FACTSHEET: ANGOLA

Last updated: 31 March 2020
Prepared by Justin Bryant
Revised by Tshepiso Hadebe

FAST FACTS

Population: 32,516,498
Capital: Luanda
President: João Manuel Gonçalves Lourenço
2019 Freedom House Score: 31/100
Data protection law? Exists, not enforced

LAW

The Data Protection Law (Law 22/11) was drafted to meet Angola's unique challenges and cultural realities. It draws on provisions from the EU and Portuguese legal regimes for the protection of personal data. While the law was signed in 2011, the enforcement authority, known as the *Agência de Proteção de Dados* (APD), was only created in October 2019 and there is presently no significant level of enforcement.

Data subjects have the right to:

- access their personal data;
- have their personal data corrected or deleted;
- ask a responsible party to limit the activities for which their data is used;
- not be subject to decisions based solely on automatic processing that would significantly affect them; and
- object to the use of their personal data for advertising purposes.

PERSONAL DATA

Personal data is any given information, regardless of its nature, including images and sounds related to a specific or identifiable individual.

Sensitive personal data is personal data related to:

- philosophical or political beliefs;
- political affiliations or trade union membership;
- religion;
- private life;
- racial or ethnic origin; or
- health or sex life (including genetic data).

To lawfully collect and process sensitive personal data, a legal provision must allow for processing and entities must obtain prior authorisation from the APD. If sensitive personal data processing results from a legal provision, the APD must be provided with notice.

COLLECTION AND PROCESSING

Except in certain circumstances provided by law, entities must obtain prior consent from data subjects and give prior notice to the APD to lawfully collect and process personal data.

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

Data processing must be limited to the purpose for which the data is collected, and personal data must not be 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); and
- call recording.

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

REGISTRATION AND ENFORCEMENT

Law 22/11 establishes the APD as Angola's data protection authority. Presidential Decree 214/16 approved the APD's Organic Statute in October 2016 and the APD was ultimately created in October 2019. Law 22/11 creates no requirement for data controllers to appoint data protection officers.

CROSS-BORDER TRANSFER

The APD must be notified prior to any international transfers of personal data to countries deemed to have an adequate level of protection.

Cross-border personal data transfers to countries without an adequate level of protection must be authorised by the ADP, and specific requirements must be met. Harmonised, compulsory internal data protection and privacy rules may demonstrate an adequate level of protection for transfers between companies in the same group.

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

SECURITY AND BREACH PROTOCOL

Law 22/11 does not mandate the reporting of data breaches, but under the Electronic Communications and Information Society Services Law, companies that offer electronic communications services to the public shall must notify the APD and the *Instituto Angolano das Comunicações*, (INACOM) of any security breach that jeopardises personal data as soon as possible.

These companies must also keep an accurate register of data breaches, with the concrete facts and consequences of each breach, and the measures put in place to remedy or stop the breach.

This protocol is also required under the Protection of Information Systems and Networks Law 7/17.

Read the legal notice and terms of use for this factsheet.