

DATA PROTECTION LAWS OF THE WORLD

Mozambique



Downloaded: 6 May 2024

MOZAMBIQUE



Last modified 18 January 2024

LAW

In Mozambique there is no specific legislation on data protection or privacy. However, there are other sources of law that impose some privacy obligations, including:

- The Civil Code (Decree-Law no. 47344, of November 25, 1966, in force in Mozambique through Edict no. 22869, dated September 4, 1967);
- The Penal Code (Law no. 24/2019, of December 24, as amended by Law no. 17/2020 of 23 December);
- The Labour Law (Law no. 23/2007, of August 1) and the new Labour Law (Law no. 13/2023, of 25 August) which enters into force on 22 February 2023;
- The Electronic Transactions Law (Law no. 3/2017, of January 9);
- The Regulations on Registration and Licensing of Intermediary Electronic Service Providers and Operators of Digital Platforms (Decree no. 59/2023, of 27 October); and
- Resolution no. 5/2019, of 20 June, ratifies the African Union Convention on Cybersecurity and Personal Data Protection (AU Convention).

In addition, the Constitution of the Republic of Mozambique provides that all citizens are entitled to the protection of their private life and have the right to honor, good name, reputation, protection of their public image and privacy. Further, Article 71 of the Constitution identifies the need to legislate on access, generation, protection and use of computerized personal data (either by public or private entities); however, implementing legislation has not yet been approved.

DEFINITIONS

Definition of personal data

The Electronic Transactions Law defines personal data as being any information in relation to a natural person which can be directly or indirectly identified by reference to an identification number or one or more factors. The AU Convention contains an indication of these factors, being: physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

The Constitution of the Republic of Mozambique imposes restrictions on recording and handling any individually identifiable information concerning a person's political, philosophical or ideological beliefs, religious beliefs, membership in a political party or trade union and (particulars) related to the person's privacy. In addition, the AU Convention also considers personal data relating to sex-life, race, health, social measures, legal proceedings and penal or administrative sanctions as sensitive.

NATIONAL DATA PROTECTION AUTHORITY

There is no data protection authority in Mozambique but the National Institute of Information and Communications Technology (*Instituto Nacional de Tecnologia de Informa#231;#227;o e Comunica#231;#227;o* – “INTIC#8221;) has some competencies in this regard.

The Cybersecurity Bill will establish INTIC as the national cybersecurity authority, insofar as it relates to electronic communications.

REGISTRATION

Decree 59/2023 requires the registration of Intermediate Electronic Services Providers and Operators of Digital Platforms. The Electronic Transactions Law defines the intermediate service provider as any person who, in representation of another, sends, receives and stores data messages, and also who provides network access services or provide services through a network. Any entity that performs such acts will qualify as an intermediate service provider and must be registered and licensed with INTIC.

The registration requirement is applicable to Intermediate Electronic Services Providers and Operators of Digital Platforms that offer services to receivers based or located in Mozambique, regardless of where the providers are based.

DATA PROTECTION OFFICERS

The Electronic Transactions Law requires the data processor to appoint someone responsible for compliance of the provisions related to electronic personal data protection.

COLLECTION & PROCESSING

Under the Constitution of the Republic of Mozambique, individually identifiable information, concerning political, philosophical or ideological beliefs, religious beliefs, membership in a political party or trade union and (particulars) related to the person#8217;s privacy may not be stored or processed in a database.

TRANSFER

The law does not generally restrict cross-border transfers of personal information. The Constitution of the Republic of Mozambique imposes restrictions on disclosures of personal information to third parties, unless prior consent from the data subject is obtained.

Although there is a prohibition against the transfer of personal data to a non-Member State under the AU Convention, this prohibition does not apply if said State ensures adequate level of protection of the privacy, freedoms and fundamental rights of the data subject. The AU Convention also requires that consent be sought from the national protection authority before the data controller may transfer the data to a third country. Currently, INTIC does not have such powers so the principle of consent of the data subject and the transfer of data to a country with an adequate data protection framework would apply. Notwithstanding, parties may approach INTIC for further guidance on this matter.

SECURITY

Under the Electronic Transactions Law, the person / entity responsible for processing electronic data, must protect personal data against risks, losses, unauthorized access, destruction, use, modification or disclosure.

The Cybersecurity Bill also establishes a duty on data processors and data controllers to ensure the confidentiality of data stored in electronic communications network.

BREACH NOTIFICATION

There is currently no breach notification requirement in Mozambique.

A Cybersecurity Bill is being discussed which intends to establish amongst other things, the legal regime applicable to the protection of data communication networks, of data, of information systems and critical infrastructures in cyberspace.

The bill stipulates which entities are required to notify in the event of a data breach.

ENFORCEMENT

Under the Electronic Transactions Act, a violation of the data protection duty or the duties of a data processor is subject to a fine of between 30 to 90 minimum wage salaries in effect in the public administration sector, in the absence of a more serious punishment.

The Penal Code (Law no. 24/2019 of December 24, as amended by Law no. 17/2020 of December 23) provides for certain cybercrimes, such as intrusion of automatized database, which is subject to imprisonment of up to two years and corresponding fine. There are also other cybercrimes such as fraud through electronic means and unauthorized use of data resulting in unjust enrichment, which is subject to imprisonment generally from a year up to five years and a corresponding fine. The new Penal Code attempts to bridge the gap by identifying cybercrimes related to data protection which are punishable.

The Cybersecurity Bill also makes provision for fines and sanctions for the violation of its provisions.

However, given that Mozambique does not have specific data protection laws nor a specific authority responsible for overseeing data protection matters, enforcement of data protection-related matters is minimal.

ELECTRONIC MARKETING

The rules applicable to electronic advertisement and marketing are provided under the Advertisement Code (Decree no. 38 /2016, of August 31) and the Electronic Transactions Law (Law no. 3/2017, of January 9).

Under the Electronic Transactions Law, express consent from a recipient is required prior to sending direct marketing communications via automated dialing systems, fax machines and email, unless one of the following applies

- If the sender obtained the contact details of the recipient during the sale or negotiations for the sale of a product or service to the recipient;
- The direct marketing refers to similar products or services to those of the recipient;
- At the moment of initial collection of the data, the recipient was offered the option to refuse of use of his contact details, and decided not to refuse;
- If the recipient did not refuse the use of its data in any subsequent communications.

Under the Advertisement Code, electronic marketing messages should be clearly identified and include sufficient information, so as to allow the common recipient to easily understand all of the following:

- The nature of the message;
- The advertiser;
- The promotional offers, such as discounts, prizes, gifts and promotional contests and games, as well as the conditions to which they are bound (if applicable).

All direct marketing message must provide recipients with information about how to opt out of further marketing communications, as well as the identity details of the source from which the contact details of the consumer have been obtained.

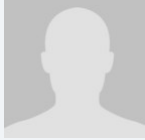
ONLINE PRIVACY

Other than the above general rule, there are no other rules applicable to online privacy.

However, the Cybersecurity Bill intends to establish the duty to ensure the integrity, confidentiality and privacy of the information systems during the communication of data using the internet.

KEY CONTACTS

Eduardo Calu



Managing Partner
SAL & Caldeira Advogados, Lda.
T +258 21 241 400
ecalu@salcaldeira.com

DATA PRIVACY TOOL

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

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.