FACTSHEET: BENIN

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

FAST FACTS

Population: 12,015,718
Capital: Porto-Novo
President: Patrice Talon
2019 Freedom House Score: 79/100
Data protection law? Enforced

LAW

The data protection regime in Benin is governed by Book V of the 2017 Digital Code of the Republic of Benin: Protection of Personal Data, and Law No. 2009-09: Dealing with the Protection of Personally Identifiable Information (PII).

These laws have considerable overlap but differ slightly in their scope. Law No. 2009-09 pertains to the digital processing of personally identifiable information in digital files or manuals, as well as personal identification mechanisms based on nominative, personal, and biometric information processed alongside a national ID number.

Book V pertains to the collection, treatment, transmission, storage, and use of personal data by a person, the state, local authorities, and legal persons, as well as automated processing and non-automated processing of personal data contained in files, or any processing of data for public security, defense, research, prosecution of criminal offenses, or the security and essential interests of the state.

Under Beninese law, individuals have:

- the right to obtain all of their personal data in an understandable form, as well as any available information as to their origin;
- the right to withdraw consent for personal data processing at any time;
- the right to object, for legitimate reasons, to the processing of personal data concerning them;
- the right to oppose the processing of their personal data for prospecting purposes;
- the right to rectify or erase personal data where it is inaccurate or incomplete;
- the right to not be subject to decisions made on the sole basis of an automated processing that would produce significant risks or harm;
- the right to be forgotten, or to have information made public about themselves deleted from record; and
- the right to obtain compensation from data controllers who, in violating the law, cause material or moral damage to a person.

PERSONAL DATA

Personal data is any information regardless of its form, including sounds and images, related to an identified or identifiable natural person.

Sensitive data is all personal data related to a person's **personal opinions, philosophical or religious beliefs, political activities, trade union membership, sexual life, race, health, genetics, prosecutions and criminal or administrative sanctions**.

Processing of sensitive data is prohibited barring certain exceptions.

COLLECTION AND PROCESSING

Personal data processing is considered legitimate if there is consent from the data subject. This requirement may be waived where processing is necessary for:

- compliance with a legal obligation to which the controller is subject;
- the performance of a public interest mission or the exercise of public authority;
- the commencement or performance of a contract in the data subject's interests or to which they are a party; or
- safeguarding the interests or fundamental rights and freedoms of the data subject.

Personal data should be:

- processed legitimately;
- collected, recorded, processed, and stored fairly, lawfully, transparently, and not fraudulently;
- collected for specific and legitimate purposes, and not subsequently processed for other purposes inconsistent with those originally stated;
- adequate, relevant, and not excessive in relation to the purposes for which personal data is collected and processed;
- accurate and updated, if necessary;
- kept in a form that allows for the identification of data subjects for no longer than the period necessary to achieve the aforementioned purposes; and
- processed to ensure adequate safety, including protection against damage, destruction, or unauthorised processing.

Interconnection of personal data shall:

- not discriminate against or infringe on the fundamental rights, freedoms, and guarantees of holders of the data;
- ensure the use of appropriate safety measures; and
- take into account the principle of relevance.

REGISTRATION AND ENFORCEMENT

The *Autorité de protection des données à caractère personnel* (APDP) is tasked with ensuring the application of the provisions of Book V and respect for privacy in general. It is an independent administrative body with legal personality and full autonomy. Among other things, its responsibilities include:

- raising public awareness of the risks, rules, and rights surrounding the processing of personal data;
- authorizing or denying requests for processing;
- receiving and investigating complaints about the misuse of personal data;
- conducting necessary inspections regarding personal data processing, and obtaining all information and documents needed;
- informing data controllers of alleged violations of the law and issuing mandatory measures for remedying these violations;
- imposing administrative sanctions on data controllers in the case of noncompliance;
- informing the public prosecutor of offenses committed under the law;
- keeping a public register of personal data processing operations;
- issuing public opinions on the state of data protection law;
- proposing amendments to simplify and improve data protection legislation, where necessary; and
- cooperating with international data protection authorities to share information and assistance, as well as participating in international negotiations.

Data controllers are required to file an annual report with the APDP concerning compliance with the processing principles.

Data controllers and processors are also required to appoint a data protection officer if:

- the processing is carried out by an authority public body or a public body, except courts acting in the exercise of their judicial function;
- the basic activities of the controller or processor consist of operations which, because of their nature, scope and / or purpose, require regular and systematic follow-up due to the scale of the people involved; or
- the basic activities of the controller or processor consist of a large-scale processing of sensitive data.

In cases other than those mentioned above, data controllers and processors may still designate a data protection officer. A group of companies or public bodies can designate a single data protection officer provided that the individual is easily accessible from each establishment, and that such an arrangement is appropriate given their organisational structure and size.

CROSS-BORDER TRANSFER

Transfer of personal data to another country is allowed only when that country provides a level of protection equivalent to that put in place by the provisions of Book V. Before any transfer of personal data to another country or an international organization, the controller must obtain prior authorization from the APDP.

The transfer of personal data to a country which does not ensure an adequate level of protection may be permitted if the data subject has given consent to the transfer or where such transfer is:

- necessary for the commencement or performance of a contract between the data subject and the data controller, or at the data subject's request;
- necessary for the execution or conclusion of a contract awarded in the interest of the data subject, or between the data controller and a third party;

- required for the protection of an important public interest, or for the declaration, exercise, or defence of a right in judicial proceedings;
- necessary to protect vital interests of the data subject; or
- made from a public register open to consultation with the general public or anyone who proves a legitimate interest, provided that the conditions laid down by law for the consultation are met in the particular case.

SECURITY AND BREACH PROTOCOL

A data controller must notify the Commissioner of the APDP of any breach to the security safeguards of personal data, without delay.

A data processor must, without delay, notify a data controller of any breach to the security safeguards of personal data held on behalf of the data controller.

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