FACTSHEET: MADAGASCAR

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

FAST FACTS

Population: 27,458,204
Capital: Antananarivo
President (Acting): Andry Rajoelina
2019 Freedom House Score: 56/100
Data protection law? Exists, not enforced

LAW

Madagascar's 2010 Constitution grants individuals the inviolability of their persons, domiciles, and of the secrecy of their correspondence. In 2015, the country's comprehensive data protection regulation called Law No. 2014-038 (DP Law) came into force upon publication in the Madagascan Official Gazette on 20 July. The DP Law draws upon the EU Data Protection Directive (95/46/EC) as well as advice from other Francophone countries belonging to the *Association francophone des autorites de protection des donnes personnelles* (AFAPDP).

Despite the fact that the law is technically in effect, the data protection authority, the *Commission Malagasy sur l'Informatique et des Libertés* (CMIL), has not yet been established. Also, requirements for breach notification are absent from the DP Law.

Some of the rights of data subjects under the DP Law include:

- the right to object to data processing;
- the right to access one's personal data;
- the right to rectification of one's personal data; and
- the right to get information about a data controller and processing of personal data relating to a person.

PERSONAL DATA

Personal data consists of any information relating to a natural person, whereby that person is or can be identified by reference to a name, an identification number or to one or more physical, physiological, psychic, economic, cultural or social elements specific to that person.

Sensitive personal data may not be processed unless strict requirements are met, and includes information relating to:

- racial origin;
- biometric and genetic information;
- political opinion;
- religious beliefs or other convictions;
- trade union affiliation; or

- health or sexual life.

COLLECTION AND PROCESSING

Personal data processing must abide by the following principles:

- Personal data must be processed fairly and lawfully and be for an explicit and legitimate purpose.
- The amount of personal data to be processed must be adequate, relevant, and not excessive regarding the purposes for which they are collected or used.
- Personal data must be accurate, complete, and current; inaccurate or incomplete data should be erased or rectified.
- Personal data must be kept in a form which allows data subjects to be identified only for the requisite period for the purposes for which they are collected or used.
- Given the nature of the data and the associated risks, a data controller must take all necessary precautions to ensure security of personal data.

Personal data processing must be based on the data subject's prior consent or fulfil one of the following conditions:

- compliance with a legal obligation of the data controller;
- protection of the individual's life;
- carrying out a public service;
- commencing or performing a contract to which the concerned individual is a party; or
- realising of the legitimate interest of the data controller or the data recipient, subject to the interests and fundamental rights and liberties of the concerned individual.

REGISTRATION AND ENFORCEMENT

Under the DP Law, CMIL is designated as an independent data protection authority. Generally, personal data processing requires a prior declaration to the CMIL, but data controllers who appoint a data protection officer are not required to issue prior declarations except in special circumstances (e.g., an extraterritorial transfer to a country that does not provide an adequate level of personal data protection).

CMIL is authorised to conduct online inspections and on-site verifications of an entity's data processing operations. When a data controller or processor has violated the DP Law, CMIL may issue:

- warnings and notices to comply with the obligations defined in the DP Law;
- notice of withdrawal of the authorisation; and / or
- a fine of up to 5% of the last financial year pre-tax turnover (not deducted from tax turnover).

Violating the DP Law is an offence. Processing personal data without prior declaration or authorisation of CMIL can result in 6 months to 2 years in prison.

CROSS-BORDER TRANSFER

A data subject's personal data may only be transferred out of Madagascar if the country provides an adequate level of protection for privacy and fundamental rights and liberties. If a country does not offer sufficient protection, a data controller may only transfer personal data if:

- the data subject consents and is informed of the absence of adequate protection; or
- the transfer is necessary:
    - for the commencement or performance of a contract between the data controller and the individual, or the conclusion or performance of a contract in the interest of the individual between the data controller and a third party;
    - to protect the public interest;
    - for consultation of a public register intended for the public's information; or
    - to assist with the acknowledgment, exercise, or defence of a legal right.

The data recipient in the receiving country cannot transfer personal data to another country without the authorisation of the original data controller and CMIL.

SECURITY AND BREACH PROTOCOL

While the DP Law necessitates that a data controller take all necessary precautions with respect to the nature of the data and the risk presented by the processing, and to preserve the security of personal data and prevent alteration, corruption or access by unauthorised third parties, it does not obligate a data controller to alert CMIL or the data subject in the case of a breach.

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