1. BENIN

Regional Economic Community: Economic Community of West African States (ECOWAS)
Population: 11 801 595
Internet Penetration: 3 801 758 users i.e. 32.2% of the population.
AUCC Ratification Status: Signed 28/01/2015

1.1. OVERVIEW

DATA PROTECTION: Benin has a data protection law (Book Five of the Digital Code). Benin has a policy strategy acknowledging data protection as a strategic objective. Benin has a data protection authority (APDP).

ELECTRONIC TRANSACTIONS: Benin has an electronic transactions law (Book Two and Four of the Digital Code). Benin has a policy strategy acknowledging electronic commerce and secure electronic transactions as a strategic objective. Benin has a National Signing Certification Authority.

CYBERCRIME AND CYBERSECURITY: Benin has a cybercrime law (Book Six of the Digital Code). Benin does not have an implemented National Cybersecurity Strategy – it is still in development. Benin has a national cybersecurity incident response team (bJC-SIRT).

1.2. DATA PROTECTION

1.2.1. Overview of Data Protection Legislation

The primary legal instrument concerning data protection in Benin is Book Five of the Digital Code (Loi n° 2017/20 portant Code du Numérique en République du Bénin) ("the Code").

The Code

The data protection provisions of the Code supersede Benin’s prior data protection law from 2009. Book Five of the Code relates to data protection and privacy. The Code, insofar as data protection and privacy is concerned, is discussed more fully below.

- The Code establishes the Personal Data Protection Authority ("APDP") as the Republic of Benin’s national data protection authority. In terms of Book Five of the Code, the Data Protection Officer, selected by the APDP, is obligated to perform certain duties and powers specified in Articles 431 – 432.

- When processing personal data, the basic principles are set out under Title II of Book Five (specifically under Articles 383 - 389). Some of these principles require that:
  - The processing of personal data must be done in a lawful, loyal, transparent and not fraudulent manner (Article 383).
  - The collection of personal data can only be carried out for a specified, explicitly consented and legitimate purposes (Article 384);
  - Personal data must be treated as confidential to the extent necessary to perform the purposes for which it was collected (Article 385); and
  - Data Controllers must ensure that they adhere to a set of obligatory responsibilities (Article 387).

- Article 381 sets out the territorial scope of the Code. Thereunder, it is stated that the Code applies to data controllers located in Benin and the Economic Community of West African States (ECOWAS) region. The Code also has jurisdictional application to data controllers located outside of the 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.

- Cross-border transfers are set out between Articles 391 – 392. The general principles for cross-border transfers are set out under Article 391, whilst derogations for cross-border transfers to Third Countries are contained within Article 392.

- Article 394 addresses the processing of ‘special/sensitive’ data. ‘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 (Sylla, 2019).

- Data subject rights are set out in Articles 437 – 441, including rights: of access; the right to information; the right to object; the right to rectification/erasure; and the right to data portability, respectively.

- A right to be forgotten in the case of publicly facing data is provided for under Article 433;

- Article 429 sets out the instances wherein prior consultation with the data protection authority will be required; and
1.2.2. Data Protection Policy Developments

The Strategic Orientations in The Digital Economy Sector, 2021 considers data protection as a key strategic objective.

1.2.3. Data Protection Institutional Measures

The primary institutions relating to data protection in Benin are:

- The Ministry of Digital and Digitisation.
- The Autorité de Protection des Données à caractère Personnel (APDP); the Personal Data Protection Authority (APDP) is responsible for ensuring that information technologies are at the service of the citizen and that they do not affect human identity, human rights, privacy, individual or public liberties. As an independent administrative authority, it carries out its missions in accordance with the provisions of the Digital Code. The APDP is a completely independent institution; and

1.3. CYBERCRIME AND CYBERSECURITY

1.3.1. Overview of Cybercrime and Cybersecurity Legislation

The primary legal instrument concerning cybercrime and cybersecurity in Benin is Book Six of the Digital Code (Loi n° 2017/20 portant Code du Numérique en République du Bénin) ("the Code").

The Code reinforces existing legislation (such as the Penal Code) and replaces the previous cyber-related law on "the fight against corruption and other similar infringements in the Republic of Benin", passed by the Beninese legislature on 30 August 2011.

Book 6 of the Code provides for both substantive criminal law and provisions relating to procedural law in respect of cybercrime and cybersecurity. The prominent provisions thereof are detailed below:

- Article 618 of the Digital Code creates a specialised Office for the fight against Cybercrime, the Office Central de Répression de la Cybercriminalité (OCRC) and describes the mechanisms of international cooperation (Article 624). The specialised Office oversees investigating of cybercrime cases and promoting awareness-raising activities at the national level. Specifically, the OCRC is tasked under Book Six (Article 494 read in conjunction with Article 608) to contend with the criminalisation of cybercrimes by adapting certain offences/sanctions to Information and Communication systems.

- Chapter I lays out general principles relating to the fight against cybercrime and includes provisions on the guarantee of fundamental rights and freedoms (Article 493) and liability of legal persons (Article 494).

- Chapter II sets out responsibilities of 'operators on the internet', including liability for internet service providers (Article 497) and the requirement to cooperate in the fight against cybercrime (Article 500).

- Chapter III lays out various cyber offences, including:
  - Article 507: Illegal access and maintenance;
  - Article 508: Infringement of computer data;
  - Article 509: Impairment of the integrity of the system;
  - Article 510: Infringement of data integrity;
  - Article 511: Abuse of devices;
  - Article 512: Computer forgery;
  - Article 513: Computer Fraud;
  - Article 514: Sending Unsolicited Messages;
  - Article 515: Deception;
  - Article 516: Embezzlement; and
  - Article 517: Unauthorised Treatment.

- Chapter IV is dedicated to offences relating to minors;
- Chapter IV, Section 3 is dedicated to bank related fraud;
- Chapter VII sets out various offences relating to property rights (including intellectual property); and
- Chapter X is dedicated to common law offences that are committed in the cyber realm.

The Digital Code also indirectly addresses infrastructure concerns in Chapter VIII of Book Six (Article 598 - 603) as it obligates security precautions such as vulnerability tests and installation of detection event issued by the Ministry in charge electronic communications. Significantly, Article 494 imposes relatively hefty sanctions on those who breach the provisions of the code. However, there are no provisions in the Code directly providing for the protection of critical infrastructure systems in Benin.

Decree on International Co-operation

In 2009 the Beninese government, through the Secretariat of the Interior, drafted Decree No. 200/MISP/DC/SGM/DGOPN/SERCT/DER/SA related to the creation of a division in charge of the fight against internet crime. This decree stipulates that victims of internet crime can approach Interpol or the Financial and Economic Brigade (BEF) with their complaints.
1.3.2. Cybercrime and Cybersecurity Policy Developments

There is no primary policy instrument relating to cybercrime and cybersecurity in Benin. However, the National Cybersecurity Strategy of Benin is in the process of development.

According to an African Union and Symantec Report, the Cybersecurity Strategy of Benin will aim to establish trust in Benin’s digital infrastructure and will have two primary objectives (African Union, Symantec, 2016):

- (1) To reduce cyber-crime nationally, and
- (2) To ensure effective cybersecurity for national ICT infrastructure and including critical infrastructure in Benin.

According to the same Report, the “Government of Benin has taken substantial steps in the development and execution of their Cyber Strategy”. On a similar note, in April 2019 the National Agency for Security Information Systems (ANSSI) organized an exchange workshop with key cyber stakeholders in Benin and experts from the International Telecommunications Union (ISOC Benin, 2019). Part of the Workshop was dedicated to “identifying and prioritizing threats, objectives, opportunities and strategic directions for the development of the national strategy” (ISOC Benin, 2019).

The African Union Symantec Report goes on to indicate that Benin has made various efforts to increase cybersecurity awareness through Benin the country:

- “The Government of Benin launched a cyber security campaign focused on the country’s youth – known as the Internet of Sensitization to Youth”;
- “The Government of Benin works with various Non-Governmental Organizations (NGOs) and civil society organizations in order to increase overall cyber security awareness.”
- “The Government of Benin are also beginning to work with the private sector through informal partnerships and recognize that cyber security requires both national and international cooperation.”
- “The Government of Benin also takes part in a number of Confidence Building Measures (CBM) through international meetings and cooperates in international cybersecurity measures through exchanges with other countries, such as the recent meetings on West African Cyber security held in Dakar, Senegal.”

1.3.3. Cybercrime and Cybersecurity Institutional Measures

The primary institutions relating to cybercrime and cybersecurity in Benin are:

- The bjCSIRT: the Benin Computer Security Incident Response Team is the first point of contact for government institutions in the Republic of Benin in the event of a computer security incident. The bjCSIRT has national stature and legal standing (bjCSIRT, 2019). The bjCSIRT has been operational since September 2017.
- The National Information Systems Security Agency (“ANSSI”): Article 606 of the Code lists the mission of the Agency which broadly includes information and cyber security roles in both public and private spheres.

1.4. ELECTRONIC TRANSACTIONS

1.4.1. Overview of Electronic Transactions Legislation


Electronic transactions provisions (in the context of electronic commerce) in the Republic of Benin are divided across three (3) Books in the Digital Code:

- Book Two governs ‘electronic writing’ (Title I) and ‘electronic signatures’ (Title III); and
- Book Four governs ‘electronic commerce’ including: electronic contracts (Title I and Title III) and advertising by electronic means (Title II).

Significant provisions arising from Book Two are laid out below:

- Electronic writing is given legal validity under Article 266;
- Electronic signatures are regulated under Title III, including provisions on qualified electronic signatures (Article 287) and qualified validation services electronic signatures (Article 291); and
- Article 317 establishes the supervisory body responsible for regulating established and trusted trust service providers in Benin. The supervisory body is attached to the Ministry of Communications. An Order by the Minister of Electronic Communications will organise and operationalise the Supervisory body.
Significant provisions arising from Book Four are laid out below:

- Article 329 provides for contractual liability in the case of electronic transactions;
- Title II (Chapters 1-2) regulate electronic advertising;
- Title III regulates electronic contracts, laying out detailed requirements and conditions for the contractual engagements between online service providers/sellers and consumers;
- Title IV regulates the liability of suppliers of goods and online services.

**United Nations Convention on the Use of Electronic Communications in International Contracts, 2005**

In November 2019, Benin acceded to the United Nations Convention on the Use of Electronic Communications in International Contracts (2005) - also known as the "Electronic Communications Convention" (UNIS, 2019). The Convention will become binding on Benin on 1 June 2020 (UNIS, 2019). The Electronic Communications Convention “aims to enhance legal certainty and commercial predictability when electronic communications are used in international contracts. It also provides the criteria to be used to establish the functional equivalence between electronic communications and paper documents - including “original” documents - as well as between electronic authentication methods and handwritten signatures.” (UNIS, 2019).

**1.4.2. Electronic Transactions Policy**

**Developments**

The primary policy document relating to electronic transactions in Benin is the Strategic Orientations in The Digital Economy Sector, 2021. Project 4 thereunder considers the generalisation of the use of electronic commerce. Quoting from the strategy:

“[The] [d]evelopment and generalization electronic commerce and mobile commerce constitutes an axis major economic stimulus and financial inclusion. The launch of this flagship project will require the implementation of the levers legal, fiscal and operational to generalize the use of e-commerce.” (Agence du Numérique, 2019).

Further, Benin’s Ministry of Digital and Digitalization, the Ministry of Industry and Trade co-organised a Workshop with the United Nations Conference on Trade and Development (UNCTAD) in October 2019 to assess Benin’s readiness for electronic commerce. The Workshop aimed to clarify Benin’s capabilities in electronic commerce and enable it to formulate a strategy to overcome obstacles to its development (Ministère du Numérique et de la Digitalisation, 2019). According to the Ministry of Digital and Digitalisation, Benin has an aim to “use Information and Communication Technologies (ICT) as a catalyst for Benin’s economic dynamism and modernization for Europe. acceleration of economic growth and social inclusion by 2021” (Ministère du Numérique et de la Digitalisation, 2019).

**1.4.3. Electronic Transactions Institutional Measures**

The primary institutional measures in Benin relating to electronic transactions are:

- The Ministry of Digital Economy of Benin;
- The Ministry of Digital and Digitalization;
- The Ministry of Communications; and
- The National Signing Certification Authority (L’autorité de certification signataire nationale).
1.5. COMPARISON WITH THE AUCC PROVISIONS ON LAWS, POLICIES AND INSTITUTIONS FOR DATA PROTECTION, CYBERCRIME AND ELECTRONIC TRANSACTIONS.

<table>
<thead>
<tr>
<th>Policy and Governance Measures</th>
<th>Legislative and Regulatory Measures</th>
<th>Institutional Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Policy which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures</td>
<td>Data Protection Laws and Regulations</td>
<td>Data Protection Authority whose responsibilities in regulating data protection include: authorisation of data processing, authorisation of cross border transfers of personal data</td>
</tr>
<tr>
<td>National Cybersecurity strategy to implement the Policy</td>
<td>Electronic Commerce Laws and Regulations</td>
<td>Electronic Signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications</td>
</tr>
<tr>
<td>A Cybersecurity Strategy is under development.</td>
<td>The Digital Code (Book 2 and 4).</td>
<td>National Signing Certification Authority (L’autorité de certification signataire nationale).</td>
</tr>
<tr>
<td>Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture</td>
<td>Cybercrime Laws and Regulations</td>
<td>State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;</td>
</tr>
<tr>
<td>Benin has engaged in various public-private partnerships to enhance cybersecurity awareness.</td>
<td>The Digital Code (Book 6).</td>
<td>The Ministry of Digital and Digitalization</td>
</tr>
<tr>
<td></td>
<td>Legislative and regulatory measures to identify the sectors regarded as sensitive for their national security and well-being of the economy (critical infrastructure), and measures to improve vigilance, security and management in such sectors</td>
<td>State Department to regulate vulnerability and safety guarantee assessments of ICT product vendors including ensuring mandatory disclosures of vulnerabilities and the solutions to such vendors consumers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Institutions with the statutory authority and legal capacity to respond to cyber security incidents, co-ordination and co-operation for (cybersecurity) restorative justice, forensic investigations, cybersecurity prosecution</td>
</tr>
<tr>
<td></td>
<td></td>
<td>National Agency for Security Information Systems (ANSSI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The bjCSIRT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The bjCSIRT</td>
</tr>
</tbody>
</table>
Disclaimer

This report was prepared independently by EndCode.

This report is based on a variety of inputs from multiple sources including official and private data sources such as public and governmental institutions, international organisations, academic research, news articles, sector reports and interviews with various stakeholders.

Accuracy of analysis and recommendations provided are dependent on the detail and accuracy of available and declared data. The information given herein is for informal guidance only and neither AUDA-NEPAD nor EndCode, nor any company or organisation stated within this paper makes any expressed or implied warranty, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, or process disclosed.

AUDA-NEPAD nor EndCode bear no responsibility for any use that may be made of this report. Should you have any queries about the content within this report, please contact AUDA-NEPAD.

About EndCode

EndCode is a specialist advisory firm - servicing local, regional and international organisations navigating technology laws and policies in Africa. EndCode believes that it can promote access to the benefits of technology and innovation on the continent by growing the body of insights available in technology law and policy areas. EndCode is distinguished by its multidisciplinary expertise in law, policy, research and advocacy in the technology environment.