DATA PROTECTION LAWS OF THE WORLD

Mauritius

DLA PIPER

MAURITIUS

Last modified 18 January 2024

LAW

Mauritius regulates data protection under the Data Protection Act 2017 (DPA 2017 or Act), proclaimed through Proclamation No. 3 of 2018 and effective on January 15, 2018. The Act repeals and replaces the Data Protection Act 2004, so as to align with the European Union General Data Protection Regulation 2016/679 (GDPR).

DEFINITIONS

Definition of personal data

Personal data is defined as any information relating to a data subject. A data subject is a natural person who is identified or identifiable, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Definition of sensitive personal data or special categories of personal data

Similar to the GDPR, the DPA 2017 refers to sensitive personal data as special categories of data. Special categories of data include personal data pertaining to any of the following about a data subject:

- Racial or ethnic origin
- Political opinion or adherence
- Religious or philosophical beliefs
- Membership of a trade union
- Physical or mental health or condition
- Sexual orientation, practices or preferences
- Genetic or biometric data that is uniquely identifying
- Commission or proceedings related to the commission of a criminal offense
- Such other personal data as the Commissioner may determine to be sensitive personal data

NATIONAL DATA PROTECTION AUTHORITY

Under DPA 2017, the Data Protection Office (DPO) is responsible for data protection oversight. The DPO is an independent and impartial public office that is not subject to the control or direction of any person or authority. The DPO is headed by the Data Protection Commissioner (Commissioner), with the assistance of public officers as may be necessary. The contact details of the DPO are:

Data Protection Office

5th Floor, SICOM Tower
Wall Street, Ebene
Republic of Mauritius

Telephone

+230 460 0251

Fax

+230 489 7341

Website

dataprotection.govmu.org/

Email

dpo@govmu.org

dpo2@govmu.org

REGISTRATION

Every person who intends to act as a data controller or a data processor (as defined below) must register with the Commissioner in a form approved by the Commissioner and is required to pay a prescribed registration fee. The Commissioner is authorized to approve applications and issue registration certificates, which are valid for three years.

Data processors and controllers must renew their registration within three months prior to the date that their registration expires. Failure to register or renew registration constitutes an offence under the Act, punishable by a fine not exceeding 200,000 or imprisonment for a term not to exceed five years.

A data controller is a person or public body who alone, or jointly with others, determines the purposes and means of personal data processing, and who has decision making power with respect to processing. A data processor is a person or public body who processes personal data on behalf of a controller.

Application for registration

Every registration application must include all of the following:

- Name and address
- Whether a representative has been nominated for the purposes of the Act, and the name and address of the representative
- A description of the personal data to be processed by the controller or processor, and of the category of data subjects, to which the personal data relate
- A statement as to whether data controller or processor holds, or is likely to hold, special categories of personal data
- A description of the purpose for which the personal data are to be processed
- A description of any recipient to whom the controller intends or may wish to disclose the personal data
- The name, or a description of, any country to which the proposed controller intends or may wish, directly or indirectly, to transfer, the data
- A general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data

A controller or processor who knowingly supplies false or misleading material information in their registration application commits an offense and could be held liable to a fine not to exceed 100,000 or imprisonment for a term not to exceed five years.

DATA PROTECTION OFFICERS

The DPA 2017 provides that every controller shall adopt policies and implement appropriate technical and organizational measures so as to ensure and be able to demonstrate that the processing of personal data is performed in accordance with the Act.

One of such measures is the mandatory requirement for the designation of a data protection officer (DPO) by all controllers and processors.

There can be one DPO for a group of companies, provided he is accessible for each company within the group.

The DPO can be an employee of the controller / processor, provided that there is no conflict of interest (if such position leads to the determination of purposes and means of processing) such as in the case of a chief executive, chief operating, chief financial, chief medical, head of marketing, head of human resource or head of IT.

The DPO can also be someone from outside the organisation.

The DPO needs to have professional experience and knowledge of data protection laws and standards.

The controller / processor is required to ensure that the DPO does not receive any instructions regarding the exercise of his functions-he should work in an independent environment and manner.

Role of DPO

The role of the DPO is to:

- advise the controller / processor and its employees about their obligations to comply with data protection laws and monitor compliance;
- train staff and conduct internal audits;
- advise on DPIAs;
- maintain a record of processing operations under his responsibility;
- be the first point of contact for the Data Protection Office and for individuals whose data are processed (employees, customers).

DPOs are not personally responsible for non-compliance with data protection requirements. Data protection compliance is the responsibility of the controller / processor.

COLLECTION & PROCESSING

Subject to exceptions provided under the Act, a controller cannot collect personal data unless the collection (a) is for a lawful purpose connected with a function or activity of the data controller, and (b) the collection is necessary for that purpose.

Where the data controller collects personal data directly from the data subject, the data controller shall at the time of collecting personal data ensure that the data subject concerned is informed of:

- The identity and contact details of the controller and, where applicable, its representative and any data protection officer
- The purpose for which the data are being collected
- The intended recipients of the data
- Whether or not the supply of the data by that data subject is voluntary or mandatory
- The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The existence of the right to request from the controller access to and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing
- The existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

- The period for which the personal data shall be stored
- The right to lodge a complaint with the Commissioner
- Where applicable, that the controller intends to transfer personal data to another country and on the level of suitable protection afforded by that country
- Any further information necessary to guarantee fair processing in respect of the data subject’s personal data, having regard to the specific circumstances in which the data are collected

Where data is not collected directly from the data subject concerned, the data controller or any person acting on his behalf shall ensure that the data subject is informed of the matters set out above.

There are six principles relating to the processing of personal data which are enumerated in the Act. Accordingly, every controller or processor need to ensure that personal data are:

- Processed lawfully, fairly and in a transparent manner in relation to any data subject
- Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, and
- Processed in accordance with the rights of data subjects

For processing of data to be lawful, it must have a legal basis. One of the legal basis is consent. According to the DPA 2017, no person shall process personal data unless the data subject consents to the processing for one or more specified purposes. Consent is defined under the Act as any freely given, specific, informed and an 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.

Processing shall also be lawful, when the processing is necessary for any of the following:

- The performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract
- Compliance with any legal obligation to which the controller is subject
- In order to protect the vital interests of the data subject or another person
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- The performance of any task carried out by a public authority
- The exercise, by any person in the public interest, of any other functions of a public nature
- The legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject
- The purpose of historical, statistical or scientific research

Special categories of personal data

Special categories of personal data, as defined above, cannot be processed unless the processing is based on one of the legal basis as described above and the processing is carried out in the course of the controller’s / processor’s legitimate activities with appropriate safeguards.

It is also possible to process special categories of personal data when:

- Processing relates to personal data which are manifestly made public by the data subject; or
- Processing is necessary for:
    - the establishment, exercise or defense of a legal claim;

- the purpose of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to a contract with a health professional subject to the obligation of professional secrecy;
- the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or
- protecting the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.

TRANSFER

A controller or processor may transfer personal data to another country where any of the following apply:

- It has provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data; or
- The data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards; or
- The transfer is necessary: (i) for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject’s request; (ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; (iii) for reasons of public interest as provided by law; (iv) for the establishment, exercise or defense of a legal claim; or (v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (vi) for the purpose of compelling legitimate interests pursued by the controller or the processor which are not overridden by the interests, rights and freedoms of the data subjects involved and where – (A) the transfer is not repetitive and concerns a limited number of data subjects; and (B) the controller or processor has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data; or
- The transfer is made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled in the particular case. Such transfer shall not involve the entirety of the personal data or entire categories of the personal data contained in the register and, where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or in case they are to be the recipients.

The Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as he may determine.

SECURITY

Under the DPA 2017, a controller or processor must, at the time of the determination of the means for processing and at the time of the processing, implement and maintain appropriate security and organizational measures for the prevention of unauthorized access to, alteration, disclosure or destruction of, or the accidental loss of the personal data.

Additionally, the controller or processor must ensure that measures provide a level of security appropriate to the harm that may result from the unauthorized access to, alteration, disclosure or destruction of, or the accidental loss of the personal data and the nature of the personal data concerned.

The measures referred to above shall include all of the following:

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

In determining the appropriate security measures, in particular, where the processing involves the transmission of data over an information and communication network, a data controller shall have regard to the:

- State of technological development available
- Cost of implementing any of the security measures
- Special risks that exist in the processing of the data, and
- Nature of the data being processed

Where a controller is using the services of a processor – (a) the controller must choose a processor that is able to provide sufficient guarantees in respect of security and organizational measures for the purpose of complying with the security measures described above; and (b) the controller and the processor shall enter into a written contract which shall provide that – (i) the processor shall act only on instructions received from the controller; and (ii) the processor shall be bound by obligations of the controller as regards security measures to be taken.

If the purpose for keeping personal data has lapsed, the controller must destroy such data as soon as reasonably practicable and notify any data processor holding such data, who in turn must destroy the data specified by the controller as soon as is reasonably practicable.

Every controller or processor has to take all reasonable steps to ensure that any person employed by him or it is aware of, and complies with, the relevant security measures.

BREACH NOTIFICATION

Under the DPA 2017, a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner. Where the Controller fails to notify the personal data breach within the 72 hours time limit, he should provide the Commissioner with the reasons for the delay. Where a processor becomes aware of a personal data breach, he shall notify the controller without undue delay.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the controller shall also communicate the personal data breach to the data subject without undue delay.

The communication of a personal data breach to the data subject shall not be required where:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the breach, in particular, those that render the data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of the data subject referred above is no longer likely to materialise; or
- it would involve disproportionate effort and the controller has made a public communication or similar measure whereby data subject is informed in an equally effective manner.

ENFORCEMENT

The DPA 2017 provides the Commissioner with enforcement authority. Where a complaint is made to the Commissioner that the Act or any regulations made under it, has or have been, is or are being, or is or are about to be, contravened, the Commissioner shall:

- investigate into the complaint or cause it to be investigated by an authorized officer, unless he is of the opinion that the complaint is frivolous or vexatious; and

- where he is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the complaint, notify, in writing, the individual who made the complaint of his decision in relation to it so that the individual may, where he considers that he is aggrieved by the decision, appeal against it to the Information and Communications Technologies (ICT) Appeal Tribunal.

If the Commissioner is of the opinion that a controller or a processor has contravened, is contravening or is about to contravene the DPA 2017, the Commissioner may serve an enforcement notice on the data controller or processor, requiring remedial efforts within a specified time frame.

A person who, without reasonable excuse, fails or refuses to comply with an enforcement notice commits an offense, and, on conviction, is liable to a fine not to exceed 50,000 Mauritian rupees and to imprisonment for a term not to exceed two years.

If the Commissioner has reasonable grounds to believe that data is vulnerable to loss or modification, she may make an application to a Judge in Chambers for an order for the expeditious preservation of such data.

The Commissioner may also carry out periodical audits of the systems and security measures of data controllers or data processors to ensure compliance with data protection principles laid down in the DPA 2017.

ELECTRONIC MARKETING

The Act regulates direct marketing, which is defined as the communication of any advertising or marketing material which is directed to any particular individual. The definition also encompasses electronic marketing.

The data subject may object to the processing of his or her personal data for purposes of direct marketing, including profiling to the extent relevant. Where a data subject objects to processing, his or her personal data may no longer be processed for that purpose. This right to object shall be explicitly brought to the attention of the data subject.

ONLINE PRIVACY

The Act applies to online privacy, though it does not contain specific provisions in relation to online privacy.

KEY CONTACTS

Juristconsult Chambers

Shalinee Dreepaul Halkhoree
Partner-Barrister
Juristconsult Chambers
T +230 465 00 20 Extension 225
sdreepaul@juristconsult.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.