MOAVOCAT

January 2024

Newsletter

PERSONAL DATA PROTECTION IN THE REPUBLIC OF BENIN

Given the exponential growth in IT resources and the digitalisation of tools in recent years, the management of personal data has become a major strategic challenge for companies.

Indeed, at the heart of digital confidence and the development of connected technologies, the protection granted to personal data is a crucial issue for individuals who, in the digital age, are becoming more sensitive to the issue of the management and the use of their data.

In Benin, as in many other countries, companies must deal with an increasingly restrictive legal framework and comply with requirements aiming to preserve, particularly the privacy, confidentiality, integrity and security of personal data.

What is personal data?

Any information of any kind whatsoever and regardless of its medium, including sound and image, relating to an ***identified or identifiable*** *natural person, referred to as the data subject.*

An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a forename or surname, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, cultural, social or economic identity.

Framework for the protection of personal data in Benin

The legal regime for the protection of personal data is mainly enshrined in Law No. 2017-20 of 20 April 2018 on the Digital Code in the Republic of Benin as amended by Law No. 2020-35 of 06 January 2021 (the "**Digital Code**").

In particular, the provisions of Section V of the Digital Code are intended to set up a legal framework for the protection of the privacy and professional life following the **processing operations of personal data.**

What is personal data processing?

Any operation or set of operations which may or may not be performed upon personal data or sets of personal data, such as collection, use, recording, organisation, structuring, retention, adaptation, modification, retrieval, storage, copying, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, encryption, erasure or destruction.

This legal framework guarantees that all processing, whatever its form, respects the fundamental rights and freedoms of individuals. The Digital Code defines the general conditions for lawful processing and specifies that personal data must be:

- legitimately treated;
- collected, recorded, processed, stored and transmitted in a lawful, fair, transparent and non-fraudulent manner;
- collected for specified, explicit and legitimate purposes and not subsequently processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and processed;
- accurate and, where necessary, updated. All reasonable steps must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified;
- kept in a form which permits identification of the persons concerned for no longer than it is necessary for the purposes for which it is collected or for which it is processed. Personal data may be kept for longer periods insofar as it is processed exclusively for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes, provided that the appropriate technical and organisational measures required to guarantee the rights and freedoms of the person concerned are implemented; and
- processed in such a way as to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These general conditions are reflected in a range of principles, including transparency, confidentiality, security, responsibility of the data controller, consent and legitimacy.

This regime, set up by the legislator, is intended to encourage **data controllers** to implement the appropriate technical and organisational resources to ensure and be able to demonstrate at any time that the processing carried out complies with the requirements set out in the Section V of the Digital Code.

What is a data controller?

Any individual or legal entity, public authority, service or any other body or association which, alone or jointly with others, takes the decision to collect and process personal data and determines the purposes and means thereof.

In particular, the provisions of the Digital Code set out various obligations incumbent on data controllers, including :

- the obligation to complete prior formalities with the Personal Data Protection Authority by notifying the processing of personal data and, where applicable, obtaining prior authorisation for processing;

the obligation to inform the person concerned about the characteristics of the processing of his or her personal data;

- the obligation to ensure the confidentiality and security of personal data processed by implementing appropriate technical and organisational measures (pseudonymisation and encryption of personal data, etc.);
- the obligation to respect the rights of the persons affected by the processing (right of access, portability, query, opposition, rectification and deletion, etc.);
- the obligation to hold a register of processing activities containing all personal data processing carried out by the entity or body; and
- the obligation to draw up an annual report to the Personal Data Protection Authority.

In addition to data controllers, co-controllers and sub-contractors, who are important stakeholders in the process of collecting and processing personal data, are also subject to the same obligations.

Moreover, the responsibility of data controllers is supported by a self-assessment mechanism. This is achieved by maintaining compliance documentation (the register of processing activities, the impact assessment, internal procedures for managing personal data, subcontracting contracts, proof that the consent of the persons concerned has been obtained where applicable, etc.).

Designing the documentation and managing the self-assessment requires the expertise of firms or specialised institutions in compliance. It should be remembered that such compliance may be subject to control by certain authorities.

The institutional framework for the protection of personal data in Benin

Section V empowers the Personal Data Protection Authority[1] ("**APDP**") to oversee its application and respect for privacy in the Republic of Benin. Its main mission is to ensure that Information and Communication Technologies (ICTs) do not constitute a risk to public freedoms and privacy.

[1] The *Autorité de Protection des Données Personnelles* is the new name of the *Commission Nationale de l'Informatique et des Libertés* (CNIL). This new name results from the application of the Additional Act A/SA.1/01/10 on the protection of personal data within the ECOWAS zone.

News 2024: Appointment of new APDP members

On 31 January 2024, the new members of the 3rd mandate of the APDP were appointed by the Council of Ministers.

The *APDP* is an administrative authority with legal personality and administrative, financial and management autonomy.

It is endowed with broad attributions and sanctioning powers to require data controllers to comply with the legislation in force. In particular, it is able to:

- authorise or refuse the processing of files in number of cases, particularly sensitive files;
- receive, by postal or electronic channels, complaints, petitions and claims relating to the processing of personal data and to inform their authors of the action taken of them, in particular if further investigations or coordination with another national data protection authority is necessary;
- carry out, without prejudice to any action before the courts, investigations, either on its own initiative or following a complaint or at the request of another national protection authority, and inform the person concerned, if he or she has submitted a complaint, of the outcome of its investigations within a reasonable period;
- inform the judicial authorities without delay of certain types of offences of which it has knowledge;
- request the controller or processor to comply with the claim of the person concerned to exercise his or her rights under the provisions of Section V;
- impose sanctions against data controllers; and
- authorise or refuse cross-border transfers of personal data to third countries.

The risks faced by companies in the event of non-compliance

In practice, the redefinition of the legal framework for the protection of personal data in Benin has encouraged companies to rethink their internal policies and to adopt a genuine compliance programme, including the deployment of procedures for the management of personal data, as well as training and awareness-raising initiatives for the various stakeholders. These steps should not be overlooked, as they will enable companies to avoid sanctions by complying with the provisions of the Digital Code.

To ensure that this legal regime is effectively implemented, the legislator has provided for various types of sanctions, including administrative sanctions and measures (warnings, formal notices, injunctions, etc.)[2] and criminal sanctions[3] .

2 Article 452 et seq. of the Digital Code.

3 Articles 460 and 461 of the Digital Code.

In the event of non-compliance with the provisions of the Digital Code, data controllers are liable to sanctions which, depending on the seriousness of the breach, may amount to up to five percent (5%) of the turnover excluding tax for the last financial year for which the accounts have been closed, subject to a limit of one hundred million (100,000,000) XOF. They are also liable to prison sentences ranging from six (06) months to ten (10) years.

In addition to these sanctions, companies that fail to comply with the legal regime for the protection of personal data must also take into consideration the reputational risk, which can sometimes be disastrous (loss of confidence from clients, partners, shareholders, etc.).

CONTACTS

Olatoundé Marius ATTINDOGBE
Partner

Sandra Yowa MUSENGA
Consultant

Street 4.226, Akpakpa, Cotonou

06 BP 3950, Cotonou

www.moavocat.com

+229 41 46 00 00

+229 91 94 94 94

contact@moavocat.com