TABLE OF CONTENTS

August 2020

1. THE LAW

1.1. Key Acts, Regulations, Directives, Bills

In 25 September 2011, Gabon adopted Law No. 001/2011 on the Protection of Personal Data (only available in French here) ('the Data Protection Law').

The Data Protection Law was enacted pursuant to the provision of Articles 1 and 47 of Constitution of the Republic of Gabon 1991 (only available in French here) ('the Constitution') and determines the rules on the processing of personal data. The objective of the Data Protection Law is to set up a system to fight invasions of privacy that may be generated by the collection, processing, use or disposal, transmission, and storage of personal data. The current version of the Data Protection Law includes the modifications arising from Order 2-PR-2020 of 30 of January 2020.

Apart from the Data Protection Law, rules on personal data protection may be found in various legislative documents in Gabon, as detailed below.

Please note that at the time of authoring this note, some links to official documents are not available.

The Electronic Communications Law

Law No. 26/2018 of 22 October 2018 regarding the Regulation of Electronic Communications in Gabon, which includes the provisions on electronic communications introduced by Order 13-PR-2018 from 23 February 2018 (only available in French here) ('the Electronic Communications Law') regulates the electronic communication sector in Gabon and establishes the regulatory authority for the sector - the Electronic Communications and Postal Authority ('ARCEP'). Among other provisions, the Electronic Communications Law regulates subscriber and terminal identification, numbering,

portability, and domain name identification. All these areas of regulation fall under the responsibility of ARCEP, except for the allocation and management of domain names which falls under the responsibility of the Minister in charge of electronic communications.

International Convention for the Suppression of the Financing of Terrorism

Law No. 02/2004 of 30 March 2005 ratifying the International Convention for the Suppression of the Financing of Terrorism (only available in French here) ('Law No. 02/2004') authorises the ratification of the International Convention for the Suppression of the Financing of Terrorism which imposes obligations on the banking sector to verify the identity and address of its customers. Law 02/2004 requires that the verification of identity be done through the presentation of an official identification document with a photograph, which must be copied and kept by the banking entity. Moreover, the address must be proven by a substantiating document. In addition, financial institutions must keep, for at least five years, all necessary records on national or international transactions performed.

CEMAC AML/CFT Regulation

Regulation No. 01/03 relating to the Prevention and Suppression of Money Laundering and Financing of Terrorism in Central Africa ('the AML/CFT Regulation') enacted by Central African Economic and Monetary Community ('CEMAC') has direct applicability in the countries belonging to CEMAC, such as Gabon. In fact, the AML/CFT Regulation replicates the same identification obligations and retention periods as Law No. 02/2004. However, the AML/CFT Regulation also provides obligations for casinos and gambling establishments.

Cybersecurity legislation

Order No. 15-PR-2018 on the Regulation of Cybersecurity and the Fight against Cybercrime (only available in French here) ('the Cybersecurity Regulation') provides a framework of the measures that must be put in place to guarantee the integrity, confidentiality, and security of data, such as authentication mechanisms and other recognised cybersecurity standards. In addition, the Cybersecurity Regulation sets out duties for network operators, electronic communication service providers, and information system operators by requiring them to retain connection and traffic data for a period of ten years and to install data traffic monitoring mechanisms on their networks and systems. Regarding network operators and electronic communication service providers, their data must only be accessible to judicial investigators. With respect to information system operators, the data must be only accessible if there is a judicial order. Notwithstanding, network operators and electronic communication service providers are liable if the use and retention of the data are not in accordance with the applicable laws and regulations.

Network operators must have an operation centre within Gabonese territory and every stakeholder must have a copy of the data in the national territory. Furthermore, electronic communication service providers and information system operators must put in place filters and measures to deal with attacks to the personal data of its subscribers. Furthermore, Order No. 7292-PM-MENCP of 16 July 2012 has created an Inter-Ministerial Technical Commission responsible for the examination of draft laws relating to the regulation of cybersecurity of electronic transactions and the protection of personal data, notably to contribute to initiatives and directives from the Economic Community of Central African States ('CEEAC') and CEMAC.

Census data protection

Order No. 578-MEEDD of 2 October 2013 regarding the Processing of Personal Data for the General Population and Housing Census ('the GPHC Order'). The GPHC Order establishes the processing operations for the establishment of an exhaustive database with individual, demographic, economic, and social data of every citizen and resident of Gabon. The envisaged data subject rights replicate those provided for in the Data Protection Law, with the exception of the right to oppose to the processing, which is not applicable.

The Constitution

Article 1 of the Constitution acknowledges and guarantees human fundamental rights. In particular, it guarantees that the secrecy of correspondence, postal communications, telegraph, telephone, and telematic communications is inviolable and that restrictions to such inviolability must be set by law and only for the purposes of public order and state security. The Constitution also provides that the limits for the use of computers to safeguard citizens and the intimate, personal and family life of people, as well as the full exercise of their rights, must be set by law. It should be noted that, in Gabon, the legislative branch shares the right to initiate new laws with the executive branch and any legislation, regulations, and orders on data protection derive directly from the Constitution.

1.2. Guidelines

Not applicable. Access to Gabonese guidelines is not well organised and, as such, the information is scarce. Any analysis regarding this matter must be considered on a sectoral and case-by-case basis.

1.3. Case Law

Not applicable. As far as we are aware, at the date of authoring this note, Gabonese case law on data protection matters is scarce.

2. SCOPE OF APPLICATION

2.1. Who do the laws/regs apply to?

Chapter I of the Data Protection Law establishes the scope of application of the legislation.

The following operations are subject to the Data Protection Law:

- any collection, transmission, use, and storage of data by a natural, legal, public, or private person;
- any automated or non-automated processing of data contained or to be included in a file;
- any processing operation carried out by a data controller on Gabonese territory or in any place where Gabonese law applies;
- any processing operation carried out by a data controller, established or not on Gabonese territory, which uses means of treatment located on the territory of Gabon, except for those that are only in transit on Gabonese territory; and
- any processing of data concerning public security, defence, research and prosecution of criminal offences.

2.2. What types of processing are covered/exempted?

The Data Protection Law applies to any personal data processing, specifically:

- any collection, processing, transmission, retention, or otherwise use of personal data by an individual or a legal entity, both in the public and private sector;
- any processing (regardless of whether or not it is automatic) of personal data intended to be included in a file (with the exceptions set out in the following paragraph);
- any processing carried out by a data controller in Gabon territory or in another location where Gabon law applies (a local controller representative should be appointed in these cases);
- any processing carried out by a data controller (regardless of it being established in Gabon) that resorts to processing means located on Gabonese territory, except in the event that the processing is carried out only for the purpose of transit; and
- any personal data concerning public security, defence, investigation and pursuit of criminal breaches or State security (even when the processing is linked to important economic or financial State interest, subject to any applicable derogations).

The following are excluded from the scope of the Data Protection Law:

- the processing of data carried out in the course of purely personal or domestic activities, except when personal data is intended for systematic communication to third parties or dissemination; and
- temporary copies associated with technical transmission and provision of access to a digital network for the purpose of automatic, transient, and intermediate storage of data, for the sole purpose of allowing certain parties with the best possible access to the data.

3. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

3.1. Main regulator for data protection

The Gabonese national authority for data protection is the Gabon data protection authority ('CNPDCP').

3.2. Main powers, duties and responsibilities

The CNPDCP is an independent administrative authority whose 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.

Chapter III of the Data Protection Law establishes the CNPDCP's powers and responsibilities which include:

- 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 ('the Government') 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 defining, 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.

4. KEY DEFINITIONS | BASIC CONCEPTS

The definitions are listed in Chapter I of the Data Protection Law.

Personal Data: Any information related to an identified or identifiable natural person, directly or indirectly referencing an identification number, or one or more elements specific to his, her, or their physical, physiological, genetic, psychological, cultural, social, or economic identity.

Sensitive Data: All personal data relating to religious, philosophical or political opinions, activities trade union, sex life, race, health, social measures, prosecution, and criminal or administrative sanctions.

Data Controller: Any natural, legal, public or private person, any organisation or association which, alone or with others, makes the decision to collect and process personal data and determines the purposes thereof.

Data Processor: Any natural, legal, public or private person, any organisation or association that processes data on behalf of the data controller.

Data Subject: The individual whose personal data is processed.

Data Subject consent: Any unequivocal, free, specific, and informed manifestation of will, by which the data subject or his/her legal, judicial or conventional representative, accepts that his/her personal data is processed either by electronic means or manually.

Health data: Any information regarding the physical and mental state of a data subject, including genetic information.

Third party: Any natural, legal, public or private person, any organisation or association other than the data subject, the data controller, the data processor, the sub-contractor and persons who, under the direct authority of the data controller or data processor, shall be entitled to process the data.

Processing of personal data: Any operation or set of operations provided for in the Data Protection Law carried out by means of automated or non-automated processes, and applied to data, such as the collection, organisation, storage, modification, extraction, copying, consulting, using, accessing, for communication by transmission, broadcast or any other form of provision, reconciliation or interconnection, as well as locking, encryption, the erasure or destruction of personal data and the interconnection of networks.

Interconnection of networks with personal data: Any connection mechanism consisting of linking the processed data for a specific purpose with other data (regardless of whether the intended processing is to be processed for identical), by one or various data controllers.

5. NOTIFICATION | REGISTRATION

5.1. Requirements and brief description

Chapter IV of the Data Protection Law establishes the formalities that must be followed to perform processing operations.

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 event of:

- 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. Indeed, 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.

As far as we are aware, the CNPDCP has not issued any guidelines or public decisions in this respect.

6. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

The obligations of data controllers are listed in Chapter V of the Data Protection Law and are organised into four groups:

- **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 in-

tegrity 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.

7. DATA PROCESSOR RIGHTS AND RESPONSIBILITIES

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.

8. DATA CONTROLLER AND PROCESSOR AGREEMENTS

An agreement between the data controller and data processor is mandatory and must be done in the form of a contract and shall include the obligations on confidentiality and security imposed by the data controller.

In addition, the agreement must provide that the data processor shall only act under the instructions of the data controller. The allocation of liability is not discussed under the Data Protection Law. However, a breach of the confidentiality obligation constitutes a violation of the professional secrecy with the consequences envisaged on the Criminal Code (only available in French here).

9. DATA SUBJECT RIGHTS

Chapter II of the Data Protection Law establishes the following data subject rights:

- right to request and access information pertaining to them and challenge the processing operation;
- right to obtain confirmation that their personal data is not subject to processing operations;
- right to obtain information relating to the purposes of the processing, the categories of personal data processed, the recipients to which the data are communicated, and possible transfers of personal data intended for a third country;
- right to obtain a copy of the personal data;
- right to obtain information regarding the origin of the data;
- right to complain to the CNPDCP;
- right to oppose for legitimate reasons the processing of personal data concerning them;
- right to oppose the processing of personal data for prospecting purposes;
- right not to be subject to decisions made on the sole basis of automated processing that would produce significant or detrimental legal repercussions for them; and
- right to have their personal data rectified, completed, updated, locked, or deleted where it is inaccurate, incomplete, equivocal, out of date, or if the collection, use, communication, or conservation is prohibited.

10. DATA PROTECTION OFFICER

10.1. DPO – compulsory appointment (yes/no)

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 European 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.

10.2. Requirements

Subject to the 10.1 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.

11. DATA BREACH NOTIFICATION

11.1. General obligation (yes/no)

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.

11.2. Sectoral obligations

None of the sectoral legislation mentioned in section 1.1 establish obligations related to data breach notification.

12. SANCTIONS

Chapter VII of the Data Protection Law stipulates the sanctions for non-compliance.

The CNPDCP shall assess and impose the following measures or sanctions, depending on the seriousness of the breach:

- a warning, that can be made public;

- a formal notice to restore compliance within a time limit defined by the CNPDCP.

If the data controller does not comply with the formal notice, the CNPDCP shall:

- suspend the data controller's data processing activities from a period up until two months, which may become permanent after the expiry of the two months;
- a pecuniary penalty between XOF 1 million (approx. €1,520) to XOF 100 million (approx. €152,000).

In case of an emergency, provided that the breach is seriously hindering the data subject's fundamental rights, the CNPDCP may:

- suspend the data processing activities of the data controller for a period up to three months;
- block certain processing operations for a period up to three months;
- ban any processing operations contrary to the provisions of the Data Protection Law.

Furthermore, if the data controller acts in bad faith other additional sanctions can be imposed.

The sanctions are imposed after a report of CNPDCP is made and after hearing the data controller.

The amount of the pecuniary penalty shall be proportionate to the seriousness of the breach and the benefits derived from such failure to comply. Upon a first breach, the fine may not exceed XOF 98.4 million (approx. €150,000). In the event of a repeat offence within five years from the date on which the pecuniary fine was imposed, it may not exceed XOF 300 million (approx. €457,000) or, in the case of an enterprise, 5% of the annual turnover.

In addition, a person who hinders the action of CNPDCP may be punished with imprisonment of six months to one year and/or with a fine from XOF 1 million (approx. €1,520) to XOF 100 million (approx. €152,000).

Finally, any offence committed by a person in breach of the Data Protection Law may also, depending on the circumstances, constitute a criminal infraction, in which case it is subject to the terms of the Criminal Code.

13. ADDITIONAL RELEVANT TOPICS

13.1. Data Transfers and Outsourcing

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 CNPD-CP. 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.

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.

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

13.2. Employment

Under the Data Protection Law, there are no specific provisions regarding privacy implications on employment, except the reference to the fact that the DPO may not be the target of any sanction or liability before his/her employer when exercising his/her rights and obligations as a DPO.

13.3. Data Retention

Under the Data Protection Law, personal data must not be kept for longer than the period necessary to achieve the purposes for which it was collected and processed.

This is naturally without prejudice to specific retention periods provided by sector-specific regulation or generally applicable judicial/administrative retention periods.

14. OTHER SPECIFIC JURISDICTIONAL ISSUES

Digital Gabon Strategy

Gabon has a Digital Gabon Strategy in force which aims to accelerate ICT activity within the country, to boost digital transition and to attract private investment.

Considering the Digital Gabon Strategy, the Government will need to update its legal and regulatory framework. In this context, there has been debate between various stakeholders regarding the need for sector-specific legislation on e-commerce, e-health, and cloud computing. We believe that, due to the nature of these legal and/or regulatory documents, they will consider, either directly or indirectly, privacy and data protection provisions.

CEMAC Electronic Communications Directive

Directive No. 07/08-UEAC-133-CM-18 of December 19, 2008 on the Legal Framework for the Protection of Users of Electronic Communications Networks and Services within CEMAC (only available in French here) ('the CEMAC Electronic Communications Directive') lays down several rules regarding processing of personal data, including, not only identification data, but also traffic data, and location data.

However, the CEMAC Electronic Communications Directive needs to be transposed, which according to its provisions should have been done within one year of its publication in 2008.

As far as we are aware, Gabon has not transposed the CEMAC Electronic Communications Directive. Consequently, although Gabon has approved legislation on electronic communications, it has no legislation specifically regulating privacy in electronic communications.