DATA PROTECTION LAWS OF THE WORLD

Niger

NIGER

Last modified 8 January 2024

LAW

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

- Law n° 2023-31 of 04 July 2023 amending law n°2022-59 of 16 December 2022 on the protection of personal data;
- Law n°2022-59 of December 16, 2022 relating to the protection of personal data;
- Decree No. 2020-309/PRN/MJ of April 30, 2020 setting the terms of application of Law No. 2017-28 of May 3, 2017 on the protection of personal data as amended and supplemented by Law No. 2019-71 of December 24, 2019;
- Order No. 000045 of October 5, 2020 determining the profile and setting the conditions of remuneration of the personal data protection correspondent;
- Law No.2018-45 of July 12, 2018 on the regulation of electronic communications in Niger; and
- Cybercrime Amendment Act 2022 (2019).

DEFINITIONS

Definition of Personal Data

Any information of any nature related to an identified or identifiable natural person, including sounds and images, directly or indirectly referencing an identification number, or one or more elements specific to his physical, physiological, genetic, psychological, cultural, social, or economic identity (Article 1 of the Law).

Definition of Sensitive Personal Data

Any personal data relating to religious or philosophical opinions or activities, political affiliation, sex life, race, health, social measures, prosecutions, and criminal or administrative sanctions (Article 1 of the Law).

NATIONAL DATA PROTECTION AUTHORITY

High Authority for the Protection of Personal Data (known by its French Acronym “**HAPDP**”).

The HAPDP is composed under the new Article 7 of the 2023 Act amending the 2022 Act on personal data of eleven members chosen because of their legal and / or technical competence.

In accordance with the new Article 6 of the aforementioned law, The HAPDP is attached to the Presidency of the Republic. The HAPDP is an independent administrative authority The HAPDP's role is to ensure that any processing of personal data is in accordance with the Law. In addition, the HAPDP's responsibilities include informing data controllers and data subjects of their rights and obligations, handling complaints, conducting audits, and sanctioning data controllers who are in breach of the Law.

REGISTRATION

The registration of processing activities via a "*register of processing activities&#8221*; does not exist in Niger.

The processing of personal data is subject to prior notification to the HAPD. If a data controller appoints a data protection officer, notification is unnecessary unless personal data is being transferred across national borders. Additionally, Article 64 Law n° 2022-59 of December 16, 2022 relating to the protection of personal data provides that the data controller must create an annual report for the HAPDP regarding personal data which is stored within the period, as fixed by the HAPDP, in relation to the purposes for which each type of processing activity was carried out.

DATA PROTECTION OFFICERS

There is no provision in the law relating to the appointment of a data protection officer.

However, Article 79 of the Law n°2022-59 of December 16, 2022 relating to the protection of personal data pertains to the designation of the personal data protection correspondent, which is defined in Article 1 as the person designated by the company carrying out the processing of personal data, to whom data subjects or interested persons may address any queries.

Article 79 of the of the aforementioned Law continues to state that the correspondent must possess the required qualifications to carry out their duties and be able to make a list of processing activities immediately accessible for any person requesting the same. The correspondent is exempt from any sanction on the part of the employer resulting from the carrying out of their duties.

Furthermore, the data controller's designation of a correspondent must be notified to the HAPDP and, in the event of failures to carry out their duties, may be discharged by request, or after consultation, from the HAPDP.

COLLECTION & PROCESSING

Any processing of personal data can only take place if the person concerned, the data subject, has expressed his consent in a free, specific, informed, and unambiguous manner. The processing of personal data is considered legitimate if the data subject gives his / her prior express consent.

The requirement of prior consent may be waived where the controller is duly authorised and the processing is necessary for:

- the performance of a contract to which the data subject is party or in order to take pre-contractual measures at his request;
- complying with a legal obligation to which the controller is subject to;
- protecting the interests or fundamental rights and freedoms of the data subject; and
- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.

The collection and processing of personal data must comply with the following principles:

- **The principles of lawfulness, fairness and transparency:** Data must be processed fairly, lawfully, and transparently. The lawfulness of the processing refers to its legal basis (legal obligation, contractual obligation, etc.). Fairness of processing refers to the manner in which the data are collected. This principle refers to the individual's right to information. Data must not have been collected and must not be processed without the knowledge of the data subject. This principle also requires providing data subjects with several pieces of information (on the processing of their data, but also on their rights).
- **The principle of proportionality:** Data must be adequate, relevant, and not excessive in relation to the purposes for which they are collected and further processed. The data controller must not collect more data than it actually needs. Thus, only data strictly necessary for the achievement of the specified purpose must be collected.
- **The principle of accuracy:** The data must also be accurate and, where necessary, updated. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they are collected and further processed, are erased or rectified.

The obligations of the Data controller include among other things:

- 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;
- collected data is retained in a form that allows the identification of the data subjects for a period that is no longer than necessary for the purposes for which it was collected;
- data subjects are informed of the data processing;
- data subjects have given their consents to the data processing;
- data subjects have the right to access the data and request amendments or deletions;
- persons with access to the system can only access the data they are allowed to;
- non-authorised persons cannot read, copy, modify, destroy, or move data;
- all data introduced in the system is authorised;
- non-authorised persons will not use data transmission facilities to enter into the data processing system;
- the identities of third parties having access to personal data will be checked;
- data is backed up with security copies; and
- data is renewed and converted to preserve it.

Under the 2022 Personal Data Act, the processing of personal data is subject to a prior notification to the HAPDP. The notification must include an undertaking that the processing meets the requirements of the Law.

However, for certain types of personal data processing, the prior authorisation of the HAPDP is required. This is particularly the case for the processing of personal data relating to genetic, medical data, and scientific research.

By contrast, the Data subject is entitled to an number of rights of which some are listed below:

Right of information: Pursuant to Article 68 of the 2022 Personal Data Act , the data controller must inform the data subject of:

- the identity and, where applicable, that of its duly authorised representative;
- the specific purposes of the processing for which the data is intended;
- the categories of data concerned;
- the recipient(s) to whom the data may be communicated;
- the possibility of refusing to appear on the file;
- the existence of a right of access to data concerning the person and a right to rectify this data; and
- the possibility of any data transfer to a third party.

Right of access: Pursuant to Article 69 of the Personal Data Act 2022, the data subjects can obtain from the data controller the following:

- information allowing to know and dispute the processing of personal data;
- confirmation of whether his / her personal data forms part of the processing;
- a copy of the data subject's personal data, as well as any available information on the data's origin; and
- information relating to the purposes of the processing, the categories of personal data processed and the recipients or categories of recipients to whom the data are communicated.

Right to rectification: Under the provisions of Article 71 of the 2022 Personal Data Act , any natural person who can prove his or her identity may require the data controller to rectify, complete, update, block, or delete, as the case may be, any personal data concerning him or her that is inaccurate, incomplete, ambiguous, out of date, or whose collection, use, communication, or storage is prohibited.

Right to erasure: Under the provisions of Article 73 of the 2022 Personal Data Act, the data subject shall have the right to obtain from the controller the erasure of personal data relating to him or her and the cessation of the dissemination of such data, in particular with regard to personal data which the data subject made available when he / she was a minor, or for one of the following reasons:

- the data is no longer necessary for the purposes for which they were collected or processed;
- the data subject has withdrawn the consent on which the processing is based or where the authorised retention period has expired and there are no other legal grounds for processing the data;
- the data subject objects to the processing of personal data relating to him or her where there is no legal ground for such processing;
- the data processing does not comply with the provisions of this Law; or
- for any other legitimate reason.

Right to object: Any data subject has the right to:

- oppose the processing of their personal data;
- oppose the processing of their personal data for prospecting purposes; and
- be informed before his / her personal data is communicated to third parties.

Interconnection of personal data shall:

- not discriminate against or limit the fundamental rights, freedoms, and guarantees of data holders;
- ensure the use of appropriate safety measures; and
- take into account the principle of relevance.

TRANSFER

Transfer of personal data to another country is allowed only when that country provides a superior or equivalent level of protection for privacy, freedoms and fundamental rights of individuals regarding the processing of personal data (Article 62 of the Law).

SECURITY

Article 82 of the 2022 Data Protection Act sets out the security obligations of data controllers and processors with regard to the protection of personal data. They must put in place technical and organisational measures to prevent distortion, damage or unauthorised access to such data, taking into account the nature, scope, context and purposes of the processing, as well as the risks to individuals. These measures may include pseudonymisation, encryption, anonymisation and encryption of personal data, as well as regular testing, analysis and evaluation procedures to ensure the security of the processing. Appropriate security policies must also be put in place, including the obligation of protection by design and protection by default of personal data necessary for each specific purpose of processing.

BREACH NOTIFICATION

Under article 83 of the 2022 Personal Data Protection Act, the controller of personal data is required to notify the Data Protection Authority (HAPDP) of any personal data breach as soon as it becomes aware of it. This notification must be made without delay and, in the event of a high risk to the rights and freedoms of the data subjects, the data controller must also inform the data subjects as soon as possible. However, the controller is not required to notify a data breach if it is reasonable to believe that the breach does not present a risk to the rights and freedoms of the data subjects. It is important to note that failure to comply with this notification obligation must be justified and substantiated by the data controller to the data protection authority. Failure to comply with this obligation may result in criminal penalties, such as imprisonment and fines, as set out in Article 98 of the Act.

Mandatory Breach Notification

Mandatory notification of personal data breaches is provided for in Article 83 of the 2022 Personal Data Protection Act. According to this article, as soon as the data controller becomes aware of a personal data breach, it must inform the HAPDP without delay. In addition, if the breach is likely to result in a high risk to the rights and freedoms of an individual, the controller must notify the data subject of the security breach as soon as possible.

ENFORCEMENT

The law empowers the HAPDP 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.

The HAPDP may, directly or through an expert authorized for this purpose, carry out checks and controls on any processing of personal data. In fulfilment of their duties, the HAPDP officers 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.

On completion of its checks and inspections, the HAPDP may impose the following administrative sanctions on offenders, without prejudice to criminal prosecution:

- a warning;
- formal notice;
- injunction to cease data processing;
- blocking of certain personal data;
- lump-sum fines;
- withdrawal of authorization.

The amount of the fine is proportionate to the seriousness of the breaches committed and to the benefits derived from the breach. The fine may not exceed the sum of XOF 100,000,000.

In the event of a repeat offence within two years of the date on which the financial penalty previously imposed became final, the amount may not exceed XOF 200,000,000 or, in the case of a company, 5% of the turnover excluding tax for the last financial year for which the accounts have been closed, subject to a limit of XOF 500,000,000.

Unlawful processing of sensitive data, direct canvassing without prior consent, failure to comply with security measures, misuse, fraudulent, unfair or unlawful collection of data, unauthorised communication of personal data, obstructing the exercise of the rights of the person concerned, unlawful storage and unauthorised disclosure of personal data are punishable by imprisonment and a fine.

Depending on the nature of the offence, the penalty may range from three (3) months to five (5) years' imprisonment and a fine of up to 50,000,000 francs.

Sanction by the data protection Authorities may be appealed before the competent administrative court.

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 58 of Law No.2018-45 of July 12, 2018 on the regulation of electronic communications in Niger).

Even when a marketer has the consent of a data subject, that consent can be withdrawn by the data subject under Article 28 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.

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 82 of the 2022 Data Protection Act, 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.