DATA PROTECTION LAWS OF THE WORLD

Angola vs Honduras

DLA PIPER

ANGOLA

Last modified 30 December 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

HONDURAS

Last modified 24 January 2022

LAW

Personal data protection is regulated mainly in:

National Constitution: Article 182 provides the constitutional protection of habeas data, giving individuals the right 'to access any file or record, private or public, electronic or hand written, that contains information which may produce damage to personal honour and family privacy. It is also a method to prevent the transmission or disclosure of such data, rectify inaccurate or misleading data, update data, require confidentiality and to eliminate false information. This guarantee does not affect the secrecy of journalistic sources.'

Law of the Civil Registry (Article 109, Decree 62-2004). This law refers only to public personal information that is contained in the archives of the Civil Registry.

Law for Transparency and for Access to Public Information (Article 3.5, Decree 170-2006). This law enables the access of any person to all the information contained in public entities, except that which is classified as 'Confidential.' It also extends the constitutional protection of habeas data and forbids the transmission of personal information that may cause any kind of discrimination or any moral or economic damage to people.

Rulings on the Law for Transparency and for Access to Public Information (Article 42, Accord 001-2008). Provide a definition of databases containing personal confidential information, and requires data subject consent, prior to the use of it by any third party.

In addition, the Law for the Protection of Confidential Personal Data (the "Law") is currently in discussion in the Honduran Congress. Congress has approved the first chapters of the Law. The complete approval of the Law and the date for when the Law will enter into force is expected in the first half of 2019.

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 stablished by the Presidential Decree 214/2016 of October 10, and it's board currently in office was nominated by the Presidential Decree 277/2019 September 6.

Public Personal Data under the Law of the Civil Registry is defined as: Public Data whose disclosure is not restricted in any way, and includes the following:

- Names and surnames
- ID number
- Date of birth and date of death
- Gender
- Domicile (but not address)
- Job or occupation
- Nationality
- Civil status

Definition of sensitive personal data

The Law for Transparency and for Access to Public Information defines 'Sensitive Personal Data' as: "Those personal data relating to ethnic or racial origin, physical, moral or emotional characteristics, home address, telephone number, personal electronic address, political participation and ideology, religious or philosophical beliefs, health, physical or mental status, personal and familiar heritage and any other information related to the honor, personal or family privacy, and self-image."

Other Definitions:

- Consent: Written and express authorization of the person to whom the personal data refers in order to disclose, distribute, commercialize, and/or use it in a different way as it was originally given for
- Confidential Information: Information provided by particular persons to the government which is declared confidential by any law, including sealed bids for public tenders
- Classified Information: Public information classified as that by the law, and / or by resolutions issued by governmental institutions

NATIONAL DATA PROTECTION AUTHORITY

Two entities are responsible for enforcing personal data protection:

1. National Civil Registry
   http://www.rnp.hn

2. Institute for the Access to Public Information
   http://www.iaip.gob.hn

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

REGISTRATION

Only Obligated Entities must inform the Institute for the Access to Public Information of their databases. Obligated Entities are:

- Government institutions
- NGO's
- Entities that receive public funds, and
- Trade unions with tax exemptions

The Institute for the Access to Public Information will maintain a list of the databases of the above-mentioned entities.

DATA PROTECTION OFFICERS

Only Obligated Entities must appoint a data protection officer.

COLLECTION & PROCESSING

Individuals, companies, and / or Obligated Entities that collect personal data may not use sensitive personal data or confidential information without the consent of the person to whom such information relates.

However, consent is not required to use or transfer personal data in the following cases:

- If the information is used for statistical or scientific needs, but only if the personal data is provided in a way that it cannot be associated with the individual to whom it relates

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

- If the information is transmitted between Obligated Entities, only if the data is used in furtherance of the authorised functions of those entities
- If ordered by a Court
- If the data is needed for the purpose it was provided to the individual or company to perform a service. Such third parties may not use personal information for purposes other than those for which it was transferred to them
- In other cases established by law

TRANSFER

Individuals and / or companies may not transfer, commercialize, sell, distribute or provide access to personal data contained in databases developed in the course of their job, except with the express and direct written consent of the person to whom that data refers, subject to certain exceptions.

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

The Institute for the Access to Public Information has the authority to require all Obligated Entities to take necessary security measures for the protection of the personal data they collect and / or use.

The current legislation neither clarifies nor specifically identifies the security policies or security mechanisms that Obligated Entities must comply with.

As a general statement, the Institute for the Access to Public Information has to ensure the security of all Public Information, of all information classified as confidential by public entities, of all sensitive personal data, and of all information to which the current legislation gives a secrecy status.

BREACH NOTIFICATION

Breach notification is not required.

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

ENFORCEMENT

The Institute for the Access to Public Information may receive complaints about abuses regarding the collection of personal or confidential data.

The Institute will impose corrective measures and establish recommendations for those persons or companies who disclose personal data, sensitive personal data or confidential data without authorization.

ELECTRONIC MARKETING

There is no law or regulation that specifically regulates electronic marketing.

ONLINE PRIVACY

There is no law or regulation that specifically regulates online privacy.

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.

KEY CONTACTS

Bufete Gutiérrez Falla y Asociados
www.gufalaw.com/

Julio Alejandro Pohl Garcia Prieto
Associate
T +504 2238-2455
julio.pohl@gufalaw.com

DATA PRIVACY TOOL

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