DATA PROTECTION LAWS OF THE WORLD

Gabon

DLA PIPER

GABON

Last modified 8 January 2024

LAW

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

- Act no. 025/2023 of 09/07/2023 amending Act no. 001/2011 of 25 September 2011 on the protection of personal data;
- 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/CEMAC/UMAC/CM of 11 April 2016 on the prevention and suppression of money laundering, terrorist financing and proliferation in Central Africa;
- Law No. 025/2021 of 28/12/2021 regulating electronic transactions in the Gabonese Republic; and
- Law No. 027/2023 of 11/07/2023 regulating cybersecurity and the fight against cybercrime in the Gabonese Republic.

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 Authority for the Protection of Personal Data and Privacy (known by its French acronym APDPVP).

According to article 8 of the 2023 law on personal data, the main tasks of the APDPVP are to inform the persons concerned and the data controllers of their rights and obligations in terms of personal data. It is also responsible for monitoring the implementation of personal data processing and the protection of privacy.

The APDPVP's remit includes in particular:

- Authorising the processing operations specified in article 80, giving an opinion on those mentioned in articles 81 and 82, and receiving declarations concerning other processing operations.
- Drawing up and publishing standards and issuing model regulations to guarantee the security of systems.

- To receive claims, petitions and complaints relating to the implementation of personal data processing, informing the authors of the action taken.
- Responding to requests for advice from public authorities and the courts, while advising individuals and organisations involved in automated data processing _ personal data.
- To inform the Public Prosecutor of offences found to have been committed and to submit observations relating to criminal law.
- Sessions of chargeur members or agents to carry out checks on personal data processing and, if necessary, obtain copies of relevant documents.
- Pronounce measures and sanctions against a controller in accordance with Articles 199 to 204.
- Respond to requests for access from data subjects to the processing of their personal data.
- To issue opinions on the compliance of draft professional rules, products and procedures for the protection of personal data with the law in force.
- Issue opinions on the guarantees offered by professional rules previously recognised as complying with the law, taking into account the fundamental rights of individuals.
- To issue labels to products or procedures that comply with the law after evaluation.
- Issue opinions on draft laws or decrees relating to the protection of individuals with regard to automated processing.
- Propose legislative or regulatory measures to adapt the protection of freedoms to developments in computer processes and techniques.
- To provide assistance in matters of personal data protection at the request of other bodies and administrations.
- To participate, at the request of the Government, in the preparation and definition of the Gabonese position in international negotiations relating to the protection of personal data and privacy.
- Being part of the Gabonese delegation to the work of the competent Community and international organisations in the field of the protection of personal data and privacy, at the request of the Government.

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 APDPVP.

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 APDPVP 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 APDPVP. Where theAPDPVP 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 APDPVP. 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,APDPVP except if a complete exemption from notification or authorisation applies. Specifically, the following activities are exempt from formalities in accordance with article 89 of the aforementioned law:

- 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 APDPVP 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; and
- the data retention periods.

DATA PROTECTION OFFICERS

Under the new law on personal data, the appointment of a Data Protection Officer (**DPO**) is no longer left exclusively to the discretion of the data controller. The law establishes the conditions under which a DPO must be appointed and limits the discretionary power of the data controller. These conditions include:

- Where the processing is carried out by a public authority or public body, with the exception of courts acting in the exercise of their judicial function;
- Where the basic activities of the controller or processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic large-scale monitoring of the data subjects;
- Where the basic activities of the controller or processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic large-scale monitoring of the data subjects;
- Where the basic activities of the controller or processor consist of large-scale processing of sensitive data and data relating to convictions for criminal offences.

In addition, a DPO position must be held by a person with the qualifications required to carry out his or her duties, namely professional qualities, particularly relating to knowledge of the law and matters relating to data protection.

The DPO is responsible for ensuring that data processing is compliant. His / her duties cover all processing carried out by the body that appointed him. In this capacity, he / she is responsible for:

- informing and advising the data controller or data processor, as well as the people in the organisation who process the data, of their obligations under this law;
- monitoring compliance with this law and with the internal rules put in place by the data controller or data processor with regard to data protection, including the allocation of responsibilities and the awareness and training of staff involved in data processing and auditing operations;
- giving an opinion on data protection impact assessments and checking that they have been carried out;

to cooperate with the APDPVP, including in the event of prior consultation by the controller when a data protection impact assessment is carried out, and to consult, as appropriate, on any other matter.

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 Articles 113 *et seq*. of the Personal Data Act 2023.

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 APDPVP before the State Counsel.

By contrast, the data subject are entitled to the following rights provided for in Articles 52 and 53 of the aforementioned Personal Data Act 2023:

- 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 (Article 169 of the Personal Data Act 2023).

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 APDPVP (article 171 in fine of the law on personal data). As far as we are aware, this list has not yet been published. However, the Data Protection Law of 2023 in its article 171 does identify the criteria which must be considered by the APDPVP 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, Article 76 of the aforementioned law allows those data controllers to 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 of 2023 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 (Articles 168 *et seq.* of the aforementioned law).

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

SECURITY

Articles 113 et seq. of the 2023 Personal Data Act state 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

There is a legal requirement to notify data breaches to APDPVP. For more details please refer to "Mandatory Breach Notification" below.

Mandatory breach notification

Under article 142 of the Data Protection Act, in the event of a data breach, the data controller is required to notify the Personal Data Protection and Privacy Authority (APDPVP) without delay. This notification must include the nature of the breach, the categories and approximate number of persons concerned, the measures taken or envisaged to remedy the breach, and the contact details of the Data Protection Officer or another contact point for further information.

In addition, if the breach is likely to result in a high risk to the rights and freedoms of the data subjects, the data controller must inform the data subject individually as soon as possible, as specified in article 145 of the aforementioned law. This communication must be made in clear and simple terms, describing the nature of the breach and providing the information and measures necessary to remedy the situation, in accordance with article 146 of the aforementioned law.

However, there are specific cases where communication to the data subject is not necessary, as provided for in Article 147 of the aforementioned Data Protection Act. These cases include, in particular, where the data controller has taken measures to protect the data affected by the breach, has taken preventive measures against any high risk to the rights and freedoms of the data subjects, or finds that communication would require disproportionate efforts. In such cases, the controller must make a public announcement or take a similar measure enabling the data subjects to be informed in an equally effective manner.

ENFORCEMENT

The law empowers the APDPVP to impose various sanctions depending on the severity of the infringement. However, the level of enforcement remains quite low due to resource limitations and the fact that this field of law is still new to the administration and business and data subjects.

In fulfilment of their duties, members of the APDPVP and sworn and authorized officials have access to places, premises, enclosures, installations or establishments used for the processing of personal data and which are for professional use, with the exception of those parts of the premises used for private purposes.

They are accompanied by Officers of the Judicial Police during inspection missions. The Public Prosecutor responsible for the area is informed in advance.

If the person in charge of the premises objects, the visit may only take place with the authorization of the President of the court in whose jurisdiction the premises to be visited are located or the judge delegated by him.

The Authority shall assess and impose the following measures or penalties, without graduation, depending on the breach of this law found:

- a warning to the data controller who fails to comply with the obligations arising from this law;
- a formal notice to cease the breaches observed within a period set by the Authority;
- a financial penalty.

The APDPVP may impose the following sanctions:

- temporary suspension from collecting and processing personal data for a period of three months, at the end of which the suspension becomes definitive;
- a fine of between one million and one hundred million CFA francs.

The amount of the fine shall be proportionate to the seriousness of the breaches committed and the benefits derived from the breach.

For the first breach, it may not exceed XOF ninety-eight million four hundred thousand. In the event of a repeat offence, it may not exceed XOF three hundred million or, in the case of a company, 5% of turnover excluding tax for the last financial year for which the accounts have been closed, subject to a limit of XOF one hundred and ninety-six million.

Where the APDPVP has imposed a financial penalty that has become final before the criminal court has given a final ruling on the same or related facts, the criminal court may order that the financial penalty be deducted from the fine it imposes.

Penalties are recovered in accordance with the legislation relating to the recovery of State tax debts.

Additional administrative penalties may also apply.

Moreover, criminal offences resulting from violation of the provisions of this law are punishable in accordance with the provisions of the Criminal Code.

Obstructing the work of the APDPVP is punishable by a prison sentence of between six months and one year and a fine of between XOF one million and XOF ten million, either by:

- opposing the performance of the tasks entrusted to its members or authorised agents;
- refusing to provide its members or authorised agents with information and documents useful for their work, or by concealing said documents or information, or by making them disappear;
- communicating information that does not correspond to the content of the recordings as it was at the time the request was made or that does not present this content in a directly accessible form.

In the event of a repeat offence, the penalties provided for in the law shall be doubled.

ELECTRONIC MARKETING

The personal data Act will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. 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 Law No. 025 /2021 of 28/12/2021 regulating 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 Article73of 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 60 of the Personal Data Act.

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

However, in accordance with article 60 of the aforementioned law, 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 113 and sq. of the data law mentioned above, 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.