DATA PROTECTION LAWS OF THE WORLD

Burkina Faso

DLA PIPER

BURKINA FASO

Last modified 8 January 2024

LAW

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

- Law No. 001-2021 of March 30, 2021 on the protection of persons with regard to the processing of personal data.
- Law 010-2004/AN on the protection of personal data.
- Decree No. 2007-283/PRES/PM/MPDH of 18 May 2007 regarding the organisation and functioning of the Commission de l'Informatique et des Libertés;
- Decree No. 2007-757/PRES/PM/MPDH/MEF appointing the members of the Commission de l'Informatique et des Libertés ; and
- Order No. 2008/001/CIL fixing the internal regulations of the Commission de l'Informatique et des Libertés.

The Burkina Faso has also adopted on 22 November 2013 the Marrakech resolution issued by the French-speaking association of data protection authorities relating to the procedure for the supervision of personal data transfers of personal data in the French-speaking world by means of binding corporate rules.

DEFINITIONS

Definition of Personal Data

Any information that allows, in any form whatsoever, directly, or indirectly, the identification of natural persons, in particular by reference to an identification number or to several characteristics specific to their physical, psychological, mental, economic, cultural or social identity (Article 5 of the Law).

Definition of Sensitive Personal Data

Any personal data relating to the data subject's health or that reveal racial or ethnic origins, political, philosophical or religious opinions, union membership, morals, investigation and prosecution of offenders, criminal or administrative penalties, related security measures or other measures of a similar nature (Article 5 of the Law).

NATIONAL DATA PROTECTION AUTHORITY

The Burkina Faso's data protection authority is the Commission de l'Informatique et des Libertés ('**CIL**').

The CIL draws its membership from various segments of society. It is charged with:

- making individual or regulatory decisions in cases provided for under the law;
- assisting with data processing inspections and obtaining all information and documents needed for its mission;
- issuing model rules to ensure security; and where appropriate, prescribing safety measures including the destruction of information;

- issuing enforcement notices to data controllers and sharing with the prosecutor’s office the offenses of which the body is aware;
- ensuring that the implementation of the right of access and rectification indicated in the acts and declarations do not impede the free exercise of this law;
- receiving complaints and petitions;
- staying informed of the latest technological developments, and keeps abreast of their effects on the right to the protection of privacy, the exercise of freedoms, and the functioning of democratic institutions;
- advising individuals and organisations that use automated processing, or who carry out tests or experiments likely to lead to such processing;
- responding to requests for public opinion; and
- proposing legislation or regulations to the Government to adapt the protection of freedoms to technological evolution.

REGISTRATION

The is no country-wide system of registration in Burkina Faso. However, the law imposes an obligation of notification and annual reporting to the National Data Protection Authority. These annual reports provide information on those responsible of personal data's activity throughout the concerned year.

DATA PROTECTION OFFICERS

We have not identified any obligation to appoint a data protection officer ('**DPO**') or any other equivalent role in the law.

COLLECTION & PROCESSING

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. These include:

- **consent and legitimacy:** unless otherwise provided by law, data controllers are obligated to obtain consent from the data subject;
- **purpose:** personal data can only be collected and processed for a specific and legitimate purpose;
- **proportionality and relevance:** personal data must only be processed in a relevant and necessary manner regarding the purpose and objectives of the processing;
- **lawfulness and fairness:** data controllers must collect and process data in a fair, lawful, and not fraudulent manner
- **data retention:** a specified period of time should be determined in advance depending on the purpose of processing to ensure that personal data is not stored indefinitely;
- **security and confidentiality:** all responsible persons for processing personal data must not only ensure the security of data or files to prevent their destruction, or alteration; but also prevent unauthorised access to personal data contained in a file or intended to form part of the files;
- **preliminary formalities:** without exception or exemption provided by law, all data controllers shall, depending on the nature of personal data processing, namely notify the CIL or ask his opinion or obtain approval, etc.

Except where provided otherwise by the law, any processing of personal data shall be carried out with the express consent of the data subject(s).

The processing of personal data can legally be carried out without the consent of the data subject(s), when it is necessary for:

- the performance of a contract to which the data subject is a party; or
- pre-contractual measures taken at the request of the data subject;
- compliance with a legal obligation to which the controller is subject and when the processing is essential to protect the life of the data subject or that of a third party;
- the purposes of preventive medicine, medical diagnosis, the administration of care or treatment, or the management of health services, provided that it is carried out by a member of a health profession or by another person who, by reason of his / her duties, is bound by professional secrecy;

- the establishment of an offence, a right, or the exercise or defence of a right in a court of law and when the said processing relates to data made public by the data subject.

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller. It may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Data subjects may request erasure of their personal data. It has the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

Unless an authorisation is required, the law provides that controllers should notify all processing to the CIL. The following are exempt from the notification requirement to CIL:

- temporary copies that are made as part of the technical activities of transmission and provision of access to a digital network for the purpose of automatic intermediate and transitory storage of data for the sole purpose of allowing other recipients of the service the best possible access to the information;
- processing carried out by a natural person for the exercise of exclusively personal or domestic activities;
- disclosed to third parties and not used to support actions or decisions against an individual;
- automated processing of personal data for the purpose of research in the field of health;
- automated processing of personal data carried out on behalf of the State, a public institution, a local authority or a legal person under private law managing a public service.

With respect to day-to-day processing of data which do not infringe on privacy or freedoms, the Law provides that the CIL establishes and publishes 'simplified norms,' which shall include certain information, including:

- the date of the declaration;
- the full name and address or the name and headquarters of the person making the request and the person who has the power to decide on the creation of the data processing (data controller) or, if he or she resides abroad, his or her representative in Burkina Faso;
- the characteristics, purpose and, if applicable, the name of the data processing operation;
- the department or departments responsible for carrying out the processing;
- the department to which the right of access is to be exercised and the measures taken to facilitate the exercise of this right
- the categories of persons who, by reason of their functions or for the needs of the service, have direct access to the information recorded;
- the personal information processed, its origin and the length of time it is kept, as well as the recipients or categories of recipients authorized to receive this information;
- the reconciliation, interconnection or any other form of linking of this information as well as its transfer to third parties;
- the measures taken to ensure the security of data and information processing and the guarantee of secrets protected by law;
- if the data processing is intended for the dispatch of personal data between the territory of Burkina Faso and abroad in any form whatsoever, including when it is the object of operations partially carried out on the territory of Burkina Faso from operations previously carried out outside Burkina Faso.

When processing complies with a simplified norm issued by the CIL, no authorisation or notification is required, but only a 'simplified declaration of conformity,' to the said norm is required. The simplified declaration of conformity shall be sent to the CIL. Unless otherwise decided by the CIL, a receipt is issued without delay after the simplified declaration of conformity has been sent to the CIL. As from receiving this receipt, the applicant can start carrying out the processing.

Except in cases where they are to be authorised by law, automated processing of personal data carried out on behalf of the State, or on behalf of any public institution, local authority, or on behalf of a private legal person operating a public service, must be authorised by decree after the CIL's approval. In the case of a negative opinion by the CIL, an appeal can be lodged to the Administrative Supreme Court *(Conseil d’Etat).*

TRANSFER

The provisions of the Law pertaining to international transfers are broadly drafted.

According to said provisions, international transfers cannot be made without the respect of the following conditions:

- To request the authorisation of the CNIL;
- To sign with the contracting party, a data confidentiality clause and a data reversibility clause in order to facilitate the complete migration of the data at the end of the contract;
- Implement technical and organisational security measures.

Additionally, the transfer can only be made to a foreign country or an international organisation if the beneficiary country or international organisation ensures an adequate level of protection equal to the one ensured in Burkina Faso (Article 42 of the law).

As a signatory to the Marrakech Resolution of 22 November 2013, Burkina Faso recognizes the application of the French-speaking RCE, which consist in a code of conduct by which a group of companies defines its internal policy on the transfer of personal data. The RCE are based and designed on the model of the European Commission’s binding corporate rules ('**BCR**').

In practice, the RCE mechanism concerns the authorities of the AFAPDP member countries that have adopted the cooperation protocol and the resolution on the framework for data transfers in the French-speaking area. These concerns at least the following 13 countries: Albania, Andorra, Belgium, Benin, Burkina Faso, France, Gabon, Luxembourg, Mauritius, Morocco, Senegal, Switzerland and Tunisia.

The RCE cover intra-group transfers of personal data carried out by a company established in an AFAPDP member country, to other companies of the group, whether the latter are located in an AFAPDP member country or not.

SECURITY

The personal data Act is not prescriptive about specific technical standards or measures.

However, the Article 24 states that the data controller shall take all necessary measures in view of the nature of the data and the architecture of the processing, in particular to prevent them from being distorted, damaged, lost, stolen or accessed by unauthorised parties.

BREACH NOTIFICATION

Not applicable.

Mandatory breach notification

We have not identified, in the law, any general obligation to notify the data subject in the case of a security breach. However, Article 21 of the law provides that in the event where 'information has been transmitted by mistake to a third party, its rectification or cancellation shall be notified to that third party, unless an exemption is granted by the control authority' (i.e. the CIL).

ENFORCEMENT

The law empowers the CIL 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 CIL may, directly or through an expert authorized for this purpose, carry out checks and controls on any processing of personal data.

However, if the data controller initiates the inspection, he or she must pay the inspection fees, the amount of which is set by order of the Minister of Finance.

On completion of its checks and inspections, the CIL 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 sanctions provided for by law are imposed on the basis of a report drawn up by one of the members of the CIL, appointed by the Chairman. This report is sent to the data controller, who may submit observations and be represented or assisted at a hearing before the CIL.

The amount of the fixed fine provided for by law is proportionate to the seriousness of the breaches committed and the benefits derived from the breach. For the first offence, the fine is one percent of sales excluding tax for the last financial year for which the accounts have been closed. In the event of a repeat offence, the fine is five percent of sales excluding tax for the last financial year for which the accounts have been closed. Fixed-rate fines are recovered as receivables from the State.

Financial penalties may also be imposed on any data controller, ranging from XOF five million (5,000,000) to XOF one hundred million (100,000,000).

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 49 of law No. 045-2009/AN of November 10, 2009 regulating electronic services and transactions in Burkina Faso and Article 14 of the personal data Act).

Even when a marketer has the consent of a data subject, that consent can be withdrawn by the data subject under Article 20 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 favourably 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 governing cookies and location data.

However, pursuant to Article 10 of the data controller must implement all appropriate technical and organisational 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 unauthorised persons.

KEY CONTACTS

Geni & Kebe
www.dlapiperafrica.com/senegal

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

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