Data Protection Laws of Senegal(Africa)

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supplement, update, lock, or delete personal data concerning him, if the data is inaccurate, incomplete, equivocal or out of date, or if its collection, use, communication, or conservation is prohibited; and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.

Complaint Portal

- Remember to include as much information as possible in your complaint, including:
    - the name of the party that processed the data;
    - their contact details, if known;
    - a brief description of the violation; and
    - the specific remedy that you are requesting.
- E-mail your complaint to the CDP: contactcdp@cdp.sn

Senegalese national data protection legislation is behind the international curve. The law is silent on many issues, such as:

- data protection for people under 18 years old;
- the notification of breaches to the Senegalese Data Protection Authority;
- cookie requirements; and
- data transfer agreements.

These failings explain why the European Union does not consider Senegal to be a safe jurisdiction in terms of data protection. However, it has never been blacklisted.

Are any changes to existing data protection legislation proposed or expected in the near future?

No.

Legal framework
Legislation
What legislation governs the collection, storage and use of personal data?

The Senegalese laws on data protection are:

- the Data Protection Act (Law 2008-12, January 25 2008);
- the Decree on the Application of the Data Protection Act (2008-721, June 30 2008); and
- the Cybercrime Law (Law 2008-10, January 25 2008).

The Data Protection Act and its decree set out:

- the conditions for data processing;
- the rights of individuals; and
- the obligations of data owners.

The Data Protection Act also establishes the Senegalese Data Protection Authority (CDP).

The Cybercrime Law outlines the criminal offences relating to data processing and the applicable penalties.

Scope and jurisdiction
Who falls within the scope of the legislation?

The following parties fall within the scope of the legislation:

- 'Data owner' – a data owner can be an individual, the Senegalese state, a local community or a public or private corporation.
- 'Data processor' – a data processor is a subcontractor acting under the authority and instruction of the data owner.

What kind of data falls within the scope of the legislation?

All data relating to an identified or identifiable individual with reference to an identification number or one or many characteristics of his or her physical, physiological, genetic, psychical, cultural, social or economic identity falls within the scope of the legislation.

Are data owners required to register with the relevant authority before processing data?

Yes. The data owner must either notify the CDP or obtain authorisation from the CDP before processing data.

Is information regarding registered data owners publicly available?

Yes.

Is there a requirement to appoint a data protection officer?

There is no obligation to appoint a data protection officer. However, Article 22 of the Data Protection Act states that the position of the person or the department which exercises the data access right must be communicated to the CDP.

Enforcement

Which body is responsible for enforcing data protection legislation and what are its powers?

The CDP is responsible for enforcing data protection legislation.

The CDP's enforcement powers are set out in Article 16 of the Data Protection Act. The CDP:

- receives complaints relating to data processing;
- informs the prosecutor of any breaches;
- conducts on-site inspections to gather information for the prosecutor. If the landlord of the premises to be inspected objects, the inspection must be authorised by the president of the competent high court;
- requests the communication of documents; and
- imposes injunctions and fines for non-compliance with the Data Protection Act.

Collection and storage of data
Collection and management
In what circumstances can personal data be collected, stored and processed?

- Personal data can be collected, stored and processed provided that:
- data is collected and processed fairly and lawfully;
- data is collected for specified, explicit and legitimate purposes and subsequently processed in a manner that is compatible with such purposes;
- data is adequate, relevant and not excessive in relation to the purposes for which it was collected;
- collected data is accurate, complete and kept up to date; and
- collected data is retained in a form that allows the identification of individuals for a period that is no longer than necessary for the purposes for which it was collected.

Are there any limitations or restrictions on the period for which an organisation may (or must) retain records?

No.

Do individuals have a right to access personal information about them that is held by an organisation?

Yes.

Do individuals have a right to request deletion of their data?

Yes.

Consent obligations
Is consent required before processing personal data?

Yes.

If consent is not provided, are there other circumstances in which data processing is permitted?

Yes. Pursuant to Article 33 of the Data Protection Act, processing is permitted without consent:

- in order to comply with any legal obligation to which the data owner is subject;
- in order to perform a public service undertaking that has been entrusted to the data owner or the data recipient;
- if the processing relates to the performance of a contract to which the individual is a party or of pre-contractual measures requested by him or her; or
- if processing the data is subject to the interests and fundamental rights and liberties of the individual.

What information must be provided to individuals when personal data is collected?

The following information must be provided to individuals when personal data is collected:

- the identity of the data owner and its representative (if any);
- the purpose of the processing;
- the category of data concerned;
- whether replies to questions are mandatory or optional, as well as the possible consequences of failure to reply to a mandatory question;
- the recipients or categories of recipient of the data;
- the right to object, for a legitimate purpose, to the collection of such data;
- the right to access the collected data and, if necessary, to have it rectified;
- the duration of the processing; and
- details of any intended transfer of the data.

Data security and breach notification
Security obligations
Are there specific security obligations that must be complied with?

Yes. The data owner must prevent the amendment of or damage to the data, as well as access by non-authorised third parties. In addition, the data owner must ensure that:

- persons with access to the system can access only the data relevant to them;
- the identity and interest of any third-party recipients of the data can be verified;
- the identity of persons accessing to the system (to view the data or add data) can be verified;
- non-authorised persons cannot access the place and equipment used for data processing;
- non-authorised persons cannot read, copy, modify, destroy or move data;
- all data introduced in the system is authorised;
- the data will not be read, copied, modified or deleted without authorisation during the transport or communication of the data;
- the data is backed up with security copies; and
- the data is renewed and converted to preserve it.

Breach notification

Are data owners/processors required to notify individuals in the event of a breach?

There is no general obligation to notify personal data security breaches to individuals.

Are data owners/processors required to notify the regulator in the event of a breach?

There is no general obligation to notify personal data security breaches to the Senegalese Data Protection Authority (CDP).

Electronic marketing and internet use
Electronic marketing

Are there rules specifically governing unsolicited electronic marketing (spam)?

Yes. The recipient must have agreed to receive unsolicited electronic marketing. However, prior approval is not required if one of the following two exceptions applies:

The information was collected directly from the recipient in accordance with the CDP's rules.

The recipient is already a customer of the company, the marketing messages relate to products or services that are similar to those that have previously been sent and the recipient has the option to object to the messages that are sent.

Cookies

Are there rules governing the use of cookies?

There is no provision governing the use of cookies.

Data transfer and third parties

Cross-border data transfer
What rules govern the transfer of data outside your jurisdiction?

A data owner cannot transfer data to another country unless the receiving country provides sufficient protection in relation to an individual's private life, liberties and fundamental rights (Article 9 of the Data Protection Act). The Senegalese Data Protection Authority (CDP) must be informed before any transfer, and authorisation must be sought.

The CDP can allow a transfer to a country that does not provide sufficient protection if the transfer:

- has the individual's consent;
- is timely and does not involve large amounts of data; and
- is necessary to:
- protect the individual's life;
- protect the public interest;
- comply with any obligations to allow the acknowledgment, exercise or defence of a legal right in court; or
- perform an agreement between the data owner and the individual or pre-contractual measures taken on its request.

In addition, the CDP can allow the transfer of data to a country that lacks sufficient protection if the data owner can provide sufficient protection to individuals and the exercise of relating rights.

Are there restrictions on the geographic transfer of data?

No.

Third parties

Do any specific requirements apply to data owners where personal data is transferred to a third party for processing?

Yes. Under Article 39 of the Data Protection Act the data owner must offer adequate guarantees to ensure the implementation of security measures. The data owner must conclude a written contractual agreement with the third party, which must:

- specify the third party's obligation regarding security protection;
- provide that the third party can act only on the data owner's instructions; and
- provide that the third party is bound by the security requirements set out in Article 71 of the Data Protection Act.

Penalties and compensation

Penalties
What are the potential penalties for non-compliance with data protection provisions?

There are two kinds of penalty for non-compliance with data protection provisions: those set down by the Senegalese Data Protection Authority (CDP) and those ordered by the court.

CDP penalties
The CDP can order:

- the provisional withdrawal of authorisation for three months – this withdrawal becomes permanent at the end of the three-month period if the data controller still does not comply with data protection laws; and
- a fine of between CFAfr1 million and CFAfr100 million.

In urgent cases the CDP can also:

- interrupt data processing for up to three months;
- freeze certain kinds of data for up to three months; and
- prohibit – temporarily or permanently – any processing that does not comply with CDP rules.

Court penalties
The court can impose one of more of the following penalties:

- imprisonment of between six months and seven years; and
- fines of between CFAfr200,000 and CFAfr10 million.

Compensation

Are individuals entitled to compensation for loss suffered as a result of a data breach or non-compliance with data protection provisions by the data owner?

Yes, individuals can request compensation in court. The court has sole discretion as to the amount of compensation.

Cybersecurity

Cybersecurity legislation, regulation and enforcement
Has legislation been introduced in your jurisdiction that specifically covers cybercrime and/or cybersecurity?

Senegal has not yet adopted a cybersecurity act, but in 2014 the government created the Cybersecurity National Centre and the ratification of the African Union Convention on Cybersecurity and Data Protection.

It also adopted the Cybercrime Law (2008-10), which completes the Penal Code and the Penal Procedures Code.

What are the other significant regulatory considerations regarding cybersecurity in your jurisdiction (including any international standards that have been adopted)?

There is no regulatory considerations regarding cybersecurity in Senegal.

Which cyber activities are criminalised in your jurisdiction?

Cyber activities that are criminalised in Senegal include:

- the unauthorised interception of communications;
- the unauthorised access to computer systems;
- the wilful destruction of computer data;
- the distribution or publication of an intimate image without consent; and
- the distribution or publication of child pornography.

Which authorities are responsible for enforcing cybersecurity rules?

No authority is responsible for enforcing cybersecurity rules.

Cybersecurity best practice and reporting
Can companies obtain insurance for cybersecurity breaches and is it common to do so?

So far, no insurer offers insurance for cybersecurity breaches.

Are companies required to keep records of cybercrime threats, attacks and breaches?

No.

Are companies required to report cybercrime threats, attacks and breaches to the relevant authorities?

No.

Are companies required to report cybercrime threats, attacks and breaches publicly?

No.

Criminal sanctions and penalties

What are the potential criminal sanctions for cybercrime?

The penalties are:

- imprisonment of between six months and 10 years;
- a fine of between CFAfr100,000 and CFAfr15 million; or
- both.

What penalties may be imposed for failure to comply with cybersecurity regulations?

There is no penalty for failure to comply with cybersecurity regulations.