FACTSHEET: MAURITIUS

Last updated: 31 March 2020
Prepared by Justin Bryant
Revised by Tshepiso Hadebe

FAST FACTS

Population: 1,271,183
Capital: Port Louis
President: Prithvirajsing Roopun
2019 Freedom House Score: 89/100
Data protection law? Enforced

LAW

Mauritius was among the first movers in the data privacy space in Africa, and as such, its regulations are robust, and in line with international standards. When the country enacted the Data Protection Act 2004 (DPA 2004), it became the first African country to establish the Office of the Data Protection Commissioner and make it operational.

As of January 2018, Mauritius regulates data protection under the Data Protection Act 2017 (DPA 2017), which repealed and replaced the former act, so as to align with the European Union General Data Protection Regulation 2016/679 (GDPR). The updates to the law include the implementation of data protection impact assessments, notification of personal data breaches, stricter security requirements attached to data processing, and clearer standards around the details of lawful processing.

Among other things, data subjects have the right to:

- have their personal data corrected;
- access their personal data;
- object in writing to the processing of their personal data, at any time;
- prevent processing of personal data for purposes of direct marketing; and
- object to a decision based solely on automatic processing that would significantly affect them or adverse legal repercussions.

PERSONAL DATA

Personal data is any information relating to a data subject. *Special categories of personal data* consist of the following:

- 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;
- uniquely identifying genetic data or biometric data;
- the commission or alleged commission of an offence;
- any proceedings for an offence committed or alleged to have been committed by a person, the disposal of such proceedings or the sentence of any Court in the proceedings; or
- such other personal data as the Commissioner may determine to be sensitive personal data.

Special categories of personal data shall not be processed without affirmative consent from the data subject or unless an exception applies.

COLLECTION AND PROCESSING

Collection must be for a lawful purpose allied to a function or activity of the data controller, and necessary for that purpose. If personal data is collected directly from the data subject, the data controller shall ensure that the data subject 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 the provision of the data by that data subject is voluntary or mandatory;
- the right to withdraw consent, at any time;
- the right to request access to and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing;
- any automated decision making, including profiling, and information about the logic involved, as well as the significance and the perceived consequences of such processing for the data subject;
- the period for which the personal data shall be stored;
- the right to file a complaint with the Commissioner;
- if the controller intends to transfer personal data to another country, and the level of protection afforded by that country; and
- any further information necessary to guarantee fair processing of the data subject's personal data under the circumstances.

If personal data is not collected directly from the data subject, the data controller or processor is responsible to make sure that the data subject knows of the matters above, and that the data is:

- processed lawfully, fairly, and transparently;
- 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 for the purposes for which they are processed;
- accurate and kept current, ensuring that inaccurate personal data is erased or rectified, without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary; and
- processed in accordance with the rights of data subjects.

REGISTRATION AND ENFORCEMENT

All data controllers and processors must register with the Commissioner, and registration is valid for three years. Failure to register or renew registration constitutes an offence under the DPA 2017, punishable by a fine not exceeding Rs200,000 or imprisonment for a term not exceeding five years.

Each data controller must also appoint a data protection officer who is responsible for compliance issues related to data collection and processing.

The Commissioner has enforcement power and may investigate complaints about regulatory violations. If the Commissioner believes that a controller or a processor has violated the DPA 2017, he, she or they may serve an enforcement notice on the data controller or processor, requiring that the defect is remedied by a certain deadline. Failing to comply with an enforcement notice is an offence punishable by a fine of up to Rs50,000 and up to two years in prison.

If the Commissioner has reasonable grounds to believe that data is vulnerable to loss or modification, he, she or they may ask a judge for an order for the expeditious preservation of such data. The Commissioner may also carry out periodic audits of the systems and security measures used by data controllers and processors.

CROSS-BORDER 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;
- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of the transfer;
- the transfer is necessary:
    - to enter or perform a contract between the data subject and the controller, or a contract in the interest of the data subject;
    - for the public interest;
    - to advance a legal claim;
    - to protect the vital interests of the data subject or other persons, where the data subject cannot consent; or
    - for compelling legitimate interests pursued by the controller or the processor which do not override the interests, rights, and freedoms of the data subjects involved and where:
        - the transfer is not repetitive and concerns a limited number of data subjects; and
        - the controller or processor has assessed all the circumstances surrounding the transfer and has provided the Commissioner with proof of appropriate data protection safeguards; 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.

SECURITY AND BREACH PROTOCOL

In the case of a personal data breach, the controller shall notify the Commissioner as soon as possible, and no later than 72 hours after becoming aware of it. If a processor learns of a breach, he, she or they shall notify the

controller without any 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 will notify the data subject as soon as possible after notifying the Commissioner.

Notifying the data subject is not required if:

1. the controller has applied appropriate technical and organisational protection measures to the personal data affected by the breach;
2. the controller has mitigated the high risk to the rights and freedoms of the data subject; or
3. it would involve disproportionate effort and the controller has made a public communication or similar measure whereby the data subject is informed just as effectively.

Read the legal notice and terms of use for this factsheet.