not justified.

Restriction of processing

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

Right to object

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.

Case: Rights of data subjects

In Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Mr González requested the removal or alteration of a link between his name in the Google search engine and two newspaper pages announcing a real-estate auction for the recovery of social security debts. The CJEU stated that "in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results".

The CJEU concluded that such actions constitute 'processing', "regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data".

CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014

Example: Rectification

Example 1: Case for non-rectification

A medical record of an operation **must not be** changed, in other words 'updated', even if findings mentioned in the record later on turn out to have been wrong. In such circumstances, only additions to the remarks in the record may be made, as long as they are clearly marked as contributions made at a later stage.

Example 2:

If somebody wants to conclude a credit contract with a banking institution, the bank will usually check the creditworthiness of the prospective customer.

For this purpose, there are special databases available containing data on the credit history of private individuals. If such a database provides incorrect or outdated data about an individual, this person may suffer negative effects. Controllers of such databases must therefore make special efforts to follow the principle of accuracy.

Case : Erasure

In Brunet v. France,564 the applicants denounced the storage of their personal information in a police database which contained information on convicted persons, accused persons and victims. Even though the criminal proceedings against the applicant had been discontinued, his details appeared in the database.

The ECtHR held that there had been a violation of Article 8 of the ECHR. In reaching its conclusion, the Court considered that, in practice, there was no possibility for the applicant to have his personal data deleted from the database.

The ECtHR also considered the nature of the information included in the database and deemed that it was intrusive to the applicant's privacy, as it contained details of his identity and personality. In addition, it found that the retention period for personal records in the database, which amounted to 20 years, was excessively lengthy, particularly since no court had ever convicted the applicant.

ECtHR, *Brunet v. France*, No. 21010/10, 18 September 2014

UNLAWFUL DISCLOSURE OF PERSONAL DATA

It is an offence if

Any controller, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such data has been collected

Any processor, 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

NOTIFICATION & COMMUNICATION OF PERSONAL DATA BREACH

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 the breach to the data subject.

Example: Disclosure

In Y v. Turkey, the applicant was HIV positive. As he was unconscious during his arrival at the hospital, the ambulance crew informed the hospital staff that he was HIV positive.

The applicant argued before the ECtHR that the disclosure of this information had violated his right to respect for private life.

However, given the need to protect the safety of the hospital staff, sharing the information was not regarded as a breach of his rights.

ECtHR, Y v. Turkey, No. 648/10, 17 February 2015

OFFENCES AND PENALTIES

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.

Example: Penalties

Offences	Penalties
Section 6: **Investigation of Complaints** 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: **Power to require information** 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**.

Example: Penalties

Offences	Penalties
Section 15: Application for registration 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 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 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

EXCEPTIONS AND RESTRICTIONS

Necessary & proportionate measure in a democratic society

Subject to section 44(4):

For the protection of national security, defence or public security

Provided that a certificate under the hand of the Prime Minister certifying for the non-application of the provision is provided.

CERTIFICATION

To help controllers or processors to demonstrate accountability and compliance with the Act

To build confidence and trust in the organisation with all stakeholders, as well as with the wider public

To allow data subjects to quickly assess the level of data protection of relevant products and services

To give legal certainty for cross-border data transfers

CERTIFICATION

The Data Protection Office encourages the establishment of data protection certification mechanisms, seals and marks.

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.
Withdrawal	• Certifications is subject to withdrawal where the conditions for issuing the certification are no longer met.

Case Law References

- CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014
- CJEU, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, 19 October 2016, para. 43
- ECtHR, S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 4 December 2008
- ECtHR, Haralambie v. Romania, No. 21737/03, 27 October 2009
- CJEU, C-101/01, Criminal proceedings against Bodil Lindqvist, 6 November 2003
- CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014
- ECtHR, *Brunet v. France*, No. 21010/10, 18 September 2014
- ECtHR, Y v. Turkey, No. 648/10, 17 February 2015

Thank You