DATA PROTECTION LAWS OF THE WORLD

Senegal

DLA PIPER

SENEGAL

Last modified 15 January 2022

LAW

The data protection regime in Senegal is mainly governed by the following laws and regulations:

- Act No 2008-12 of 25 January 2008 Concerning Personal Data Protection ("**the Act**")
- Decree No 2008-721 of 30 June 2008 relating to the the implementation of Act No 2008-12 of 25 January 2008 Concerning Personal Data Protection ("**the implementing Decree**")
- Directive ("*Circulaire*") No. 2757 of June 24, 2014, designating focal points of the CDP within the ministries taken by the Prime Minister's Office regarding the census of files relating to personal data
- Act No. 2008-08 of January 25, 2008, on electronic transactions
- Act no. 2016-29 dated 8 November 2016 amending the criminal code
- Act. No. 10-2021 of 25th June 2021 amending the criminal code.

DEFINITIONS

Definition of Personal Data

"**Personal Data**" means all data relating to an identified or identifiable individual with reference to an identification number or one, or many, characteristics of his physical, physiological, genetic, psychical, cultural, social or economic identity (Article 4 of the Act).

Definition of Sensitive Personal Data

"**Sensitive Personal Data**" means data relating to: religious, philosophical or political opinions or union activities; sex life; race; health; social measures and prosecutions; and criminal and administrative sanctions. (Article 4 of the Act).

NATIONAL DATA PROTECTION AUTHORITY

The National Data Protection Authority is the "*Commission de Données Personnelles*" ("**CDP**").

The CDP is an independent administrative authority responsible for ensuring that the processing of personal data is carried out in accordance with the provisions of this law.

CDP main duties include:

- informing the data holders and the data controllers of their rights and obligations. To this end:
  - it receives the formalities prior to the creation of processing of personal data;
  - it receives complaints, petitions and claims relating to the implementation of the processing of personal data and informs their authors of the follow-up given to them;
  - it informs the public prosecutor without delay of the offences of which it has knowledge;

  - it may, by special decision, entrust one or more of its members or agents of its services with the task of carrying out verifications relating to any processing and, where appropriate, obtaining copies of any document or information medium useful for its mission;
  - it may, under the conditions defined in articles 29 to 32 of this law, impose a sanction on a data controller;
  - it responds to any request for an opinion.
- approving the charters of use that are presented to it;
- keeping a directory of personal data processing at the disposal of the public;
- advising the persons and organizations that have recourse to the processing of personal data or that carry out tests or experiments that may lead to such processing;
- authorizing, under the conditions provided for in the Act, the transborder transfer of personal data;
- presenting to the Government any suggestion that may simplify and improve the legislative and regulatory framework for data processing;
- cooperating with the personal data protection authorities of third countries and to participate in international negotiations on personal data protection;
- publishing the authorizations granted and the opinions issued in the directory of personal data processing;
- drawing up an annual activity report submitted to the President of the Republic and the President of the National Assembly.

REGISTRATION

The is no country-wide system of registration in Senegal. However, the processing of personal data may be subject to prior notification to, or authorization/Prior approval from the CDP.

Notification regime

Businesses must notify the CDP in respect of their processing activities, except in the following cases:

- Non-profit processing for religious, philosophical or political associations, or trade unions (when the data correspond to the purpose of the association or trade union, concern only their members and are not disclosed to third parties).
- Processing for the sole purpose of keeping a register; by law, this is intended exclusively to provide public information and is open to consultation for any person with a legitimate interest.

(Article 18 of the Act)

Authorization/Prior approval regime

Prior approval from the CDP is required for processing of:

- Genetic data;
- Data relating to offences, convictions or security measures;
- Data that involve an interconnection of files;
- Data that include a national identification number;
- Biometric data;
- Data that are of public interest, particularly for historical, statistical or scientific purposes.

Authorisation is however not required in the following cases:

- Data processing for private purposes only;
- Temporary data copies for transmission, network access and automatic storage purposes, provided they are made to improve network user access;
- Data processing by non-profit organisations for religious, philosophic, political or union purposes only;
- Data processing for public register purposes.

Notice/Opinion regime ("Avis")

The automated processing of personal information carried out on behalf of the State, a public institution or a local authority or a legal person under private law managing a public service are decided by regulatory act taken after a reasoned opinion from the CDP. Such processing relates to:

- State security, defense or public safety;
- the prevention, investigation, recording or prosecution of criminal offences or the execution of criminal sentences or security measures;
- the population census;
- personal data that reveal, directly or indirectly, the racial, ethnic or regional origins, parentage, political, philosophical or religious opinions or trade union membership of persons, or that relate to the health or sexual life of persons when they are not covered by provisions related to interconnexion of data;
- the processing of salaries, pensions, taxes, and other settlements.

(Articles 20 and 21 of the Act)

DATA PROTECTION OFFICERS

The appointment of a Data Protection Officers ("**DPO**") is left at the exclusive discretion of the data controllers regarding businesses.

However, the Act provides that department responsible for carrying out the processing and the categories of persons who, by reason of their duties or for the needs of the department, have direct access to the recorded data as well as the function of the person or department with whom the right of access to its processed data is exercised shall be communicated to the CPD. (Article 22 of the Act)

Additionally, the CDP is however available to assist businesses regarding the training of their DPO on Data protection law and regulations.

Regarding ministries, the appointment of data focal points of the CDP ("*Points focaux*") is required in each ministry for the purposes of the census and declaration of files and databases according to Directive No. 2757 of June 24, 2014, designating focal points of the CDP within the ministries regarding the census of files relating to personal data.

COLLECTION & PROCESSING

Data controllers are subject to the following principles and requirements.

The obligations of data controllers include:

- **Transparency**: Data Controllers must inform the Data Subjects about the processing and personal data processed.
- **Security**: Data Controllers are required to ensure the security of personal data. They must prevent the data's alteration and damage, or access by non-authorised third parties.
- **Confidentiality**: The Data Controller must ensure confidentiality and security of the processing.

(Articles 34 and 35 of the Act)

The Data holders/subjects have rights to:

- Access and obtain the following from the Data Controller: Information which they are entitled to know, and which will allow them to contest the processing, confirmation of whether their personal data forms part of the processing, a copy of their personal data (in an accessible form), as well as any available information on the data's origin and information relating to the purposes of the processing and categories of processed data; recipients or categories of recipients to whom the data are disclosed; and transfer of personal data outside the country.
- Request that the Data Controller rectify or delete their personal data if they are inaccurate, incomplete, unclear, or expired, or if the collection, usage, disclosure, or retention of the data is prohibited.
- Object to the processing on legitimate grounds including for marketing purpose unless the processing satisfies a legal obligation.

- Complain to the CDP at any time the processing of their Personal Data does not comply with Data Protection Act.

(Articles 33, 62, 63 and 69 of the Act)

TRANSFER

Transfer of personal data to another country is prohibited unless the receiving country provides sufficient protection for the Data Subject's private life, liberties and fundamental rights.

Countries members of the African Associations of data protection (*'Association Francophone des Autorités de Protection des Données Personnelles'*) are considered to have sufficient protection for the Data Subject's private life, liberties and fundamental rights. Other countries are assessed on case-by-case basis and on criteria including the existence of data protection law and authority responsible of data protection.

A transfer to a country not offering a sufficient level of protection is possible if the transfer is timely and non-massive, if the Data Subject agrees to it or if the transfer is necessary to:

- Protect the life of the Data Subjects/Holders;
- Protect the public interest;
- Comply with obligations allowing the acknowledgment, exercise, or defence of a legal right in court; and
- Perform an agreement between the Data Subject and the Data Processor or take precontractual measures upon the request of the Data Subject.

In any case, prior transferring personal data, the Data controller must inform the CDP. The information must include:

- The name and address of the data sender;
- The name and address of the data recipient;
- The full data file and description;
- The type of personal data transferred;
- The number of persons concerned;
- The data processing purpose;
- The transfer method and frequency;
- The first transfer date.

(Articles 49-51 of the Act)

SECURITY

Data Controllers are required to ensure the security of personal data. They must prevent the data's alteration and damage, or access by non-authorised third parties. In this regard, Data Controllers should make sure that:

- Persons with access to the system can only access the data that they are allowed to access;
- The identity and interest of any third-party recipients of the data can be verified;
- The identity of persons who have access to the system (to view or add data) can be verified;
- Unauthorised persons cannot access the place and equipment used for the data processing;
- Unauthorised persons cannot read, copy, modify, destroy, or move data;
- All data entered onto the system are authorised;
- The data will not be read, copied, amended, or deleted without authorisation during the transport or communication of the data;
- The data are backed up with security copies;
- The data are renewed and converted to preserve them.

(Article 71 of the Act)

BREACH NOTIFICATION

Breach notification is subject to following sanctions:

- Imprisonment for a period of between one and seven years;
- Fines of between XOF 500,000 and 10 million. The judge can choose one of the sanctions listed above or a combination of them.

(Article 431-14 of the Criminal Code).

Where the breach is imputable to a legal person, its criminal liability will be held according to the provisions of the article 25 of Act. No. 10-2021 of 25th June 2021 amending the criminal code.

Mandatory breach notification

No mandatory breach notification protocol is provided under Senegal law.

ENFORCEMENT

The CDP have enforcement powers including:

- Investigative powers: The CDP can conduct three types of investigation:
  - **On-site inspections:** In this case, the CDP may have access to any materials (servers, computers, applications, etc.) and any place (offices, buildings) in which personal data are processed;
  - **Documentary inspections: T**hese inspections allow the CDP to obtain disclosure of documents or files upon written request;
  - **Hearing inspections:** These inspections consist of interrogation in their offices or summoning representatives of Data Controllers to obtain any necessary information.
- Administrative fines for infringements of the Data Protection Act: The CDP has power to impose administrative fines for infringement of the Data Protection Act provisions. The fines should be fine between XOF 1 million and XOF 100 million.
- Non-compliance with a data protection authority: Non-compliance with the CDP can lead to the following sanctions:
  - a warning;
  - an injunction to put an end to defaults within the time limit set by the Commission; or
  - a provisional withdrawal of the authorisation granted for a period of three months at the expiry of which the withdrawal becomes final.

In case of urgency, the CDP can:

- interrupt a processing for a duration that cannot exceed three months;
- lock certain kinds of data for a duration that cannot exceed three months; or
- prohibit, provisionally or definitively, data processing that does not comply with the Act.

(Article 29-31 of the Act)

ELECTRONIC MARKETING

Data Subjects have the right to object, free of charge, to the processing of their Personal Data for direct marketing.

The sending of marketing communications is forbidden on principle unless the recipient agrees to it.

Also, there are two exceptions where prior approval is not required:

- The recipient's information was collected directly from him, in accordance with the provisions of the Act.
- The recipient is already a customer of the company, the marketing messages relate to products or services that are similar to those previously provided, and the recipient is given the possibility of objecting to all messages sent to him.

(Article 16 of the Act No. 2008-08 of January 25, 2008, on electronic transaction and article 47 of the Act)

Sending marketing communications in breach of applicable restrictions are subject to following sanctions:

- seven years' imprisonment;
- or an XOF 1 million fine;
- or both above sanctions.

(Article 431-20 of the Senegalese Criminal Code)

ONLINE PRIVACY

There is no specific restriction on the use of cookies under the Act. However, the CDP requires that the Data Subject is informed of the use of cookies and to collect his consent.

KEY CONTACTS

Geni & Kebe
www.dlapiperafrica.com/senegal

Mouhamed Kebe
Partner
Geni & Kebe
T +221 76 223 63 30
mhkebe@gsklaw.sn

Mahamat Atteib
Associate
Geni & Kebe
T +221 77 737 41 74
m.atteib@gsklaw.sn

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.