DATA PROTECTION LAWS OF THE WORLD

Gabon

GABON

Last modified 10 January 2022

LAW

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

- Law No. 001/2011 on the Protection of Personal Data "the Law";
- Law No. 26/2018 of 22 October 2018 regarding Electronic Communications in Gabon;
- Law No. 02/2004 of 30 March 2005 ratifying the International Convention for the Suppression of the Financing of Terrorism;
- Regulation No. 01/03 -CEMAC-UMAC relating to the Prevention and Suppression of Money Laundering and Financing of Terrorism in Central Africa;
- Order n°00000014/PR/2018 of February 23, 2018 on the regulation of electronic transactions in the Gabonese Republic; and
- Order No. 15-PR-2018 on the Regulation of Cybersecurity and the Fight against Cybercrime.

DEFINITIONS

Definition of Personal Data

Any information relating to an identified or identifiable natural person, directly or indirectly, by reference to an identification number or to one or more elements, specific to his physical, physiological, genetic, psychological, cultural, social or economic identity (Article 6 of the Law).

Definition of Sensitive Personal Data

All personal data relating to religious, philosophical, political or trade union opinions or activities, sex life, health, social race, health, social measures, prosecution, criminal or administrative sanctions (Article 6 of the Law).

NATIONAL DATA PROTECTION AUTHORITY

The Gabonese National Authority for Data Protection is the CNPDCP *(La Commission nationale pour la protection des données à caractère personnel).* Its main duties are to ensure that any processing of personal data is carried out in accordance with the provisions of the Data Protection Law and to inform all data subjects, data controllers, and others involved of their rights and obligations.

The CNPDCP deals with:

- receiving the notifications of data controllers regarding processing operations;
- authorising processing operations that involve a high risk to rights and liberties of individuals;
- establishing and publishing standards for personal data processing and enacting model regulations for security (in this

context, CNPDCP has issued guidelines on the processing of personal data in the context of CCTV systems);
- receiving complaints, petitions, and claims relating to the processing of personal data of an individual;
- advising public authorities, and where appropriate individuals and organisations on how to implement data processing operations;
- informing, without delay, the Public Prosecutor on offences committed;
- carrying out inspections, audits, and obtaining all information and documents considered necessary;
- answering requests for accessing processing operations;
- giving opinions, if requested, on the level of compliance of organisations as well as designing compliance products and rules;
- awarding compliance labels regarding personal data processing complying with the Data Protection Law;
- proposing to the Government of Gabon legislative or regulatory measures with regard to the evolution and adaptation of new technologies and the processing of personal data;
- representing Gabon in the international community on data protection related matters;
- preparing and denying, at the request of the Prime Minister, the Gabonese position on data protection related matters in view of international negotiations;
- imposing sanctions and penalties and delivering enforcement notices to data controllers in the case of non-conformity with the Data Protection Law; and
- submitting an annual activity report to the President of the Gabon National Assembly

REGISTRATION

The is no country-wide system of registration in Gabon. However, The processing of personal data may be subject to prior notification to, or authorisation from CNPDCP.

The requirement of prior authorisation is applicable in the following circumstances:

- automatic or non-automatic processing of data regarding criminal convictions and infractions, except for processing carried out by Justice officials in the context of their obligations to ensure the security of possibly affected persons;
- automatic processing of genetic data (except when carried out by healthcare professionals for the purpose of preventive medicine, medical diagnosis or the provision of medical care and treatment);
- automatic processing which, considering the nature of the data or of the underlying purpose of processing, may result in excluding an individual from rights, benefits, contributions, or contract(s), without a legal or regulatory basis;
- automatic processing aimed at interconnection by one or more entities in the context of public service aimed at different public interests, or interconnection between different entities, for different purposes;
- processing which concerns a person's registration number in a national identification database;
- automatic processing of data containing comments, observations, and analysis of social difficulties experienced by individuals; and
- automatic processing of biometric data required for controlling the identity of individuals.

The CNPDCP shall take a decision within two months from receiving the request for authorisation. This time limit may be renewed once by a decision from the President of the CNPDCP. Where the CNPDCP has not taken a decision within these time limits, the application for authorisation shall be deemed to be rejected.

Specific activities for data processing are subject to ministerial approval. These include data processing carried out on behalf of the State and aimed at State security, defence or public safety, or which is carried out for the purpose of preventing, investigating, detecting, pursuing, or executing criminal infractions is approved by the competent Government ministry(ies), subject to a prior opinion by the CNPDCP. Other matters are also approved by legislative measures, such as publicly relevant processing aimed at public census.

Other data processing operations are subject to a mere prior notification to the CNPDCP, except if a complete exemption from notification or authorisation applies.

Specifically, the following activities are exempt from formalities:

- processing operations aimed solely at forming a register which is legally intended exclusively for public information and is

open to public consultation by any person with legitimate interest;
- processing operations by any organisation, not-for-profit organisation, or any religious, political, philosophical, or trade union organisation or association - this exemption only applies if;
    - the processing operations corresponds to the formal and official purpose of said organisation/association;
    - the processing relates only to its members, and, where applicable, to people who have regular contact with the organisation/association in the context of its activity; and
    - the data is not disclosed to third parties, unless the data subject has given its/her consent;
- processing operations for which the data controller has appointed a data protection officer ('DPO'), unless personal data is being transferred across borders

In addition, the CNPDCP may identify specific data processing operations which, due to their simplicity and low-risk level, may be subject only to a simplified notification process. This simplified process includes:

- the purposes of the processing operations;
- personal data or categories of personal data processed;
- the category or categories of persons concerned;
- the addressees or categories of addressees to whom personal data are communicated;
- the data retention periods.

DATA PROTECTION OFFICERS

No, the appointment of a DPO is left at the exclusive discretion of the data controller. In any event, we call attention to the concept of DPO in the context of the Gabon law. Indeed, the position of DPO in the Data Protection Law is not entirely aligned with the terms in which this position is defined and approached in the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). Please note that the Data Protection Law precedes the GDPR and has not since been amended. Rather, the concept is interpreted, in practice, as a position whereby a person assumes responsibilities on data protection within the company, and as a potential point of contact with the CNPDCP.

Notwithstanding the above, this position must be a person with the required qualifications to carry out its role, namely professional qualities, in particular relating to knowledge of law and data protection related matters. If this position exists within the data controller's organisation, this must be made known to the CNPDCP.

COLLECTION & PROCESSING

The data processor must present sufficient guarantees to ensure the security and confidentiality of personal data. This requirement does not relieve the data controller of its obligation to ensure compliance with the measure concerning security and confidentiality displayed in Chapter V of the Data Protection Law.

The obligations of data controllers include:

- **Transparency**: The data controller must inform the data subject of the terms of processing when the data is not collected from the data subject. In addition, the data controller must inform the data subject at least before the first communication and must also guarantee a lawful basis to carry out the processing operation
- **Confidentiality**: The data controller must assure that the processing of personal data is only carried out under his authority and instructions. In addition, the data controller must guarantee that only individuals who have technical and legal knowledge regarding the integrity of data, and in this sense the data controller must ensure that the individuals dealing with personal data has signed a non-disclosure agreement
- **Security**: The data controller is required to take any appropriate precautionary measures in regard to the nature of personal data, and, in particular, the data controller shall prevent personal data from being distorted, damaged, or unauthorised access by third parties. In particular, the data controller must:
    - create different levels of access permissions, on a need-to-know basis depending on the position of its employees, thus avoiding unauthorised actions;
    - use encryption or pseudonymisation;
    - keep a record of who accesses the personal data, when and why, ensuring traceability of its use;

  - maintain backups in secondary sources to prevent accidental changes or loss of data; and
  - ensure the identity of the person who wants to access the data or the identity of the parties to whom the data will be disclosed.
- **Retention**: The data controller must guarantee that the data is kept for no longer than the purpose for which was collected.

The Data Protection Law expressly provides for limited data controller rights, and in practice provides data controllers with the right to:

- process personal data in the conditions provided for by law;
- refuse compliance with unreasonable requests and demands from data subjects; and
- appeal any sanctioning decisions by the CNPDCP before the State Counsel.

By contrast, the data subject are entitled to the following rights:

- obtain all of their personal data in an understandable form, as well as any available information as to the origin;
- oppose, for legitimate reasons, the processing of personal data concerning them;
- oppose the processing of their personal data for prospecting purposes;
- rectify, complete, update, lock, or delete personal data concerning them, where it is inaccurate, incomplete, equivocal, out of date, or if collection, use, communication or conservation is prohibited; and
- not be subject to decisions made on the sole basis of an automated processing that would produce significant or detrimental legal repercussions for them.

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 (Articles 89 and sq. of the Law).

TRANSFER

Data transfers to another country are prohibited unless the other country ensures an adequate level of privacy protection and protection of fundamental rights and freedoms of individuals with regard to the processing operation.

The list of countries that comply with this adequate level of protection shall be published by CNPDCP. As far as we are aware, this list has not yet been published. However, the Data Protection Law does identify the criteria which must be considered by the CNPDCP in order to determine adequacy:

- the legal provisions existing in the country in question;
- the security measures enforced;
- the specific circumstances of the processing (such as the purpose and duration thereof); and
- the nature, origin, and destination of the data.

As an alternative to the 'adequacy' criteria, data controllers may transfer data if:

- the data subject has consented expressly to its transfer;
- the transfer is necessary to save that person's life;
- the transfer is necessary to safeguard a public interest;
- the transfer is necessary to ensure the right of defence in a court of law; or
- the transfer is necessary for the performance of a contract between the data subject and the data controller, at the request of the data subject, or for the performance of a contract between the data controller and a third party in the interest of the data subject.

Please kindly note that, except in very specific circumstances, the international transfer of non-encrypted personal data for the purpose of investigation in the health sector is not possible, given the sensitivity of the data at stake.

In relation to outsourcing, the Data Protection Law does not provide for specific provisions, except:

- the obligations applicable to the relationship with data processors;
- when data processors are located outside the country, the provisions applicable to international data transfers; and
- general security obligations, which vary depending on the nature of the data at stake (Article 94 and sq. of the Law).

No references are included to specific concerns regarding, for example, outsourcing to the cloud or to data centres.

SECURITY

Article 66 of the Law states that in order to guarantee 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 accessed by unauthorized third parties. In particular, he/she shall take all measures to:

- guarantee that, for the use of an automated data processing system, authorized persons can only access personal data within their competence;
- guarantee that the identity of third parties to whom personal data may be transmitted can be verified and established;
- guarantee that the identity of persons who have had access to the information system and which data have been read or introduced into the system, at what time and by which person, can be verified and established posteriori;
- prevent any unauthorized person from accessing the premises and equipment used for data processing;
- prevent data carriers from being read, copied, modified, destroyed or moved by an unauthorized person;
- prevent the unauthorized entry of any data into the information system and the unauthorized access, modification or deletion of stored data;
- prevent the use of data processing systems by unauthorized persons using data transmission facilities;
- prevent unauthorized reading, copying, modification or deletion of data during data communication and transport of data carriers;
- back up data by making back-up copies;
- refresh and, if necessary, convert the data for permanent storage.

No specific requirements other than those set forth in the Law.

BREACH NOTIFICATION

No, there is no general data breach notification requirement. However, this is without prejudice to specific CNPDCP rights to monitor and control compliance and, in this context, demand information, documentation and other materials in the context of its supervisory powers.

Mandatory breach notification

No mandatory breach notification protocol is stipulated under Gabonese law.

ENFORCEMENT

As of 22 December 2021, we have not identified any notable enforcement decision issued by the CNPDCP pertaining to the Law.

ELECTRONIC MARKETING

The personal data Act will apply to most electronic marketing activities, as these will involve some use of personal data (eg, an email address which includes the recipient's name).

The general rule for electronic marketing is that it requires the express consent of the recipient (see Article 37 of Order n°00000014/PR/2018 of February 23, 2018 on the regulation of electronic transactions in the Gabonese Republic).

Even when a marketer has the consent of a data subject, that consent can be withdrawn by the data subject under Article 14 of the Personal Data Act.

The data subject has the right to object at any time to the use of his/her personal data for such marketing under Article 13 of the Personal Data Act.

This right to object must be explicitly brought to the attention of the data controller.

However, the data controller may not respond favorably to a request to exercise the right to object if it demonstrates the existence of legitimate reasons justifying the processing, which override the interests, fundamental rights and freedoms of the data subject.

ONLINE PRIVACY

The Law does not provide any specific rules for governing cookies and location data.

However, pursuant to Article 66 and sq. of the Law, data controller must implement all appropriate technical and organizational measures to preserve the security and confidentiality of the data, including protecting the data against accidental or unlawful destruction, accidental loss, alteration, distribution or access by unauthorized persons.

KEY CONTACTS

Geni & Kebe
www.dlapiperafrica.com/senegal

Dr. Sangare Mouhamoud
Associate
Geni & Kebe
T +2250779107541
m.sangare@gsklaw.sn

Dr. Francky Lukanda
Senior Associate
Geni & Kebe
T +2250584344660
f.lukanda@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.