FACTSHEET: SENEGAL

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

FAST FACTS

Population: 16,603,742
Capital: Dakar
President: Macky Sall
2019 Freedom House Score: 72/100
Data protection law? Enforced

LAW

The right to privacy is part of the Senegalese constitution, but 2008 legal reforms saw the enactment of Law No. 2008-12 on the protection of personal data, as well as other ICT-related laws. The Senegalese example is impressive, as their law entered into force in 2014, the data protection commission known as the *Commission des Données Personnelles* (CDP) was established, and the CDP's website is highly accessible and informative with regular reports about the activities of the CDP and resources for citizens looking to exercise their rights under the law.

Under Law No. 2008-12, an individual has the right to:

- be informed by any data controller if they hold personal data about that individual;
- access and know how personal data concerning them is being processed;
- object, for legitimate reasons, to the processing of personal data concerning them;
- have a data controller correct, supplement, update, lock, or delete personal data concerning him, if the data is inaccurate, incomplete, equivocal or out of date, or if its collection, use, communication, or conservation is prohibited; and
- not be subject to a decision made on the sole basis of an automated processing that would produce adverse legal repercussions for them.

PERSONAL DATA

Personal data is any information relating to a natural person identified, or directly or indirectly identifiable, by reference to an identification number or to one or more elements, specific to their physical, physiological, genetic, psychic, cultural identity, social or economic.

Sensitive data includes all personal data relating to **religious, philosophical, or political opinions or activities, trade union membership, racial identity, sexual life, health, social measures, prosecutions, criminal or administrative sanctions**.

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 processing must abide by the following principles:

- personal data must be collected, recorded, processed, stored, and transmitted fairly, lawfully, and not fraudulently;
- personal data must be collected for specific, explicit, and legitimate purposes and cannot be further processed in any manner incompatible with those purposes;
- personal data must be adequate, relevant, and not excessive in relation to those purposes;
- personal data must be accurate and updated, if necessary;
- personal data must be kept for a period not exceeding the period necessary for the purposes for which they were collected or processed; and
- personal data must be treated confidentially and be adequately protected, in particular where the processing includes data transmissions in a network.

Additionally, the law includes provisions concerning interconnection:

- Interconnection of files is allowed when it involves data controllers running services for the public interest, or when implemented by the state to support the administration of remote services within a framework of e-government.
- Interconnection of databases may only be implemented to achieve statutory objective or legitimate interests of data controllers.

REGISTRATION AND ENFORCEMENT

The CDP is an independent administrative authority which is mandated to ensure that the processing of personal data is implemented in accordance with the provisions of Law No. 2008-12. The body is authorised to:

- receive petitions and complaints relating to personal data processing and follow up with those aggrieved;
- inform the public prosecutor of offences committed under the law;
- appoint one or more of its members or agents its services to carry out checks on any processing and, where appropriate, obtain copies of any document or information material useful to its mission;
- maintain a public directory of personal data processing operations;
- advise individuals and organisations who process personal data or who may do so in the future;
- submit suggestions to the Government for simplifying and improving the legislative and regulatory framework for data processing;
- cooperate with data protection authorities in other countries and participate in international negotiations on personal data protection; and

- submit an annual activity report to the President of the Republic and the President of the National Assembly.

Those wishing to process personal data must submit a declaration to the CDP in advance. Breaches of Law No. 2008-12 will result in a data controller receiving an enforcement notice from the CDP. If the controller fails to comply with the enforcement notice, the CDP can sanction the entity through:

- a temporary withdrawal of the authorisation for a period of three months at the end of which period, if compliance is not satisfied, becomes final; and
- a fine of one million to one hundred million CFA francs.

In case of emergency, when implementing processing of personal data has constituted a violation of rights and freedoms, the CDP, after adversarial procedure, can decide:

- to delay processing for a maximum of three months;
- to lock certain personal data processed for a maximum of three months; or
- to temporarily or permanently prohibit the controller from processing against the provisions of the law.

CROSS-BORDER TRANSFER

Transfer of personal data to another country is allowed only when that country provides sufficient legal protection for privacy, freedoms and fundamental rights of individuals to the processing of personal data.

Transfer of personal data to a country where these protections are not provided for is possible when the data subject has expressly consented to the transfer, or to protect the data subject's life, to safeguard the public interest, in exercise or defence of a legal claim, and in execution of a contract in data subject's interest.

SECURITY AND BREACH PROTOCOL

Data controllers are required to take every precaution with regard to the nature of data to prevent them from being distorted, damaged, or accessed by unauthorised third parties. There are no breach notification requirements stipulated under Senegalese law.

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