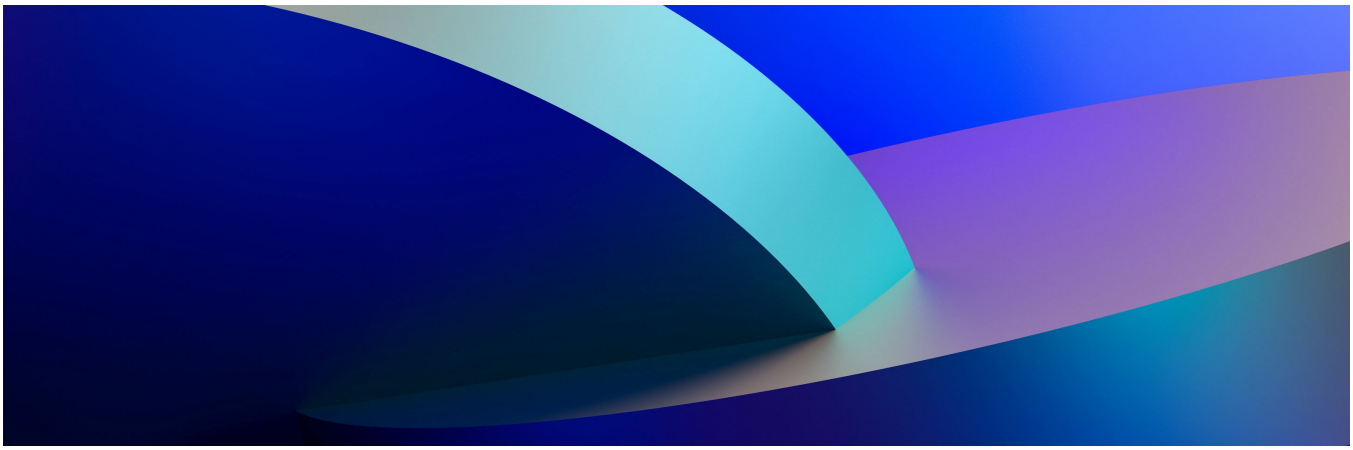

# Data protection and cybersecurity laws in Angola

## Data protection

### 1. Local data protection laws and scope

- **Law no. 22/11**, of 17 June (Data Protection Law);
- **Law no. 23/11**, of 20 June (Law of Electronic Communications and Information Services);
- **Law no. 7/17**, of 16 February (Law of Network and IT Systems Protection);
- **Presidential Decree no. 108/16**, of 25 May (General Electronic Communications Regulation);
- **Presidential Decree no. 202/11**, of 22 July (Regulation on Information Technologies and Services);
- **Resolution 33/19 of 9 July** (African Union Convention on Cybersecurity and Data protection);
- **Law no. 2/20**, of 22 January (Video surveillance);
- **Law no. 11/20**, of 23 April (Mobile Identification or Location and Electronic Surveillance);
- **Law no. 38/20**, of 11 November (Angolan Criminal Code);
- **Presidential Decree 275/20**, of 21st October (Regulation of the Activity of the Private Credit Information Centres).

### 2. Data protection authority

Agency of Data Protection (APD): https://www.apd.ao/ao/

### 3. Anticipated changes to local laws

There are no relevant anticipated changes to local laws.

### 4. Sanctions & non-compliance

APD under the current law has administrative supervision and enforcement powers.

According to Angolan Law, APD has the power to impose fines regarding **Administrative Sanctions**, as follows:

**1. Law no. 22/11, of 17 June**

Violation of specific requirements for the processing of personal data, non-compliance with the obligation of notifying APD and non-compliance with the APD provisions to cease access to open data

transmission networks to data controllers who do not comply with the law from USD 75,000 up to USD 150,000

Violation of specific requirements for the processing of personal data, the violation of data processing principles and data processing without consent from data subjects from USD 65,000 up to USD 130,000.

**Note:** The attempt of any of the above-mentioned misdemeanour actions or omissions is punishable.

**2. Law no. 23/11, of 20 June**

Violation of security provisions, violation of confidentiality and violation of traffic data from USD 30,000 up to 150,000.

**3. Law no. 7/17, of 16 February**

Non-compliance with the provisions of this law, or the violation of any of the requirements in the scope of data protection and security in the networks and information systems leads to the application of fines set at the amount from AOA 7m up to AOA 200m.

#### Criminal sanctions

**1. Law no. 22/11, of 17 June**

**Non-compliance with data protection obligations**

Prison sentence of three months up to 18 months, or a corresponding fine.

**Unauthorised access Tampering or destruction of personal data**

Prison sentence from six months to two years.

**Qualified disobedience**

Prison sentence up to three years.

**Breach of confidentiality duty**

Prison sentence up to 18 months or a corresponding fine.

**Note:** The attempt of any of the above-mentioned crimes is punishable with prison sentence up to six months, or a corresponding fine.

**2. Law no. 38/20, of 11 November (Angolan Criminal Code)**

**Electronic Falsehood**

Whoever, with intent to mislead or harm, inputs, alters, deletes or suppresses data in an information system or, in general, interferes with the processing of such data in such a way as to produce false data that may be considered true and used as evidence, shall be punished prison sentence up to two years or the application of a fine up to 240 days.

**Information Technology Data Damage**

Whoever, with intent to cause damage to a third party or to obtain benefit for himself or for a third party, alters, deteriorates, renders useless, deletes, suppresses or destroys, in whole or in part, or in any way renders other people's data inaccessible, shall be punished prison sentence from one year up to 12 years or the application of a fine up to 360 days.

**Illegitimate reproduction of computer program, databases and topography of**

**semiconductor products**

Prison sentence from two years up to three years or the application of a fine from 240 days up to 360 days.

**Note:** The attempt of any of the above-mentioned crimes is punishable.

**5. Registration / notification / authorisation**

According to Law no. 22/11, of 17 June, the processing of personal data is subject to prior notification or authorisation by the Data Protection Agency.

If mere notification is required, the Data Protection Agency must take a decision on the request made by the data controller within 30 days of receipt of the request.

The notifications and requests for authorisation sent to the APD must contain the following information:

- Identification of the data controller;
- Purpose of processing;
- Description of the category of data and respective data subjects;
- Identification of the recipients;
- Any interconnection of processing of personal data;
- Period of data retention;
- How the exercise of the rights of the data subjects is guaranteed;
- Planned data transfers to third countries;
- Preliminary description of the security measures adopted.

**6. Main obligations and processing requirements**

In accordance with the APD's guidelines and the national data protection law itself, the data controller's obligations are:

- To notify the APD in advance of any processing or combination of processing of personal data, totally or partially autonomous, intended to serve one or more interrelated purposes;
- To notify the APD of any subsequent changes that may occur;
- To process data lawfully, legally and in good faith;
- To collect data for specified, explicit and legitimate purposes;
- Collect data that is adequate, relevant and not excessive in relation to the purposes for which it is collected and subsequently processed;
- Ensure that data are accurate and up-to-date and take reasonable steps to ensure that inaccurate or incomplete data are erased or rectified;
- To provide the data subject with all information required by law, without forgetting the specific information required when data is collected over open networks;
- Not to process personal data in a way incompatible with the purposes for which they have been collected. If the data controller intends to carry out processing, it must first request the authorisation of the APD or the consent of the data subjects;
- To guarantee the data subject a right of access, freely and without restrictions, at reasonable intervals and without excessive delays or costs;
- Guarantee the data subject the right to freely exercise the right to object to processing for the purposes of direct marketing or any other form of prospecting;
- Obtain prior consent from data subjects for the purposes of direct marketing using automated calls or fax machines;
- Obtain and maintain consent from the data subject for the processing of personal data;

- Implement technical and organisational measures to ensure data protection against accidental loss, destruction, alteration, unauthorised disclosure or access. It shall also enforce the legal obligation of professional secrecy with respect to the processed personal data;
- Not to interconnect personal data unless authorised by the APD or required by law;
- Whoever has access to personal data obtain through video-surveillance systems is obliged to comply with professional secrecy;
- Personal data accidentally obtained by the video-surveillance systems, relating to intimate or personal data of a purely social nature and which do not have criminal relevance, should be destroyed immediately by the responsible person for the system;
- Not to communicate data to third parties that have not notified their processing to the APD;
- To destroy the personal data once the authorised storage period has expired;
- To stop the processing of personal data when a situation arises that is not in accordance with the law and has been instructed to do so by the competent authority.

Other obligations are established in separate legislation, which are foreseen in Law no. 7/17, of 16 February, that determines the Network and IT Systems Protection legal regime, as follows:

- Operators of information systems shall proceed with the encryption of electronic communication networks in order to guarantee the technical and security conditions under which communication is carried out for the transmission of traffic and location data relating to natural and legal persons;
- Cyberspace operators and service providers must submit to APD and INACOM an accident and incident management plan, in the event of a computer emergency, before commencing activities;
- The use of databases must obey the technical standards and specialised procedures of adequate protection of access, storage, duplication of files, treatment and recovery of automated information.
- Electronic communications operators shall ensure that retained data are of the same quality and subject to the same security and protection as those data on the network;
- Electronic communications operators shall take appropriate technical and organisational measures to protect data against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure;
- Electronic communications operators shall take appropriate technical and organisational measures to ensure that only authorised employees and partners (including processors) have access to personal data;
- Electronic communications operators must destroy personal data as soon as the information is no longer necessary for the purpose for which it was collected or if required by instruction of the competent authorities.

**7. Data subject rights**

**Law no. 22/11**, of 17 June, comprises the following rights that may be exercised by data subjects:

- Right to information;
- Right of access;
- Right to object;
- Right of rectification and erasure;
- Right to non-automated individual decisions.

**8. Processing by third parties**

Personal data may only be communicated to a data processor under a contract or other legal document, in writing, which establishes the obligation of the processor to comply with the provisions of the Angolan Data Protection Law and act in accordance with the instructions of the data controller.

Subsequently, it will be necessary to notify the APD of such transfer.

**9. Transfers out of country**

International transfer of data to countries that ensure an adequate level of protection (guarantee of protection as established in Angolan law) is subject to notification to the Data Protection Agency (APD), which will issue an assessment report.

The transfer of data to a country that does not guarantee an adequate level of protection is subject to authorisation by the APD, which can only be granted if one of the following circumstances or others established in specific legislation are verified:

- Consent of the data subject;
- Transfer arises from the application of international law;
- Humanitarian purpose;
- Transfer necessary for the execution of a contract, at the request of the parties;
- Necessary transfer to protect public interests or to defend a right in legal proceedings;
- Transfer necessary to protect the vital interests of the data subject;
- Transfer through a source accessible to the public;
- If the recipient guarantees contractually adequate data protection.

Data transfer by electronic means should be carried out at a high level of encryption and protection according to the state of the art, including encoding, ciphering or other methods.

**10. Data Protection Officer**

The appointment of a data protection officer is not legally required.

**11. Security**

Law no. 22/11, of 17 June, clearly provides that the data controller must implement appropriate technical and organisational measures to safeguard the data processing risks, for example:

- Prevent unauthorised persons from having access to the files and processing facilities;
- Prevent unauthorised persons from reading, copying, use, modify or remove data supports;
- Ensure the verification of the entities to whom the personal data may be transmitted through the data transmission facilities.

**12. Breach notification**

There is no legal or institutional provision for reporting mechanisms on personal data breaches. The APD recommends direct contact with the data controller by the data subject and, in the event of non-compliance practices, the data subject should file a complaint before the APD, mentioning the identification of the alleged perpetrator and documents or other evidence to support the allegations.

Notwithstanding, regarding a security breach that compromises the integrity of personal data and other information, Law no. 23/11, of 20 June, establishes that the operator must notify immediately the APD and INACOM.

For any breach regarding information systems, within the scope of Law no. 7/17, of 16 February, it is the responsibility of the operators of electronic communication network services to implement the preventive services of warnings, alerts, recommendations and information on security, in order to ensure the continuous promotion of network integrity and reliability.

**13. Direct marketing**

Regarding advertising and marketing matters, Angola enacted Law no. 23/11, of 20 June referent to

Electronic Communications and Information Services which foresees the consumer's right not to receive unsolicited emails and the right to the protection of their rights when acquiring products and services on the internet and in relation to advertising.

For this matter, Resolution no. 33/19 of 9 July (African Union Convention on Cybersecurity and Data Protection) establishes that the direct marketing is authorised in the following situations:

- The address details of the recipient are obtained directly from the recipient;
- The recipient has consented to be contacted by the marketing partners of the issuer;
- Direct marketing refers to similar products or services provided by the same individual or company.

**14. Cookies and adtech**

Angola has no particular rule regarding the use of Cookies. Hence, the general legal framework on data protection shall apply.

**15. Risk scale**

Low

**16. Useful links**

- APD website
- INACOM website

## Cybersecurity

**1. Local cybersecurity laws and scope**

- **Resolution 33/19 of 9 July** (African Union Convention on Cybersecurity and Data protection);
- **Law 38/20**, of 11 November (Angolan Criminal Code);
- **Law no. 23/11**, of 20 June (Law of Electronic Communications and Information Services);
- **Law no. 7/17**, of 16 February (Law of Network and IT Systems Protection);
- **Presidential Decree no. 108/16**, of 25 May (General Electronic Communications Regulation);
- **Presidential Decree no. 202/11**, of 22 July (Regulation on Information Technologies and Services);
- **Presidential Decree 275/20**, of 21st October (Regulation of the Activity of the Private Credit Information Centres).

**2. Anticipated changes to local laws**

There are no relevant anticipated changes.

**3. Application**

- **Resolution 33/19 of 9 July** (African Union Convention on Cybersecurity and Data Protection);
- **Law no. 38/20**, of 11 November (Angolan Criminal Code).
- **Law no. 7/17**, of 16 February (Law of Network and IT Systems Protection);

**4. Authority**

In Angola there is still no culture of cybersecurity in organisations and government bodies (executive). What does exist is an embryonic structure that has been in the process of carrying out some cybersecurity tests.

However, the creation of a cybersecurity regulatory authority and specific legislation to regulate this matter is still absent.

**5. Key obligations**

- According to **Law no. 7/17**, of 16 February (Law of Network and IT Systems Protection), cyberspace networks should ensure the integrity, confidentiality and privacy of communications by implementing logical and physical security services.
- The body responsible for promoting the information society service providers and operators must ensure the security of any device or set of devices for storing, processing, retrieving or transmitting digital data when running a computer program.
- Internet operators and service providers shall promote the registration of users and the implementation of measures and necessary tools for the anticipation, detection, reaction and recovery in situations of network security threats.
- Cyberspace operators and service providers must submit to APD and INACOM an accident and incident management plan, in the event of a computer emergency, before commencing activities.
- Additionally, operators shall proceed with the encryption of electronic communication networks in order to guarantee the technical and security conditions under which communication is carried out for the transmission of traffic and location data relating to natural and legal persons.

**6. Sanctions & non-compliance**

**Criminal sanctions:**

**1. Law no. 38/20, of 11 November (Angolan Criminal Code)**

**Illegal access to information system and raid through information system**

Prison sentence from two years up to eight years, or an application of a fine up to 240 days.

**Illegitimate interception in information system**

Prison sentence from two years up to eight years, or the application of a fine up to 240 days.

**IT sabotage**

Crimes against communications and information systems are punishable with prison sentence from two years up to eight years, or the application of a fine up to 240 days.

**IT Falsehood**

Prison sentence from two years up to ten years, or the application of a fine from 240 days up to 360 days.

**Illegitimate reproduction of computer program, databases and topography of semiconductor products**

Prison sentence from two years up to three years, or the application of a fine from 240 days up to 360 days.

**Illegitimate interception in information system**

Whoever, by technical means, intercepts or records non-public transmissions of data processed within an information system shall be punished by a prison sentence from two to eight years, or a fine up to 240 days.

**Note:** An attempt of any of the above-mentioned crimes is also punishable.

**7. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?**

In Angola there is still no culture of cybersecurity in organisations and government bodies (executive). What does exist is an embryonic structure that has been in the process of carrying out some cybersecurity tests.

Thus, the creation of a cybersecurity regulatory authority and specific legislation to regulate this matter is still absent.

For any breach regarding information systems, within the scope of Law no. 7/17, of 16 February, it is the responsibility of the operators of electronic communication network services to implement the preventive services of warnings, alerts, recommendations and information on security, in order to ensure the continuous promotion of network integrity and reliability.

**8. National cybersecurity incident management structure**

In Angola there is still no culture of cybersecurity in organisations and government bodies (executive). What does exist is an embryonic structure that has been in the process of carrying out some cybersecurity tests.

Thus, the creation of a cybersecurity regulatory authority and specific legislation to regulate this matter is still absent.

For any breach regarding information systems, within the scope of Law no. 7/17, of 16 February, it is the responsibility of the operators of electronic communication network services to implement the preventive services of warnings, alerts, recommendations and information on security, in order to ensure the continuous promotion of network integrity and reliability.

**9. Other cybersecurity initiatives**

A national framework to strengthen cybersecurity is being planned, however, prior to execution, a convention has been concluded among African countries to create guidelines to combat cybersecurity, which is the only specific legislative instrument in force.

**10. Useful links**

N/A

# Key Contacts

Alberto Galhardo Simões
Lisbon
Partner
Partner

# Authors

João Leitão Figueiredo
Lisbon
Partner
Partner

João Rodrigues
Senior Associate
left_cms