DATA PROTECTION LAWS OF THE WORLD

Senegal

SENEGAL

Last modified 23 February 2024

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 on electronic certification in application of law no. 2008-08 of 25 January 2008 on electronic transactions.
- Act No. 2008-08 of January 25, 2008, on electronic transactions; and
- Act no. 2016-29 dated 8 November 2016 amending Law No.65-60 of 21 July 1965 on the Penal Code of Senegal.

As regards international conventions, Senegal is a member of the African Union Convention on Cyber Security and Protection of Personal Data known as the Malabo Convention adopted by the General Assembly of the African Union on 27 June 2014.

The aim is to create a comprehensive legal framework for e-commerce, data protection, cybercrime and cybersecurity on the continent.[1]

1: Christelle HOUETO, "Entry into force of the Malabo Convention on Cybersecurity in Africa: The countries".

DEFINITIONS

Definition of Personal Data

“Personal Data” means all data relating to an identified or identifiable individual by reference to an identification number or one, or many, characteristics of his / her physical, physiological, genetic, psychical cultural, social and economic identity. [1]

Definition of Sensitive Personal Data

“Sensitive Personal Data” means all data relating to religious, philosophical or political opinions or union activities; sex, life, race, health, social measures and prosecutions; and criminal and administrative sanctions.[2]

Definition of Electronic Trading

“Electronic Trading” means the act of offering, purchasing or supplying goods and services via computer systems and telecommunication networks such as the Internet or any other network using electronic, optical or other similar means enabling remote exchanges of information.[3]

Definition of Processing

“Processing [of Personal Data]” means any operation or set of operations which is performed upon data, whether or not by automatic means, such as collection, use, recording, organisation, storage, adaptation, alteration, retrieval, transmission, dissemination or otherwise making available, alignment or combination, blocking, encryption, erasure or destruction of personal data.

1: 2008-12 on the Protection of Personal Data; Article 4 Number 6

2: 2008-12 on the Protection of Personal Data; Article 4 Number 8

3: Article 1er of the African Union Convention on Cyber Security and Protection of Personal Data

NATIONAL DATA PROTECTION AUTHORITY

The authority responsible for data protection is the Senegalese Data Protection Authority established by Law No. 2008-12 of 25 January 2008.[1]

Commission for the Protection of Personal Data of Senegal (CDP) is located at 34 Sicap Mermoz VDN Lot B. 25528 Dakar, Fann.

The CDP is composed of eleven 11 members chosen because of their legal and / or technical competence. They:

- Ensure that the processing of character data is implemented in accordance with the legal provisions;
- Inform the data subjects and controllers of their rights and obligations;
- Regulate the assurance that information and communication technologies (ICTs) do not threaten the freedoms and privacy of Senegalese;
- Advise individuals and organizations who have used personal data processing or who have already undergone tests or experiences of a nature about such treatments;
- Publish the authorizations granted and the declaration issued to the directory of the processing of personal data and draw up an annual report of activities submitted to the President of the Republic and the President of the National Assembly.

The CDP also formulate recommendations by cooperating with the personal data protection authorities of third countries and participate in negotiations on the protection of personal data.[2]

1: 2008-12 on the Protection of Personal Data; Articles 5 and following
2: cdp.sn/missions

REGISTRATION

Businesses must notify the CDP in respect of its processing activities, except in the following case:

- 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.
- The non-profit processing for religious, philosophical, or political associations, or trade unions.[1]

According to Article 22 of the DPA, the declaration must include:

- The identity and address of the Data Controller or his representative;
- Purpose(s) of the processing and the description of its general functions;
- Possible interconnections between databases;
- Personal data processed and categories of persons concerned by the processing;

- Time period for which the data will be kept;
- Department or person(s) in charge of data processing;
- Recipient(s) or categories of recipients of the processed data;
- Persons or departments before which the right of access is exercised;
- Measures taken to ensure the security of the processing; and
- Identity and address of the data processor.

The registration process, following the collection and processing of personal data, must comply with the requirements set by law. Thus, in addition to the prior consent of the author of the information, the registration of data is also subject to the respect of the right to information and the principles of transparency, clarity, confidentiality, compliance with the rules of ethics and ethics governing certain professions.[2]

1: 2008-12 of 25 January 2008 on the Protection of Personal Data, Article 18
2: 2008-12 of 25 January 2008 on the Protection of Personal Data,Article 22

DATA PROTECTION OFFICERS

The law designates a Personal Data Protection Commission (the CDP), whose role it is to ensure that any processing of personal data is in accordance with the law. The commission is also responsible for informing data controllers and data subjects of their rights and obligations, handling complaints, conducting audits, and sanctioning data controllers who are in breach of the law.

COLLECTION & PROCESSING

Processing is any operation performed on personal data. The most common are collection, operation, management, retention or transfer, copying, and to some extent, interconnection.[1]

The controller of personal data is defined as the natural or legal person, public or moral; any other body or association which alone or jointly with others, makes the decision to collect and process personal data and determine the purposes.[2]

The provisions of Article 34 of the aforementioned law requires the person in charge of the procedure to treat personal data lawfully, fairly and not fraudulently. The collection and processing of personal data can not be done freely. The law speaks of a collection for legitimate purposes, for specific explicit purposes.

Personal data must be treated confidentially and be protected, especially if the processing involves data transmissions in a network.[3]

1: 2008-12 of 25 January 2008 on the Protection of Personal Data, Article 4.19
2: 2008-12 of 25 January 2008 on the Protection of Personal Data, Article 4.15
3: 2008-12 of 25 January 2008 on the Protection of Personal Data, Article 38

TRANSFER

Under Senegalese law it is possible to transfer personal data to a third country. When transferring data to a foreign country, the controller is required to submit a duly motivated request to the Personal Data Protection Commission if the transfer lacks an adequate level of protection. This request is possible only when the controller provides a sufficient guarantee of protection of the rights of the data subject regarding compliance with the privacy of the fundamental rights and freedoms of individuals concerned and the exercise of the corresponding rights.

The level of protection in question is assessed in the light of, inter alia, the security measures, the specific processing characteristics such as its purpose, duration, nature, origin and the destination of the processed data.[1]

There are a number of obligations that affect the controller. The data transfer can only be made in a country that offers the same guarantees of protection as Senegal unless the request is accepted.

In derogation of the obligation of the recipient country of the data subject of the transfer, the law provides for the possibility of transferring data to a third country which does not offer the same level of protection, subject to certain conditions.

Indeed, this transfer must be punctual, non-massive and the person to whom the data relates must express his / her consent to a transfer of these data. It must also be expressed if the transfer is necessary to one of the following conditions:

- to safeguard the life of this person;
- the safeguarding of the public interest;
- compliance with obligations to ensure the recognition, exercise or defense of a right to justice;
- to the execution of a contract between the controller and the person concerned, or
- pre-contractual measures taken at the request of the latter.

1: 2008-12 of 25 January 2008 on the protection of personal data, Article 49-51

SECURITY

According to Article 71 of the Protection of Personal Data, all data controllers have an obligation to ensure the security of personal data. The data controller is required to take all necessary precautions with regard to the nature of the data and, in particular, to prevent it from being distorted, damaged, or unauthorized third parties having access to it. Data Controllers must make sure that:

- authorized persons can only access data personal nature within their competence;
- the identity and interests of any third parties recipients of the data can be verified;
- identity of persons having access to the information system can be verified;
- unauthorized persons are prevented from accessing the place and equipment used for data processing;
- unauthorized persons are prevented from reading; coping; modifying, moving and destroying data;
- all data introduced in the system is authorized;
- Data will not be read, copied, modified or erased without authorization during the transport or communication of the data.
- Data is backed up with security copies;
- Data are renewed and converted to preserve them.

BREACH NOTIFICATION

Based on Senegal’s law and regulations there is no legal requirement to report data breaches to the CDP. Nevertheless, the data controller is required to respect confidentiality, security and data retention requirements of the data subject.

There is also no legal requirement for data breaches to be reported to affected individuals.

Mandatory breach notification

No mandatory breach notification protocol is provided under Senegal law.

ENFORCEMENT

The Commission for the Protection of Personal Data has the power to investigate, warn, and sanction. There are three forms of investigations that can be carried out:

- onsite inspections;
- documentary inspections;

- hearing inspections.

The CDP can also send a warning to a controller that does not comply with legal regulations. Six major corporations in 2014 /2015 received warnings and notices from the CDP.

In regards to sanctions, The CDP has the power to carry out civil / administrative sanctions and criminal sanctions. When there is a breach the CDP can carry out a civil or administrative sanction by:

- a provisional withdrawal for three months of the given authorisations; the withdrawal becomes definitive at the end of the three month period if the breach remains.
- fines of between 1 million XOF and 100 Million XOF.
- in urgent cases, the CDP can also interrupt the processing of data for a duration that can not exceed three months.
- lock certain kinds of data for a duration not exceeding three months.
- prohibit processing that does not comply with the regulation.

The CDP can also carry out a criminal sanction consisting of imprisonment between six and seven years; in addition to demanding a fine between 200000 XOF and 10 Million XOF.[1]

1: 2008-12 of 25 January 2008 on the Protection of Personal Data, Articles 29-32

ELECTRONIC MARKETING

According to Article 47, in Senegal it is prohibited for anyone to carry out direct marketing using any means of communication in any form whatsoever, of the data for a staff of a natural person who has not expressed his consent prior to receiving such surveys.[1] It is important to note that Article 47 does not differentiate between the means of marketing but prohibits all direct marketing that lacks prior consent.

Article 16 of the Senegalese Electronic Transactions Law[2] provides more specific regulations on the marketing of data. The following are prohibited:

- direct marketing by sending a message by means of an automated calling machine, a fax machine or an e-mail using, under whatever form the contact details of a natural person who has not expressed its prior consent to receive direct surveys.
- The exception to this, is if the recipient’s details have been collected directly from in accordance with the provisions of the Law on the Protection of Personal data or on the occasion of a sale or supply of services, the direct marketing concerns similar products or services provided by the same natural or legal person, and if the consignee is offered, expressly and unambiguously, the possibility to oppose, without cost, except those related to the transmission of the refusal and in a simple way, to the use of its coordinates when they are collected and whenever an email from propsection is specifically addressed to said person.
- However, in any case, it is prohibited to issue, for direct marketing purposes, messages via automatic calling machines, faxes and emails, without indicating valid details to which the addressee could usefully forward a request to cease the use of their information for marketing.

1: 2008-12 of 25 January 2008 on the Protection of Personal Data, Articles 47
2: Senegalese Electronic Law

ONLINE PRIVACY

The law on Personal Data and the Senegalese Electronic Transactions Law does not contain provisions on online privacy or cookies.

KEY CONTACTS

Geni & Kebe
www.dlapiperafrica.com/senegal

Mouhamed Kebe
Managing 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.