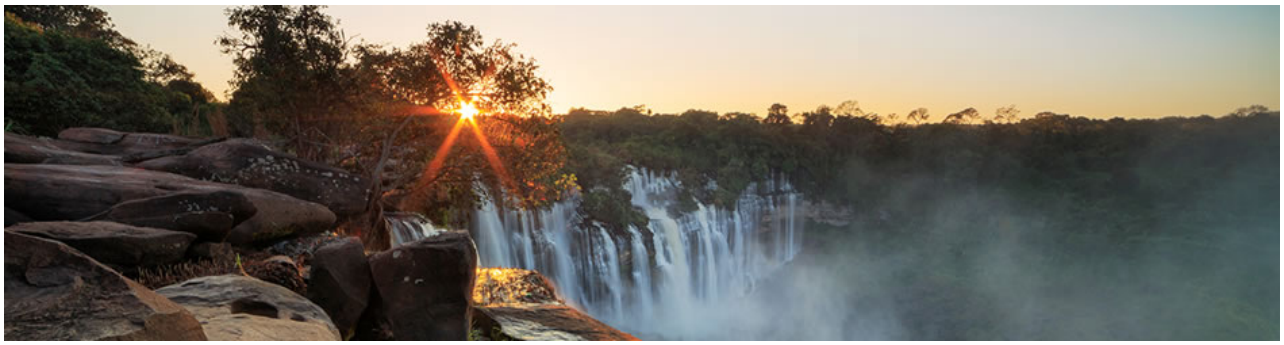
DATA PROTECTION LAWS OF THE WORLD

Angola

ANGOLA



Last modified 24 January 2018

LAW

Data Protection Law (Law no. 22/11 of 17 June), Electronic Communications and Information Society Services Law (Law no. 23/11, of 20 June 2011) and Protection of Information Systems and Networks Law (Law no. 7/17, of 16 February).

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 deemed to be an individual that may be directly or indirectly identified, notably, by reference to her/his identification number or to the combination of specific elements of her/his physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

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

- philosophical or politic 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

Agência de Proteção de Dados (APD). Although the Data Protection Law provides for the creation of the APD and in October 2016 it has been approved the Organic Statute of APD by Presidential Decree 214/2016 (which is in force), such authority has not yet been created.

REGISTRATION

In general terms, depending on the type of personal data and on the purposes of the processing either:

- prior notification to APD, or
- prior authorisation from the APD,

is required. Please note that in the case of authorisation, compliance with specific legal conditions are mandatory.

The APD may exempt certain processing from the notification requirement. In general terms, notification and authorisation requests should include the following information:

- 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 the conditions for a data subject to execute further rights of access, rectification, deletion, opposition and updating
- any predicted transfers of personal data to third countries
- a general description (which will allow the APD to assess the suitability of the measures adopted to ensure the processing security).

DATA PROTECTION OFFICERS

There is no obligation to appoint data protection officers.

COLLECTION & PROCESSING

In general terms, personal data collection and processing of personal data is subject to express and prior consent from the data subject and prior notification to the APD. However, data subject consent is not required in certain circumstances provided by law.

With respect to sensitive data processing, collection and processing is only allowed where there is a legal provision allowing such processing and prior authorization from the APD is obtained (please note that the authorization may only be granted in specific cases provided by law). If the sensitive personal data processing results from a legal provision, the same shall be notified to APD.

In any case data processing must fulfull the following general principles: transparency, legality, good faith, proportionality, truthfulness, and respect to private life as well as to the 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:

- 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 which do not ensure an adequate level of protection are subject to prior authorization from the APD which will only be granted in case specific requirements are fulfilled. In case of transfers between the companies of 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 however, 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

The data controller must implement appropriate technical and organizational measures and to adopt adequate security levels in order to protect personal data against 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.

Having regard to the state of the art and the cost of their implementation, 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. Specific security measures shall be adopted regarding certain type of personal data and purposes (notably, sensitive data, call recording and video surveillance).

Also, according to Protection of Information Systems and Networks Law the service providers, operators and companies offering information society services must: (i) guarantee the security of any device or set of devices used on the storage, processing, recovery or transmission of computer data on execution of a computer programme 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 computer emergency.

BREACH NOTIFICATION

There is no mandatory breach notification 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 recklessly that leads to destruction, loss, partial or total modification or non-authorized access to personal data transmitted, stored, retained or by 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 is not yet created, the level of enforcement is not significant at this stage.

Electronic Communications

INACOM regulates, inspects and verifies compliance with the Electronic Communications and Information Society Services Law, and applies the penalties related to violations of it. Although, unlike the APD, the INACOM exists, the level of enforcement is still not significant yet.

ELECTRONIC MARKETING

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

The processing of personal data for this purpose may be conducted without data subject consent in specific circumstances, notably:

- when the advertising is addressed to the data subject as representative, employee of a corporate person and
- when the advertising communications are sent to an individual with whom the supplier of a product or a service has already concluded transactions provided the opportunity to refuse was expressly provided to the customer at the time of the transaction and this does not involve an additional cost. In this case, the data subject has the right to oppose to his personal data processing for advertising/direct marketing purposes.

ONLINE PRIVACY

The Electronic Communications and Information Society Services Law establishes the right for all Citizens to enjoy protection against abuse or violations of their rights through the Internet or by 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 protection and safeguarding to their consumer rights and as users of networks or electronic communications services.

In view of the above it is in general not allowed to store 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/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 storing of specific information and the access to such information is only allowed on the condition that the subscriber/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 communication operators may also store traffic data only to the extent required and 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 data and localization data exclusively for the purpose of:

- investigation
- detection or
- prosecution of criminal offences on Information and Communication Technologies (ICT).

Location data

The processing of Location Data 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 the processing and the possibility of disclosure to third parties for the provision of value added services.

Electronic communication operators must ensure the possibility to withdraw consent at any time, or temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication. This shall be provided by using simple means, which are free of charge to the user. The processing should be limited to those employees in charge of electronic communications services accessible to the public.

The Location Data may be kept for criminal investigation or evidence purposes.

KEY CONTACTS

VCA – Law Firm
www.vca-angola.com

Orlanda Vuite
Associate
ADCA Advogados Angola
T +244 926 61 25 25
o.vuite@adca-angola.com

Carmina Cardoso
Of Counsel
T +244 926 61 25 25
c.cardoso@vca-angola.com

DATA PRIVACY TOOL

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