



## Data protection in Benin

**09 October 2019**

*Africa Law and Business*

Benin has been one of Africa's front-runners when it comes to data protection law. Aissatou Sylla and the Benin data protection authority (APDP), explain the practicalities of the Benin Digital Code.

In 2009, Benin became the seventh African country to enact data protection laws, following the trail of Mauritius, Cape Verde, the Seychelles, Tunisia, Senegal and Morocco. In 2018, whilst 27 countries still did not have privacy laws, Benin revamped its legal framework on data protection as part of larger project, the Benin Digital Code (Le Code numérique du Bénin) which also covers: networks and electronic communication services, e-ID and e-signature, e-commerce, trust services providers, cybercrime. This code is one of the most sophisticated and unified legal frameworks governing technology in Africa.

Technically speaking the new data protection legislation (the Act) is more advanced than the 2009 Data Protection Act in that it provides clearer definitions with examples, exceptions and adjustments to rules where they cannot be implemented or complied with from a practical point of view. The Act also cross-references other parts of the code, such the E-commerce Section with respect to direct marketing.

The digital code was promulgated two years after the entry into force of the 2016 European General Data Protection Regulation (GDPR) and several GDPR principles can be found in the Act, even though most of them were adapted to Benin's requirements.

### **Personal data**

'Personal data' is defined as any information relating to an identified or identifiable natural person. The definition is similar to the GDPR definition and is, as a matter of fact, more detailed as it makes a direct reference to sound and image. The Benin data protection authority, the Autorité de protection des données à caractère personnelles (APDP), formerly known as CNIL, considers that this definition applies to the data of a deceased individual.

'Sensitive personal data' is defined as any data relating to a person's race, health, religious or philosophical, trade union opinions and activities or sexual activities. The APDP considers that

even though bank details do not fall within the definition of sensitive personal data, they should be processed using a similar standard of diligence.

### **Processing and Extra-Territorial Scope**

The definition of 'data processing' is broad and almost identical to the GDPR definition. It covers, for example, data collection, alteration, consultation, erasure and encryption. The Act applies to data controllers located in Benin and the Economic Community of West African States (ECOWAS) region. It also applies to data controllers located outside ECOWAS and those who provide goods and services (even free of charge) to individuals located in Benin or who monitor the behaviour of individuals located in Benin. European and American social media or fintech companies processing the data of individuals located in Benin therefore fall under the scope of Benin data protection law.

### **Legal basis for processing**

As is the case in most African countries with privacy laws, the default legal basis for processing personal data in Benin is the consent of the data subject. An exception is made where the party processing the data is a professional journalist. However, no exceptions are made where the data subject is a public person in a public function (for example, a celebrity walking the red carpet, a politician at a campaign meeting) which can cause practicality issues. The main exceptions to the consent requirement are the performance of a contract, compliance with a legal obligation, permission or obligation by law to process personal data, necessity for public bodies to perform their public duties and protection of fundamental interests or rights.

The absence of the notion of legitimate interest as a legal basis for processing constitutes the main difference with EU law and the law of Benin's neighbour, Nigeria, that provide that personal data can be processed without the data subject's consent, on the basis of the data controller's legitimate interest. The intent is, according to the European Commission, to allow processing of personal data in order to carry out tasks related to business activities when processing is not necessarily justified by a legal obligation or carried out to execute the terms of a contract with an individual.

### **Data protection office and accountability**

The Act introduces governance and accountability obligations inspired by GDPR, such as the obligation for data controllers to hold a record of their processing activities.

In addition, the Act imposes the appointment of a data protection officer (DPO) when the data controller is a state-owned organisation (except judicial bodies) or when the activities of the data controller or data processor involve, on a large scale, people monitoring or processing of sensitive data. The rules regarding the appointment of a DPO are not as strict as GDPR's. However, appointing a DPO could be more appealing in Benin than in the EU because, under the Act, organisations with a DPO are exempt from notifying the APDP of data their processing activities.

## Data subjects' rights

Data controllers must provide the data subjects with information describing the processing activities, such as data category, purpose of processing, data recipients, the existence of profiling activities, identification and contact details of the data controllers, or data subject rights.

The key data subject rights are the right to rectify, erase, update the data, the right to be forgotten, the right to access the data processed by the data controller, the right to object and to withdraw consent to processing.

The Act is more detailed than GDPR with respect to the timeframes within which data controllers must comply with their obligations.

The Act and the whole digital code show a significant effort by the Benin government to create a technology and privacy legal framework which is compatible with the international requirements and which, at the same time, is capable of being complied with given the economic and infrastructural reality of the country, especially with regard to small-to-medium enterprises.

*For a look at the data protection law in Uganda, [click here](#).*

*Aissatou Sylla is a senior associate specialising in technology, media and telecommunications in the Paris office of Hogan Lovells.*

*Etienne-Marie Fifatin is chairman and Marieannick Ouendo is head of legal and litigation of the Autorité de protection des données à caractère personnelles (APDP) in Benin.*

***First published in Africa Law and Business.***

## Contacts



**Aissatou  
Sylla**

Senior  
Associate

> [Read the full article online](#)