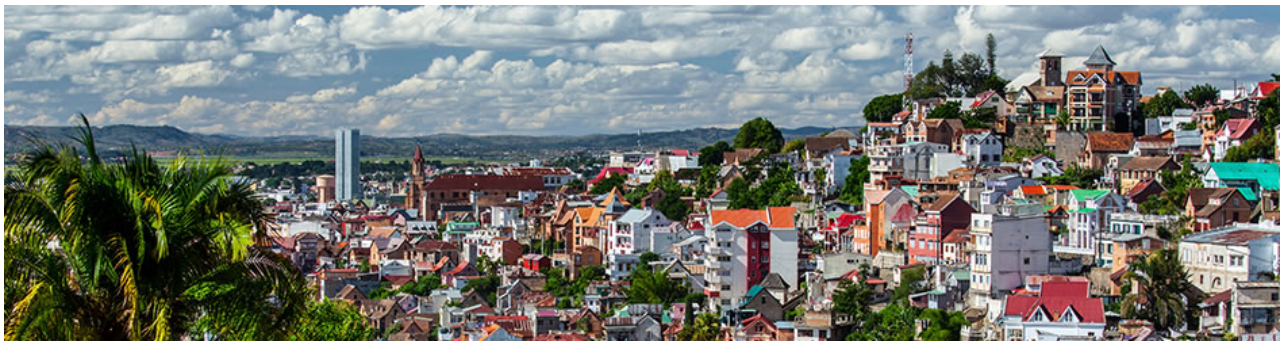
DATA PROTECTION LAWS OF THE WORLD

Madagascar

DLA PIPER

MADAGASCAR



Last modified 1 December 2023

LAW

Law No. 2014-038 relating to protection of personal data is the main regulatory framework in Madagascar (the “**Data Protection Law**”).

After discussion at the National Assembly of Madagascar, the Data Protection Law was adopted on 16 December 2014. The Law was promulgated by the President of Republic of Madagascar on 9 January 2015 and published in the Official Gazette of the Republic of Madagascar on 09 June 2015.

The Data Protection Law has been in force for nine (09) years, but its application is not yet effective, as no implementing decree has been published.

DEFINITIONS

Definition of personal data

Personal data is any information relating to a natural person, whereby that person is or can be identified, directly or indirectly, by reference to a name, an identification number or to one or more elements specific to him / her such relating to physical, physiological, psychical, economic, cultural or social.

Definition of sensitive personal data

Sensitive personal data means data which includes information relating to:

- racial origin;
- biometric and genetic information;
- political opinion;
- religious belief or other convictions;
- trade-union affiliation; and / or
- health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Law provides for the creation of the *Commission Malagasy sur l'Informatique et des Libertés* (“CMIL”). However, the CMIL has not yet been established. The decree setting out the CMIL’s assignment and organisation has just been adopted by the Council of Government on 28 November 2023, and is awaiting adoption by the Council of Ministers. Its effective implementation is expected in 2024.

REGISTRATION

Except for certain data processing that is subject to exemption, authorisation, ministerial order or decree, the processing of personal data requires a prior declaration to the CMIL.

The prior declaration to the CMIL shall specify, where relevant, *inter alia*:

- the identity and the address of the data controller (*responsable du traitement*) (i.e. the natural or legal person who either alone or jointly with other persons determines the purpose and the means of the personal data processing and implements such processing itself or appoints a data processor for that purpose);
- the purpose(s) of the processing;
- the interconnections between databases;
- the types of personal data processed, their origins and the categories of persons affected by the processing;
- the duration for which the data will be kept;
- the department or persons in charge of implementing the data processing;
- the existence of data transfer to other country;
- the measures taken in order to ensure the security of the processing;
- the use of a data processor (*sous-traitant*).

The CMIL has to issue its decision on any authorisation application 2 months following receipt of the application. An additional time period of 2 months can be added to this period after decision of the President of the CMIL. The absence of decision of the CMIL during these periods is considered as a refusal of the application.

DATA PROTECTION OFFICERS

The Data Protection Law does require the appointment of a data protection officer (*délégué à la protection des données à caractère personnel*) in Madagascar provided that the CMIL is operational because the appointed data protection officer (“**DPO**”) should be notified to the CMIL.

The appointment of a DPO exempts an entity from making prior declarations to the CMIL.

The appointment of a DPO does not exempt an entity from requesting prior authorisation, where necessary (for example where there is a transfer of data to a country that does not provide an adequate level of protection for personal data).

The DPO must be a resident of Madagascar.

COLLECTION & PROCESSING

The following principles must be satisfied when personal data is collected and processed:

- all personal data must be processed fairly and lawfully for specific, explicit and legitimate purposes and subsequently processed in accordance with these purposes;
- all personal data collected must be adequate, relevant and non-excessive in view of the purposes for which it is collected;
- all personal data must be accurate and comprehensive and when necessary, kept up to date;
- all personal data must be retained no longer than is necessary for the purposes for which it is processed.

The processing of personal data must receive the data subject's prior consent or fulfill one of the following conditions:

- compliance with a legal obligation of the data controller;

- the purpose of the processing is to protect the individual's life;
- the purpose of the processing is to carry out a public service;
- the processing relates to the performance of a contract to which the concerned individual is a party, or pre-contractual measures requested by that individual;
- processing relates to the realisation of the legitimate interest of the data controller or the data recipient, subject to the interest and fundamental rights and liberties of the concerned individual.

The conditions for processing of sensitive personal data include most of the above conditions, but contain an additional list of more restrictive conditions that must also be satisfied such as requirement to obtain prior consent of the data subject, or in the absence of consent where the processing is undertaken to carry out a public service and is required by law or priorly authorised by the CMIL.

TRANSFER

The transfer of a data subject's personal data to a third party country is allowed only if the country guarantees to individuals a sufficient level of protection in terms of privacy and fundamental rights and liberties.

The sufficiency of the protection is assessed by considering all the circumstances surrounding the transfer, in particular the nature of the data, the purpose and the duration of the proposed processing, country of origin and country of final destination, rules of law, both general and sectorial in force in the country in question and any relevant codes of conduct or other rules and security measures which are complied with in that country.

Data controllers may transfer personal data to a third country that is not deemed to offer adequate protection only if:

- the data subject consents and duly informed of the absence of adequate protection;
- the transfer is necessary:
  - for the performance of a contract between the data controller and the individual, or pre-contractual measures;
  - undertaken at the individual's request;
  - for the conclusion or the performance of a contract in the interest of the individual, between the data controllers and a third party;
  - for the protection of the public interest;
  - for consultation of a public register intended for the public's information;
  - to comply with obligations allowing the acknowledgment, the exercise or the defense of a legal right.

In all cases, the data recipient in the third party country cannot transfer personal data to another country, except with the authorisation of the first data controller and the CMIL.

SECURITY

The data controller must take all useful precautions, with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, amongst other things, prevent alteration, corruption or access by unauthorised third parties.

BREACH NOTIFICATION

The Data Protection Law does not set out any general or specific obligation to notify the CMIL or the data subject in the event of a data security breach.

ENFORCEMENT

The CMIL has the power to proceed with verifications of any data processing, and, as the case may be, to request a copy of every document that it considers useful in respect of verifications. The CMIL agents are authorised to carry out online inspections and on-site verifications of a data controller or a data processor.

In cases where the CMIL is of the opinion that a data controller or a data processor has contravened the provisions of the Data Protection Law, then it may serve, in accordance with the severity of the violation committed:

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

The Data Protection Law provides that any processing of personal data in contravention with its provisions is considered an offence. For example, processing of personal data without prior declaration to or authorisation of the CMIL can result in imprisonment of 6 months to 2 years (Article 62 of the Data Protection Law).

In addition to any penalty, the Court may order the erasure of all or part of the personal data which was the object of the processing considered an offence.

ELECTRONIC MARKETING

The Data Protection Law does not provide specific restrictions on the use of electronic marketing. However, the data subject has a right to opt out of allowing their personal data to be used for marketing purposes without providing any reason.

ONLINE PRIVACY

The Data Protection Law does not yet address location data, cookies, local storage objects or other similar data-gathering tools.

KEY CONTACTS

Madagascar Law Offices

Sahondra Rabenarivo
Managing Partner
Madagascar Law Offices
T +(261) 20 23 25623
sahondra@aln-madagascar.com

DATA PRIVACY TOOL

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