# DATA PROTECTION LAWS OF THE WORLD

Chad

# CHAD

*Last modified 17 January 2024*

## LAW

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

- Act No. 007/PR/2015 of February 10, 2015, on Personal Data protection (‘**The Act**’);
- Decree No. 075/PR/2019 of January 21, 2019 implementing the provisions of application of the Act N°007/PR/2015 of February 10, 2015 on the protection of personal data;
- Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification;
- Ordinance No. 002/PR/2019 amending Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification;
- Ordinance No.012/PT/2023 dated 1st August 2023 amending the Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification;
- Ordinance No. 014/PT/2023 dated 30 August 2023 amending the Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification;
- Ordinance No. 009/PCMT/2022 amending Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification;
- Act No. 009/PR/2015 on the cybersecurity and the fight against the cybercrime;
- Ordinance No. 008/PCMT/2022 on the Cybersecurity in the Republic of Chad; and
- Act No. 008/PR/2015 on electronic transactions.

## DEFINITIONS

### Definition of Personal Data

**Personal data:** Any information relating to a natural person, identified or identifiable directly or indirectly, by reference to an identification number or to one or more elements specific to his or her physical, physiological, genetic, psychological, cultural, social, and economic identity. (Article 5 of the Act)

### Definition of Sensitive Personal Data

**Sensitive data:** Data relating to religious, philosophical, political, trade union opinions or activities, sex or racial life, health, social measures, prosecutions, and criminal or administrative charges. (Article 5 of the Act)

## NATIONAL DATA PROTECTION AUTHORITY

The National Data Protection Authority is the *Agence Nationale de Sécurité Informatique et de Certification É lectronique* ('**ANSICE**').

ANSICE is responsible for ensuring compliance, on the national territory, with the provisions of the Act. As such, it has the power to sanction any violation of the Act.

ANSICE main duties include:

- informing the data holders and the data controllers of their rights and obligations;
- receiving the formalities prior to the creation of processing of personal data;
- receiving complaints, petitions and claims relating to the implementation of the processing of personal data and informs their authors of the follow-up given to them;
- informing the judicial authorities without delay of the offences of which it has knowledge;
- entitling its members or agents with the task of carrying out verifications relating to any processing and, where appropriate, obtaining copies of any document or information medium useful for its mission;
- imposing a sanction on a data controller;
- keeping a directory of personal data processing at the disposal of the public;
- authorizing, under the conditions provided for in the Act, the transborder transfer of personal data.

(Article 6 of the Act Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification)

## REGISTRATION

The is no country-wide system of registration in Chad. However, the processing of personal data may be subject to prior notification to, or authorization/Prior approval from the CDP.

### Regime of authorisation

The authorisation of the ANSICE is required for the processing of any personal data relating to:

- genetic, biometric data, and research in the health field;
- offenses, convictions, or security measures;
- interconnection of files;
- national identification number or any other identifier of the same nature; or
- public interest in particular for historical, statistical, or scientific purposes.

### The regime of declaration

Apart from the data provided for by the authorisation regime, any processing of personal data must be declared in a written form and addressed to ANSICE.

### Notice/Opinion regime ("Avis")

The automated processing of personal information carried out on behalf of the State, a public institution or a local authority or a legal person under private law managing a public service are decided by regulatory act taken after a reasoned opinion from the ANSICE. Such processing relates to:

1. State security, defense or public safety;
2. the prevention, investigation, recording or prosecution of criminal offences or the execution of criminal sentences or security measures;
3. the population census;
4. personal data that reveal, directly or indirectly, the racial, ethnic or regional origins, parentage, political, philosophical or religious opinions or trade union membership of persons, or that relate to the health or sexual life of persons when they are not covered by provisions related to interconnexion of data;
5. the processing of salaries, pensions, taxes, and other settlements.

(Articles 51, 52 and 53 of the Act)

## DATA PROTECTION OFFICERS

There are no specific provisions relating to the appointment of a Data Protection Officers (‘**DPO**’) under the Act. This issue is left at the exclusive discretion of the data controllers.

## COLLECTION & PROCESSING

Data collection and processing are subject to the following principles and requirements:

- The collection, recording, processing, storage, and transmission of personal data must be lawful, fair, and not fraudulent;
- Data must be collected for specified, explicit, and legitimate purposes;
- Data must be relevant and not excessive in relation to the purposes for which they are collected and further processed;
- Data must be kept for a period not exceeding the period necessary for the purposes for which they were collected /processed;
- The data collected must be accurate and, if necessary, updated whenever necessary;
- Data controller must inform the data subject of any personal data processing operation that involves personal data; and
- Personal data must be treated confidentially and protected.

The Data holders/subjects have rights to:

- **To be informed:** Pursuant to Article 35 and seq. of the Act, the data controller must inform the data subject of:
  - the identity of the data controller and its representative (if any);
  - the purposes of the processing;
  - the category of data concerned;
  - the recipients or categories of recipients of the data;
  - the right to object to the collection of such data;
  - the right to access the collected data and have it edited;
  - the duration of the processing; and
  - details on any intended transfer of the data.
- **To access:** Pursuant to Article 38 of the Act, data subjects have a right of access and they can obtain the following from the data controller:
  - information allowing for data subjects to be aware of and the possibly to contest the processing;
  - confirmation of whether his/her personal data forms part of the processing;
  - copy of his/her personal data as well as any available information on the origin of the data; and
  - information relating to the purposes of the processing, categories of data processed, recipients, or categories of recipients, to whom the data are disclosed, and information relating to the transfer of personal data outside the country.
- **To rectification:** In light of the provisions of Article 48 of the Act, any data subjects may require that the data controller rectifies their personal data if it is inaccurate, incomplete, unclear, or expired, or if the collection, usage, disclosure, or retention of the data is prohibited.
- **To erasure:** In light of the provisions of Article 48 of the Act, any data subjects may require that the data controller deletes their personal data if it is inaccurate, incomplete, unclear, or expired, or if the collection, usage, disclosure, or retention of the data is prohibited.
- **Right to object/opt-out:** Pursuant to Article 45 of the Act, any data subject has the right to object, with legitimate reasons, to the processing of his/her personal data. The data subject also has the right to be informed before his/her personal data is communicated or used by a third party and also to object the communication or the use of the personal data.

## TRANSFER

In light of Article 29 of the Act, the data controller cannot transfer personal data to another foreign country non-member of the CEMAC/CEAC unless that country provides a sufficient level of protection for the privacy, fundamental rights, and freedoms of individuals.

Moreover, prior to any transfer of personal data abroad, the data controller must first inform the regulatory authority, ANSICE.

CEMAC is the French acronym of Economic and Monetary Community of Central Africa. CEEAC is the French acronym of the Economic Community of Central Africa States.

A transfer to a non CEMAC/CEEAC country not offering a sufficient level of protection is possible if:

- the Data Subject agrees to the transfer;
- the transfer protects the life of the Data Subjects/Holders;
- the transfer Protect the public interest;
- the transfer is necessary to the performance of an agreement between the Data Subject and the Data Processor or take precontractual measures upon the request of the Data Subject;
- If the transfer intervenes from a public register which, according to law and regulations, is focused on the public information and open to the public consultation.

The ANSICE may allow the Data controller to transfer data to a foreign country non-member of CEMAC/CEEAC if the Data controller provides sufficient protection for the Data Subject’s private life, liberties, and fundamental rights.

(Articles 30-33 of the Act)

## SECURITY

Data Controllers are required to ensure the security of personal data. They must prevent the data’s alteration and damage, or access by non-authorised third parties. In this regard, Data Controllers should make sure that:

- Persons with access to the system can only access the data that they are allowed to access;
- The identity and interest of any third-party recipients of the data can be verified;
- The identity of persons who have access to the system (to view or add data) can be verified;
- Unauthorised persons cannot access the place and equipment used for the data processing;
- Unauthorised persons cannot read, copy, modify, destroy, or move data;
- All data entered onto the system are authorised;
- The data will not be read, copied, amended, or deleted without authorisation during the transport or communication of the data.
- The data are backed up with security copies;
- The data are renewed and converted to preserve them.

(Article 60 of the Act)

## BREACH NOTIFICATION

Breach of the provisions of Personal Data Act including breach notification is subject to following administrative sanctions by the ANSICE:

- a warning to the data controller who does not comply with the obligations arising from the Law;
- a formal notice to put an end to the breaches concerned within the time limit which it fixes;
- penalties in accordance with the observed shortcomings;
- interruption of treatment for a maximum of three years;
- blocking for a maximum of three months of certain processed personal data; or
- temporary or permanent prohibition of processing contrary to the provisions of the Act.

(Article 8 Article 8 of Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification)

In addition, a judge can take the following sanctions in case of breach notification:

- Imprisonment from between 1-5 years;

- Fines between XAF 1 million to XAF 10 million.

(Article 438 of the Criminal Code)

### Mandatory breach notification

No mandatory breach notification protocol is provided under Chadian law.

## ENFORCEMENT

The ANSICE have enforcement powers including:

- Investigative powers: The ANSICE can conduct investigation to discover facts and evidences of the violation of the Act. Administrative fines for infringements of the Data Protection Act
- Non-compliance with the ANSICE instructions/decisions can lead to the following sanctions:
    - a warning;
    - an injunction to put an end to defaults within the time limit set by the ANSICE; or
    - a provisional withdrawal of the authorisation granted for a period of three months at the expiry of which the withdrawal becomes final.

In case of urgency, the ANSICE can:

- interrupt a processing for a duration that cannot exceed three months.
- lock certain kinds of data for a duration that cannot exceed three months; or
- rohibit, provisionally or definitively, data processing that does not comply with the Act.

Additionally, the Act has the power to issue a temporary or permanent ban. The ban does not require a court order.

(Article 8 of Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification and Article 81 of the Act)

## ELECTRONIC MARKETING

Sending of marketing communications is forbidden on principle unless the recipient agrees to it.

Also, there are specific cases under which prior approval is not required:

- the recipient’s information was collected directly from him, in accordance with the provisions of the Act;
- the recipient is already a customer of the company, the marketing messages relate to products or services that are similar to those previously provided, and the recipient is given the possibility of objecting to all messages sent to him;
- if it clearly explained to the Data subjects where their data is collected that they have right to object, free of charge, to the processing of their Personal Data for electronic marketing;
- when the electronic marketing concerns the data of legal personals which are not constitute personal data.

(Article 49 of Act No. 008/PR/2015 on electronic transactions)

Breach of the provisions of Personal Data Act including breach of electronic marketing provisions are subject to following administrative sanctions by ANSICE:

- a warning to the data controller who does not comply with the obligations arising from the Law;
- a formal notice to put an end to the breaches concerned within the time limit which it fixes;
- penalties in accordance with the observed shortcomings;
- interruption of treatment for a maximum of three years;
- blocking for a maximum of three months of certain processed personal data; or
- temporary or permanent prohibition of processing contrary to the provisions of the Act.

In addition, a judge can take the following sanctions in case of violation of provisions of Act No. 008/PR/2015 on electronic transactions including on its provisions relating to electronic marketing:

- imprisonment from between 1-10 years;
- and fines between XAF 1 million to XAF 5 million.

(Article 168 of Act No. 008/PR/2015 on electronic transactions)

## ONLINE PRIVACY

There is no specific restriction on the use of cookies under the Act. However, the ANSICE requires that the Data Subject is informed of the use of cookies and to collect his consent.

## KEY CONTACTS

**Geni & Kebe**
www.dlapiperafrica.com/senegal

Mouhamed Kebe
Managing Partner
Geni & Kebe
T +221 76 223 63 30
mhkebe@gsklaw.sn

Mahamat Atteib
Associate
Geni & Kebe
T +221 77 737 41 74
m.atteib@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.