

DATA PROTECTION LAWS OF THE WORLD

Angola



Downloaded: 27 January 2021

ANGOLA



Last modified 12 January 2021

LAW

Angola regulates data privacy and protection issues under the Data Protection Law (Law no. 22/11, 17 June 2011), the Electronic Communications and Information Society Services Law (Law no. 23/11, 20 June 2011) and the Protection of Information Systems and Networks Law (Law no. 7/17, 16 February 2017).

DEFINITIONS

Definition of personal data

The Data Protection Law defines personal data as any given information, regardless of its nature, including images and sounds related to a specific or identifiable individual.

An identifiable person is an individual directly or indirectly identified, notably, by reference to his or her identification number or to the combination of specific elements of his or her physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

The Data Protection Law defines sensitive personal data as personal data related to:

- Philosophical or political beliefs
- Political affiliations or trade union membership
- Religion
- Private life
- Racial or ethnic origin
- Health or sex life (including genetic data)

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Law establishes the *Agência de Proteção de Dados* (APD) as Angola's data protection authority. APD's Organic Statute was established by the Presidential Decree 214/2016 of October 10, and its board currently in office was nominee by the Presidential Decree 277/2019 September 6.

REGISTRATION

As provided by Law, entities shall provide prior notice to, or obtain prior authorization from, APD (depending on the type of personal data and purpose of processing) to process personal data. Please note that in the case of authorization, compliance with specific legal conditions is mandatory. APD has authority to exempt certain processing from notification requirements.

Generally, notification and authorization requests should include the following:

- The name and address of the controller and of its representative (if applicable)
- The purposes of the processing
- A description of the data subject categories and the personal data related to those categories
- The recipients or under which categories of recipient to whom the personal data may be communicated and respective conditions
- Details of any third party entities responsible for the processing
- The possible combinations of personal data
- The duration of personal data retention
- The process and conditions for data subjects to exercise their rights
- Any predicted transfers of personal data to third countries
- A general description (to allow APD to assess whether security measures adopted are suitable to protect personal data in its processing)

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Generally, entities must obtain prior express consent from data subjects and provide prior notice to the APD to lawfully collect and process personal data. However, data subject consent is not required in certain circumstances provided by law.

To lawfully collect and process sensitive personal data, a legal provision must allow for processing and entities must obtain prior authorization from APD (please note that the authorization may only be granted in specific cases provided by law). If sensitive personal data processing results from a legal provision, APD must be provided with notice.

All data processing must follow these general principles: transparency, legality, good faith, proportionality, truthfulness and respect to private life as well as to legal and constitutional guarantees.

It is also mandatory that data processing is limited to the purpose for which the data is collected and that personal data is not held for longer than is necessary for that purpose.

There are specific rules applicable to the processing of personal data related to the following:

- Sensitive data on health and sexual life
- Illicit activities, crimes and administrative offenses
- Solvency and credit data
- Video surveillance and other electronic means of control
- Advertising by email
- Advertising by electronic means (direct marketing)
- Call recording

Specific rules for the processing of personal data within the public sector also apply.

TRANSFER

International transfers of personal data to countries with an adequate level of protection require prior notification to the APD. An adequate level of protection is understood as a level of protection equal to the Angolan Data Protection Law. APD decides which countries ensure an adequate level of protection by issuing an opinion to this respect.

International transfers of personal data to countries that do not ensure an adequate level of protection are subject to prior authorization from the APD, which will only be granted if specific requirements are met. For transfers between companies in the same group, the requirement of an adequate level of protection may be reached through the adoption of harmonized and

mandatory internal rules on data protection and privacy.

Please note that the communication of personal data to a recipient, a third party or a subcontracted entity is subject to specific legal conditions and requirements.

SECURITY

Data controllers must implement appropriate technical and organizational measures and adopt adequate security levels to protect personal data from accidental or unlawful total or partial destruction, accidental loss, total or partial alteration, unauthorized disclosure or access (in particular where the processing involves the transmission of data over a network) and against all other unlawful forms of processing.

Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, relative to the entities facilities and implementation costs. Specific security measures shall be adopted regarding certain type of personal data and purposes (notably, sensitive data, call recording and video surveillance).

Under the Protection of Information Systems and Networks Law, service providers, operators and companies offering information society services must: (i) guarantee the security of any device or set of devices used in the storage, processing, recovery or transmission of computer data on execution of a computer program and (ii) promote the registration of users as well as the implementation of technical measures in order to anticipate, detect and respond to risk situations. The Law requires an accident and incident management plan in case of a computer emergency.

BREACH NOTIFICATION

There is no mandatory breach notification requirement under the Data Protection Law.

However, pursuant to the Electronic Communications and Information Society Services Law, companies offering electronic communications services accessible to the public shall, without undue delay, notify the APD and the Electronic Communications Authority, *Instituto Angolano das Comunicações*, (INACOM) of any breach of security committed with intent or that recklessly leads to destruction, loss, partial or total modification or non-authorized access to personal data transmitted, stored, retained or in any way processed under the offer of electronic communications services.

Companies offering electronic communications services accessible to the public shall also keep an accurate register of data breaches, indicating the concrete facts and consequences of each breach and the measures put in place to repair or prevent the breach.

The same applies under Protection of Information Systems and Networks Law.

ENFORCEMENT

Data protection

As mentioned above, the competent authority for the enforcement of Data Protection Law is the APD. However, considering that the APD was recently created, the level of enforcement is not significant at this stage.

Electronic communications

INACOM regulates and monitors compliance with the Electronic Communications and Information Society Services Law, and issues penalties for its violation. Presently, INACOM's level of enforcement is not yet significant.

ELECTRONIC MARKETING

The dissemination of electronic communications for advertising purposes is generally subject to the prior express consent of its recipient (opt-in) and to prior notification to APD.

Entities may process personal data for electronic marketing purposes without data subject consent in specific circumstances,

notably:

- When advertising is addressed to the data subject as representative employee of a corporate person, and
- When advertising communications are sent to an individual with whom the product or service supplier has already concluded a transaction, provided an opportunity to refuse consent was expressly provided to the customer at the time of the transaction at no additional cost.

ONLINE PRIVACY

The Electronic Communications and Information Society Services Law establishes the right of all Citizens to enjoy protection against abuse or violations of their rights through the Internet or other electronics means, such as:

- The right to confidentiality of communications and to privacy and non-disclosure of their data
- The right to security of their information by improvement of quality, reliability and integrity of the information systems
- The right to security on the Internet, specifically for minors
- The right not to receive spam
- The right to the protection and safeguarding of their consumer rights and as users of networks or electronic communications services

In view of the above, entities are generally prohibited from storing any kind of personal data without prior consent of the user. This does not prevent technical storage or access for the sole purpose of carrying out the transmission of a communication over an e-communication network or if strictly necessary in order for the provider of an information society service to provide a service expressly requested by the subscriber or user.

Traffic data

The processing of traffic data is allowed when required for billing and payment purposes, but processing is only permitted until the end of the period during which the bill may lawfully be challenged or payment pursued. Traffic data must be eliminated or made anonymous when no longer needed for the transmission of the communication.

The storage of specific information and access to that information is only allowed on the condition that the subscriber or user has provided his or her prior consent. The consent must be based on accurate, clear and comprehensive information, namely about the type of data processed, the purposes and duration of the processing and the availability of data to third parties in order to provide value added services.

Electronic communications operators may store traffic data only to the extent required and for the time necessary to market electronic communications services or provide value added services. Prior express consent is required and such consent may be withdrawn at any time.

Processing should be limited to those employees in charge of:

- Billing or traffic management
- Customer inquiries
- Fraud detection
- Marketing of electronic communications
- Services accessible to the public
- The provision of value added services

Notwithstanding the above, electronic communication operators should keep in an autonomous file all traffic and localization data exclusively for the purpose of:

- Investigation
- Detection, or
- Prosecution of criminal offenses on Information and Communication Technologies (ICT)

Location data

Location Data processing is only allowed if the data is made anonymous or to the extent and for the duration necessary for the provision of value added services, provided prior express consent is obtained. In this case, prior complete and accurate information must be provided on the type of data being processed, as well as the purposes and duration of processing and any possibility of disclosure to third parties for the provision of value added services.

Electronic communication operators must ensure that data subjects have the opportunity to withdraw consent, or temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication, at any time. The withdrawal mechanism must be provided through simple means, free of charge to the user. Processing should be limited to those employees in charge of electronic communications services accessible to the public.

KEY CONTACTS

ACDA



Joni Garcia

Associate
ACDA
T +244 926 61 25 25
j.garcia@adca-angola.com



Murillo Costa Sanches

Of Counsel
ACDA
T +244 926 61 25 25
m.sanches@adca-angola.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 © 2021 DLA Piper. All rights reserved.