DATA PROTECTION LAWS OF THE WORLD

Benin

Downloaded: 7 August 2024

BENIN

Last modified 8 January 2024

LAW

The data protection regime in Benin is governed by two pieces of legislations namely the Law No. 2017-20 of April 20, 2018 on the digital code and the Law No. 2009-09 of May 22, 2009 Dealing with the Protection of Personally Identifiable Information.

The Law on the digital code deals with the collection, treatment, transmission, storage, and use of personal data by a person, the state, local authorities, and legal persons, as well as automated processing and non-automated processing of personal data contained in files, or any processing of data for public security, defense, research, prosecution of criminal offenses, or the security and essential interests of the state.

By contrast, the Law on the Protection of Personally Identifiable Information relates to the digital processing of personally identifiable information in digital files or manuals, as well as personal identification mechanisms based on nominative, personal, and biometric information processed alongside a national ID number.

DEFINITIONS

Definition of Personal Data

The personal data is defined as any information relating to an identified or identifiable natural person. It makes a direct reference to sound and image (Article 1 of the Digital Code).

Definition of Sensitive Personal Data

Pursuant to Article 1 of the Digital Code, the following personal data is considered 'sensitive' and is subject to specific processing conditions: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade union membership; genetic data; and health-related data; data concerning a person's sex life or sexual orientation, prosecution to criminal and administrative penalties.

NATIONAL DATA PROTECTION AUTHORITY

The APDP (The Beninese data protection authority) is the regulator for data in the Republic of Benin. It is an independent and administrative body with a legal personality as it ensures the application of the provisions of the Digital Code and the right to privacy.

The APDP’s powers and responsibilities which include:

- raising public awareness of the risks, rules, and rights surrounding the processing of personal data;
- authorising or denying requests for processing;
- receiving and investigating complaints about the misuse of personal data;
- conducting necessary inspections regarding personal data processing, and obtaining all information and documents needed;

- informing data controllers of alleged violations of the law and issuing mandatory measures for remedying these violations;
- imposing administrative sanctions on data controllers in the case of noncompliance;
- informing the public prosecutor of offenses committed under the law;
- keeping a public register of personal data processing operations;
- issuing public opinions on the state of data protection law;
- proposing amendments to simplify and improve data protection legislation, where necessary; and
- cooperating with international data protection authorities to share information and assistance, as well as participating in international negotiations.

Data controllers are required to file an annual report with the APDP concerning compliance with the processing.

REGISTRATION

The is no country-wide system of registration in the Republic of Benin. However, the law imposes an obligation of notification and requires the controller to keep a register of processing activities carried out under its responsibility.

Pursuant to Article 405 of the Digital Code, Automated or non-automated processing carried out by public or private bodies and involving personal data must, prior to their implementation, be the subject of a prior declaration to the Authority or be entered in a register kept by the person designated for that purpose by the controller.

All processing of personal data is subject to a reporting obligation to the Authority, except for the exemptions provided for in Book V of the Digital Code (see Articles 408, 410, 411, and 417 of the Digital Code).

In terms of Article 435 of the Digital Code, each controller and, where applicable, the controller's representative shall keep a register of the processing activities carried out under their responsibility.

This register shall include all of the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations;
- where applicable, transfers of personal data to a third country or to an international organization, including the identification of that third country or international organization;
- the time limits for the deletion of the different categories of data;
- a general description of technical and organizational security measures.

Each processor and, where applicable, the processor's representative of the processor shall also maintain a record of all categories of processing activities performed on behalf of the controller including:

- the name and contact details of the sub-processor(s) and of each controller on whose behalf the processor is acting and, where applicable, the names and contact details of the controller's or processor's representative and of the data protection officer;
- the categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or to an international organization, including the identification of that third country or international organization and, in the case of transfers, the documents attesting to the existence of appropriate safeguards;
- a general description of the technical and organizational security measures.

The above-mentioned records must be in written form, including electronic form.

The controller or processor and, if applicable, their representative shall make the register available to the Authority upon request.

The obligation to keep a register does not apply to small and medium-sized enterprises except in the following cases:

- if the processing they carry out is likely to involve a risk to the rights and freedoms of the data subjects;
- if it is not occasional or if it concerns in particular the special categories of data referred to in article 394 paragraph 1 of the numerical code, or personal data relating to criminal convictions and offences.

DATA PROTECTION OFFICERS

According to the Article 430 of the Digital Code, a Data Protection Officer (DPO) must be appointed when the data controller is a state-owned organization or when the activities of the data controller or data processor involve monitoring individuals or processing of sensitive data on a large scale.

Although the Digital Code does not impose a strict duty for the appointment of a DPO, organizations with a DPO are exempt from notifying the APDP of data processing (Article 408 of the Digital Code).

COLLECTION & PROCESSING

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 383):

- processed lawfully, fairly and transparently;
- collected for specific, explicit, and legitimate purposes and not subsequently processed in a manner inconsistent with those purposes;
- processed appropriately, in a manner relevant and not excessive with regard to the purposes for which they are collected and processed;
- accurate and, if necessary, updated. All reasonable steps must be taken to ensure that inaccurate or incomplete data is erased or corrected;
- kept in a form that allows the identification of data subjects for a period not exceeding that necessary to achieve the purposes for which they are collected or for which they are processed;
- processed in a manner that ensures appropriate security of personal data

Notwithstanding the above, the overriding principle governing the processing of personal data in Benin is the prior consent of the data subject (see Articles 6 of the Data protection Law and 389 of the Digital Code.)

There are some exceptions to this principle. The prior consent of a data subject is not required when processing the data is meant to:

- comply with a legal obligation to which the controller is subject to;
- perform a task in the public interest or a task falling within the exercise of public authority, which is entrusted to the controller or the third party to whom the data are shared;
- perform a contract to which the data subject is a party or perform pre-contractual measures taken at the request of the data subject;
- protect fundamental interests or rights;
- perform certain activities in the framework of journalism, research or artistic or literary expression in compliance with the ethical rules of these professions.

When the processing is entrusted to a subcontractor, the controller or, where appropriate, his representative in the Republic of Benin, must:

- choose a subcontractor providing sufficient guarantees sufficient guarantees with regard to technical and organizational security and organizational measures relating to the processing;
- conclude a contract with the processor either in writing or via electronic means;
- define among other things the responsibility of the processor with regard to the data controller and their incumbent obligations in the privacy and security of the data

Under the applicable data protection law in Benin, individuals possess the following rights:

- right to obtain all their personal data in a clear format, as well as any available information as to their origin;
- right to withdraw consent for personal data processing at any time;
- the right to object, for lawful reasons, to the processing of their personal data;
- right to oppose the processing of their personal data for marketing purposes;
- right to rectify or erase personal data when it is deemed inaccurate or incomplete;
- right to not be subject to decisions made on the sole basis of an automated processing that would produce significant risks or harm;
- right to be forgotten, or to have information made public about themselves deleted from records; and
- right to obtain damages from data controllers when a breach occurs, leading to a material or non-pecuniary damage to a person.

Right to be informed

Data controllers must provide data subjects with information describing, among other things:

- the processing activities, such as data category;
- the purpose of processing;
- data recipients;
- the existence of profiling activities; and
- identification and contact details of the data controllers, or data subject rights.

Right to access

Any natural person whose personal data is processed may request from the controller information making it possible to know and contest the processing of their personal data, communication in intelligible form of data to personal character that concerns them as well as any available information as to their origin.

Right to rectification

Any natural person may require the data controller to correct, complete, update, block, or delete personal data concerning him, which is inaccurate, incomplete, ambiguous, out of date, or irrelevant, as the case may be, and as soon as possible, or whose collection, use, disclosure, or retention is prohibited. To exercise their right of rectification or deletion, the interested party sends a request, by post or electronically, dated and signed to the controller, or his representative.

Within 45 days following receipt of the request provided for in the previous paragraph, the controller communicates the rectifications or erasures of the data made to the data subject himself as well as to the persons to whom they are inaccurate, incomplete, equivocal, outdated, irrelevant or whose collection, use, communication, or storage is prohibited, have been communicated.

Right to erasure

See section above.

Right to object / opt-out

Any natural person has the right to object, at any time, for legitimate reasons, to the processing of personal data concerning him. It has the right, on the one hand, to be informed before data concerning it is communicated for the first time to third parties or used on behalf of third parties for purposes of prospecting, in particular commercial, charitable or political, and, on the other hand, to be expressly offered the right to oppose, free of charge, said communication or use.

Right to data portability

Data subjects have the right to receive the personal data concerning them that they have provided to a controller, in a structured, commonly used and machine-readable format, and have the right to transmit this data to another controller. processing without the controller to whom the personal data has been communicated obstructing it, when:

- the processing is based on consent or on a contract; and
- the processing is carried out using automated processes.

When the data subject exercises his right to data portability in application of the first paragraph, he has the right to obtain that the personal data are transmitted directly from one controller to another, when this is technically possible.

This right does not apply to processing necessary for the performance of a task of public interest or relating to the exercise of public authority vested in the controller. The right referred to in the first paragraph does not infringe the rights and freedoms of third parties.

TRANSFER

A personal data processor may transfer data to a foreign country if the receiving country ensures an adequate level of protection for the privacy and human rights and freedoms of the persons concerned.

The level of protection will be assessed according to:

- the data protection laws of the recipient country;
- the safety measures; and
- the processing characteristics (end, duration, nature, origin, destination of processed data).

It is worth noting that a country may not provide sufficient data protection, but if a recipient country is not deemed 'safe' in protecting data, but a data transfer is followed by protective measures such as contractual clauses or internal rules, assent could be provided by the APDP.

For instance, some data, such as biometric data, health data, data related to serious infringements, and data regarding crime, will be considered as involving specific risks for human rights and freedom of individuals' data. These data will need to be approved under Article 41 of the Law on the Protection of Personally Identifiable Information.

SECURITY

The Law on the Digital Code adopts a proportionate, context-specific approach to security.

Article 426 of this Law states that in order to guarantee the security of personal data, the controller and / or its processor must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, interception, in particular where the processing involves the transmission of data over a network, and against all other forms of unlawful processing.

These measures must ensure, taking into account the state of the art and the costs associated with their implementation, an appropriate level of security, taking into account, on the one hand, the state of the art in the field and the costs involved in applying these measures and, on the other hand, the nature of the data to be protected and the potential risks.

It is also the responsibility of the data controller, his representative and the sub-processor to ensure compliance with these security measures.

The Law on the Digital Code does require controllers and processors to consider the following when assessing what might constitute adequate security:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

No specific requirements other than those set forth in the Law.

BREACH NOTIFICATION

A data controller must notify the Commissioner of the APDP of any breach to the security safeguards of personal data, without delay (Article 427 of The Law on the Digital Code).

The notification must, at a minimum:

- describe the nature of the security breach that affected personal data including, if possible, the categories and approximate number of individuals affected by the breach and the categories and approximate number of personal data records affected;
- provide the name and contact information of the Data Protection Officer or other point of contact from whom additional information can be obtained;
- describe the likely consequences of the security breach; and
- describe the steps taken or proposed to be taken by the controller to remedy the security breach, including, if applicable, steps to mitigate any adverse consequences.

Mandatory Breach Notification

Please refer to the comments above under Notification.

ENFORCEMENT

The data protection laws empower the authorities 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 Authority may issue a warning to a data controller who fails to comply with the obligations arising from the Digital Code. It may also give formal notice to the data controller to put an end to the non-compliance within a set period of time, which may not exceed eight (08) days.

The following constitute serious infringement of the Digital code:

- unfairly collecting personal data;
- communicating personal data to an unauthorized third party;
- collecting sensitive data, data relating to offences or to a notional identification number, without complying with the legal conditions;
- collect or use personal data in such a way as to cause a serious breach of fundamental rights or of the privacy of the individual concerned;
- prevent the Authority's services from carrying out an on-site inspection, or obstruct such an inspection.

Where the data controller fails to comply with the formal notice, the Authority may impose the following sanctions, in accordance with the principle of adversarial proceedings:

- a pecuniary penalty, except in cases where processing is carried out by the State;
- an injunction to cease processing personal data;
- a final or temporary withdrawal of the authorization granted in application of the provisions of the Digital Code;
- blocking of certain personal data.

The amount of the fine is proportionate to the seriousness of the breaches committed and to the benefits derived from the breach.

For the first breach, it may not exceed XOF fifty million (50,000,000). In the event of repeated breaches within five (05) years of the date on which the penalty previously imposed became final, it may not exceed XOF one hundred million (100,000,000) or, in the case of a company, five percent (5%) of sales excluding tax for the last financial year closed, up to a maximum of XOF one hundred million (100,000,000).

Where the Authority has imposed a fine that has become final before the criminal court has given a final ruling on the same or related facts, the latter may order that the fine be deducted from the fine imposed.

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 245 of the Law No. 2017-20 of April 20, 2018 on the digital code in the Republic of Benin).

Even when a marketer has the consent of a data subject, that consent can be withdrawn by the data subject under Article 334 of the Law No. 2017-20 of April 20, 2018 on the digital code in the Republic of Benin.

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

Not applicable.

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.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.