Republic of Mauritius

Data Protection Office

MINISTRY OF TECHNOLOGY, COMMUNICATION AND INNOVATION

DATA PROTECTION OFFICE

DATA PROTECTION ACT 2017

This leaflet is only an introductory guide on the Data Protection Act 2017. Please consult the Data Protection Office for any further query.

AIM OF THE DATA PROTECTION ACT 2017

- To strengthen the control and personal autonomy of data subjects over their personal data, thereby contributing to respect for their human rights and fundamental freedoms, in particular their right to privacy, in line with current relevant international standards, in particular the European Union's General Data Protection Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

- 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.

WHAT DOES PERSONAL DATA MEAN?

Personal data means any information relating to a data subject.

WHAT IS BIOMETRIC DATA?

Biometric data means any personal data relating to the physical, physiological or behavioural characteristics of an individual which allow his unique identification, including facial images or dactyloscopic data.

WHAT IS GENETIC DATA?

Genetic data means personal data relating to the general characteristics of an individual which are inherited or acquired and which provide unique information about the physiology or health of the individual and which result, in particular, from an analysis of a biological sample from the individual in question.

WHAT ARE SPECIAL CATEGORIES OF PERSONAL DATA?

Special categories of personal data means personal data pertaining to —

(a) his racial or ethnic origin;
(b) his political opinion or adherence;
(c) his religious or philosophical beliefs;
(d) his membership of a trade union;
(e) his physical or mental health or condition;
(f) his sexual orientation, practices or preferences;
(g) his genetic data or biometric data uniquely identifying him;
(h) the commission or alleged commission of an offence by him;
(i) any proceedings for an offence committed or alleged to have been committed by him,

the disposal of such proceedings or the sentence of any Court in the proceedings; or

(j) such other personal data as the Commissioner may determine to be sensitive personal data ;

WHO IS A DATA SUBJECT?

Data subject means 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.

WHO IS A CONTROLLER?

The person who or the 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.

WHO IS A PROCESSOR?

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

WHAT DOES PROCESSING MEAN?

It is 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.

WHAT DOES PERSONAL DATA BREACH MEAN?

It is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

WHAT IS PSEUDONYMISATION?

It is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

DATA PROTECTION OFFICE

The Data Protection Office is a public office which acts with complete independence and impartiality and 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.

WHAT ARE THE 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. The Commissioner now has enhanced powers with regard to the handling of complaints namely the amicable resolution of disputes whenever possible.

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.

WHAT ARE THE OBLIGATIONS OF CONTROLLERS AND PROCESSORS?

PART IV of the Act relates to a number of obligations which have been imposed on controllers and processors to ensure that processing of personal data is done in a fair and lawful manner such as:

Principles relating to processing of personal data	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	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.
Collection of personal data	Conditions where controllers can collect personal data of data subject are provided in this section.
Conditions for consent	Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her. Accordingly, the controller bears the burden of proof for establishing the data subject's consent to the processing of his personal data for a specified purpose.
Notification of a personal data breach	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 personal data breach to data subject	The controller must also communicate the personal data breach to the data subject without undue delay, where that breach is likely to result in a high risk to the rights and freedoms of the individual.
Duty to destroy personal data	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	The Act lays down the conditions for legal basis required for processing.
Special categories of personal data	The Act provides for the processing of special categories of personal data, sensitive personal data, which now includes genetic and biometric data.
Personal data of child	Children merit specific protection with regard to their personal data, as they are less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. The Act introduces new safeguards for the processing of personal data of a child.
Security of processing	In addition to security measures for ensuring confidentiality, integrity, availability and recovery from failure, the introduction of new requirements such as pseudonymisation and encryption has been provided.
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	The Act now requires the controller/processor to maintain records of their processing activities.

WHEN SHOULD A CONTROLLER/PROCESSOR CONDUCT A DATA PROTECTION IMPACT ASSESSMENT?

Data Protection Impact Assessments (DPIA) enable organisations (controller or processor) to work out the risks that are inherent in proposed data processing activities before those activities commence. Thus, a DPIA must be carried out by the controller/processor prior to any potentially high-risk processing.

CAN A CONTROLLER TRANSFER PERSONAL DATA ABROAD?

Transfer of personal data to another country may take place only if the controller has adduced appropriate safeguards with respect to the protection of personal data to the Data Protection Office or has complied with the conditions laid down in the provisions of this Act relating to the transfer of personal data outside Mauritius.

HOW THIS LAW CATERS FOR THE RIGHTS OF DATA SUBJECTS?

Part VII of the Act stipulates the rights of data subjects. The Act has enhanced the rights of data subjects by giving substantial rights including:

Right of access	Automated individual decision making	Rectification, erasure or restriction of processing	Right to object	Exercise of rights
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.	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).	Data subjects have the right to: rectify inaccurate personal data, to delete their personal data if the continued processing of those data is not justified or to withdraw their consent and to restrict the processing of personal data (meaning that the data may only be held by the controller, and may only be used for limited purposes).	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.	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.

IS IT AN OFFENCE NOT TO COMPLY WITH THE DATA PROTECTION ACT?

Yes. 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.

WHAT IS CERTIFICATION REFERRED TO IN SECTION 48 OF THE ACT?

To enhance transparency and compliance with the Act, certification has been introduced to help controllers or processors to demonstrate compliance with the Act, and also to allow data subjects to quickly assess the level of data protection of relevant products and services.

Contact Details: DATA PROTECTION OFFICE
5th Floor, Sicom Tower, Wall Street, Ebene
Phone: +230 4600251
Email: dpo@govmu.org
Website: http://dataprotection.govmu.org