# Data Protection in Mauritius

*An overview of the current regulatory framework in the field of data protection in Mauritius*

Bibi Chambers

5 March 2020

# Data Protection in Mauritius

## Relevant Legislation

Data Protection Act 2017 (DPA 2017)

## Aims of DPA 2017

DPA 2017 came into effect on 15 January 2018 in the Republic of Mauritius. The previously in force Data Protection Act 2004 (DPA 2004) is now repealed in its entirety.

DPA 2017 aims to provide greater protection to personal data. The DPA 2017 seeks to achieve this aim by strengthening the control and personal autonomy of data subjects over their personal data. This is in accordance with current relevant international standards in the field of data protection. DPA 2017 seeks to simplify the regulatory environment for business in the digital era; accordingly, DPA 2017 promotes the safe transfer of personal data to and from foreign jurisdictions as a result of globalisation and IT infrastructures enabling such transfers.

In the context of DPA 2017, personal data means any information relating to a data subject, for example National Identity Card number, bank account details and telephone number.

DPA 2017 recognises a subset of personal data known as "special categories of personal data". These are frequently referred to as sensitive personal data, and include, but not limited to, racial or ethnic origin, political opinion, genetic data, and sexual orientation amongst others. It is noteworthy that the DPA 2017 allows other categories of personal data to be added to the "special categories of personal data".

## Application of DPA 2017

DPA 2017 shall apply to a data controller or data 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.

Any data controller or data processor not established in Mauritius shall nominate a representative established in Mauritius.

### Established in Mauritius

Any person who:

- is ordinarily resident in Mauritius; or
- carries out data processing operations through an office, branch or agency in Mauritius

shall be treated as being established in Mauritius.

## Who are concerned by DPA 2017?

DPA 2017 concerns data subject, data controller, and data processor.

### Data Subject

Data subject means an identified or identifiable individual, in particular by reference to an identifier.

The identifier may be unique to the individual (for example his or her full name), or in combination may identify the individual (for example last name and date of birth).

### Data Controller

Data controller is a person or public body, who 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 of the personal data.

### Data Processor

Data processor is a person or public body, who processes personal data on behalf of the controller.

A third party, under the direct authority of a data controller or data processor, can be authorised to process personal data.

Irrespective of the relationship between the data processor, data controller, and third-party/ies the same limitations would apply to the processing of personal data as consented to by the data subject.

## What activities are concerned by DPA 2017?

DPA 2017 is concerned with the processing and transfer of personal data.

### Processing of Personal Data

The processing of personal data covers a broad range of activities. These activities include an operation or series of operations, manual or automated, performed on personal data or sets of personal data for the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

In simple terms, processing is concerned with any operation performed by data controller or data processor on personal data belonging to the data subject.

### Transfer of Personal Data

DPA 2017 allows transfer of personal data to another country. The transfer of personal data is only possible by a data controller or data processor, if the following conditions are complied with:

- appropriate safeguards are implemented for the protection of personal data and these safeguards are to the satisfaction of the Data Protection Commissioner; and
- the data subject has provided explicit consent to the proposed transfer.

Furthermore, the transfer of personal data must be necessary, or the transfer of personal data is made from a register which is intended to provide information to the public and which is available for consultation by the public or by any person who can demonstrate a legitimate interest in the consultation of the register.

### When is transfer of personal data considered necessary under DPA 2017?

DPA 2017 considers a transfer to be necessary, in the following instances:

- performance of a contract between a data subject and data controller (for example purchasing a boat from a foreign shipyard), or implementation of pre-contractual measures made at the data subject's request (for example performing a credit check prior to a hire purchase transaction);
- for the conclusion or performance of a contract concluded for the benefit

of the data subject between the data controller and another person (for example delivery of goods by courier);
- for reasons of public interest as provided by law (for example submitting information about financial transactions in line with AML/FATF regulations);
- for the establishment, exercise or defence of a legal claim;
- to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- for the pursuance of compelling legitimate interests by the data controller or data processor, provided these do not override the interests, rights and freedom of the data subjects involved and is not repetitive and concerns a limited number of data subjects; and appropriate safeguards are in place.

## What are the next steps for those concerned with DPA 2017?

### Registration

DPA 2017 prohibits anyone to act as data controller or data processor prior to its registration with the Data Protection Commissioner.

In the application for registration, the data controller or data processor need to provide the following information:

- name and address
- nominated representative (if any);
- description of personal data to be processed and categories of data subjects to which the personal data relate;
- statement as to whether or not the applicant is likely to store special categories of personal data,
- purpose for which the personal data are to be processed;
- description of individuals to whom the data controller may disclose the personal data;
- particulars of any transfer of personal data to another country; and
- safeguards to be implemented to mitigate any risk associated with the processing of personal data and mechanism to ensure the protection of personal data.

Furthermore, in the event of any change in the particulars provided to the Data Protection Commissioner, the data controller or data processor need to notify in writing the Data Protection Commissioner of such change, within 14 days from the date of the change.

### Renewal of Registration Certificate

The holder of a registration certificate can be renewed not later than 3 months before the date of expiry

### Cancellation or Variation of Terms and Conditions of Registration Certificate

The Data Protection Commissioner may cancel or vary the terms of a registration certificate, if:

- false or misleading information were provided during the application for registration; or
- fails, without lawful excuse, to comply with DPA 2017 or any term and condition specified in the registration certificate.

## What are the obligations of those concerned with DPA 2017?

Part IV of DPA 2017 provides a number of obligations which are imposed on data controllers and data processors.

The general stance adopted by DPA 2017 with regards to processing of personal data is that the processing must be done in a fair

and lawful manner. This stance DPA 2017 is in accordance with prevailing international standards on fair information processing principles.

### Duties of Data Controller under DPA 2017

DPA 2017 imposes a series of obligations on data controller, namely:

- adopt policies and implement appropriate technical and organisational measures to ensure the secure processing of personal data;
- keep a record of all processing operations;
- perform Data Protection Impact Assessment;
- obtain prior authorisation from the Data Protection Office prior to any processing of personal data is carried to ensure compliance of intended processing and mitigate any risk associated with such processing;
- appoint an officer responsible for data protection compliance issues (commonly known as Data Protection Officer)

### Data Protection Impact Assessment (DPIA)

A DPIA is performed to enable an organisation (controller or processor) to evaluate the inherent risk posed by the proposed data processing activities. A DPIA is mandatory prior to any potentially high-risk processing under DPA 2017.

## Who ensures compliance with DPA 2017?

The Data Protection Office headed by the Data Protection Commissioner.

The mission of the Data Protection Office is to safeguard the processing of personal data in the present age of information and communication

The overall vision of the Data Protection Office are as follows:

- A society where data protection is understood and practiced by all.
- The right to privacy and data protection is primordial to 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 controllers and processors.

The Data Protection Commissioner ensures compliance with DPA 2017. As such, the Data Protection Commissioner:

- can issue or approve Codes of Practice, or Guidelines;
- maintain register of data controllers and data processors;
- investigate any complaint or information which give rise to a suspicion that an offence may have been committed under DPA 2017;
- conduct security checks, and periodical Compliance Audits; and
- any other acts which fosters the vision of the Data Protection Office, and aims of DPA 2017.

## How does the Data Protection Commissioner ensure compliance with DPA 2017?

The Data Protection Commissioner ensures that data controller, data processor and other individuals processing personal data complies with the provisions of DPA 2017 and regulations made under it in the following manners:

- conduct investigations into complaint received alleging infringements of DPA 2017 and/or its regulations;
- require information which are necessary to allow the Data Protection Commissioner to discharge its functions and exercise powers under DPA 2017;
- apply to the Judge in Chambers for a preservation where there is a risk that the data is vulnerable to loss or modification;
- enforcement notice;

- power to seek assistance of such persona or authority to assist the Data Protection Commissioner discharge his or her functions;
- power to enter and search, subject to a warrant being issued by a Magistrate;
- inspect and assess security measures implemented prior to the processing or transfer of personal data;
- conduct periodical Compliance Audits of the systems of data controllers and data processors; and
- the Data Protection Commissioner may offer data controller and data processor the opportunity to be certified (voluntary and valid for a maximum of 3 years).

## Right of Appeal

Any person who is aggrieved by a decision of the Data Protection Commissioner issued under DPA 2017, may within 21 days from being notified of that decision appeal to the Tribunal.

## Offences

Where no specific penalty is provided under DPA 2017, any person who does not comply or contravenes DPA 2017 shall on conviction be liable to a fine not exceeding MUR 200,000 and to imprisonment for a term not exceeding 5 years.

Any data controller or processor who knowingly supplies false or misleading information in the application for registration to the Data Protection Commissioner shall commit an offence. The sentence upon conviction is a fine not exceeding MUR 100,000 and imprisonment for a term not exceeding 5 years.

Any data controller or data processor who fails to notify the Data Protection Commissioner of a change in particulars within 14 days from the date of the change shall commit an offence. The sentence upon conviction is a fine not exceeding MUR 100,000 and imprisonment for a term not exceeding 5 years.

## Glossary

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

**DOCUMENT** A disc, tape or other device in which information other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and

a film, tape or other device in which visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device

**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, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

**THIRD PARTY** A person or public body other than a data subject, a controller, a processor or a person who, under the direct authority of a controller or processor, who or which is authorised to process personal data

**TRIBUNAL** Tribunal means the ICT Appeal Tribunal set up under section 35 of the Information and Communication Technologies Act

# For More Information

Abdullah Yusuf Ali Bauluck, Barrister at Law

T +(230) 208 4547
M +(230) 5853 7648
E y.bauluck@bibichambers.com

Joseph Désiré Dian, Barrister at Law

T +(230) 208 4547
M +(230) 5984 6649
E desire.dian@bibichambers.com

This guide was authored by Bibi Chambers.