

FACTSHEET: BURKINA FASO

Last updated: 31 March 2020

Prepared by Justin Bryant

Revised by Tshepiso Hadebe



FAST FACTS

Population: 20,708,683

Capital: Ouagadougou

President: Roch Marc Christian Kaboré

2019 Freedom House Score: 60/100

Data protection law? Enforced

LAW

The Constitution of Burkina Faso, 1991 provides for the right to privacy and confidentiality of correspondence. [Law N°010- 2004/AN](#) was passed to apply these rights to individuals' personal data, and in 2007, Burkina Faso became the first French speaking country in sub-Saharan Africa with an operative data protection authority, the [Commission de l'Informatique et des Libertés](#) (CIL). As the body has been functioning for over a decade, it has had time to discover certain flaws in the law and in its implementation and highlight areas in need of reform. A revision of the law has been drafted, but not yet passed.

Under Law N°010- 2004/AN, individuals have the right to:

- be informed at the time of collection of the purposes for which the data are used and the identity of the data controller;
- access their personal data without delay or excessive costs;
- oppose, for legitimate reasons, the processing of personal data concerning them;
- oppose the processing of personal data for marketing or advertising;
- correct personal data being held about them if it is inaccurate or incomplete; and
- not be subject to decisions made on the sole basis of an automated processing that would produce adverse legal ramifications for them.

PERSONAL DATA

Personal data is information in any form that allows, directly or indirectly, for the identification of persons by reference to an identification number, or to elements specific to their physical, psychological, philosophical, economic, cultural, or social identities.

Unless otherwise provided by law, it is forbidden to collect or process personal data related to a data subject's **health, racial origins, ethical, political, philosophical or religious opinions, union membership, or behaviours, without his, her or their consent.**

COLLECTION AND PROCESSING

The data protection principles in Law N°010- 2004/AN reflect those found elsewhere in the [Convention of the African Union](#) and the [ECOWAS Supplementary Act](#). These principles include:

- **consent and legitimacy:** unless otherwise provided by law, data controllers are obligated to obtain consent from the data subject;
- **purpose:** personal data can only be collected and processed for a specific and legitimate purpose;
- **proportionality and relevance:** personal data must only be processed in a relevant and necessary manner regarding the purpose and objectives of the processing;
- **lawfulness and fairness:** data controllers must collect and process data in a fair, lawful, and not fraudulent manner;
- **data retention:** a specified period of time should be determined in advance depending on the purpose of processing to ensure that personal data is not stored indefinitely;
- **security and confidentiality:** all responsible persons for processing personal data must not only ensure the security of data or files to prevent their destruction, or alteration; but also prevent unauthorised access to personal data contained in a file or intended to form part of the file; and
- **preliminary formalities:** without exception or exemption provided by law, all data controllers shall, depending on the nature of personal data processing, notify the CIL or ask his opinion or obtain approval, etc.

REGISTRATION AND ENFORCEMENT

The CIL as an independent regulatory authority, drawing its membership from various segments of society. The body is charged with:

- making individual or regulatory decisions in cases provided for under the law;
- assisting with data processing inspections and obtaining all information and documents needed for its mission;
- issuing model rules to ensure security; and where appropriate, prescribing safety measures including the destruction of information;
- issuing enforcement notices to data controllers and sharing with the prosecutor's office the offences of which the body is aware;
- ensuring that the implementation of the right of access and rectification indicated in the acts and declarations do not impede the free exercise of this law;
- receiving complaints and petitions;
- staying informed of the latest technological developments, and keeps abreast of their effects on the right to privacy, the exercise of freedoms, and the functioning of democratic institutions;
- advising individuals and organisations that use automated processing, or who carry out tests or experiments likely to lead to such processing;
- responding to requests for public opinion; and
- proposing legislation or regulations to the Government to adapt the protection of freedoms to technological evolution.

CROSS-BORDER TRANSFER

The CIL allows International data transfers by legal or contractual means. The legal process necessitates that the host country either has comprehensive personal data protection legislation or its legal system otherwise provides adequate protection. The contractual process, in case of the absence of data protection legislation, requires two companies to abide by a contract of the personal data transfer in accordance with the protection legislation. The

CIL recognises the binding corporate rules (BCR) of the [*Association francophone des autorités de protection des données*](#) (AFAPDP) as an alternative to the contractual process.

SECURITY AND BREACH PROTOCOL

No breach notification protocol is stipulated under Burkinabe law.

Read the [*legal notice*](#) and [*terms of use*](#) for this factsheet.