CYBERSECURITY ASSESSMENT REPORT
REPUBLIC OF CONGO
3. REPUBLIC OF CONGO

3.1. OVERVIEW

DATA PROTECTION: The Republic of Congo has a data protection law (29/2019). The Congo Digital Strategy 2025 envisions privacy protection guarantees. Whilst Law 29/2019 requires the establishment of a data protection authority, this has yet to be accomplished.

ELECTRONIC TRANSCTIONS: The Republic of Congo does not have an active electronic transactions law. It has, however, drafted its Electronic Transactions Bill, 2018. The Republic of Congo is also subscribed to the OHADA Uniform Law, 2010 which validates electronic transactions in the Republic. The Congo Digital Strategy 2025 makes provision for e-commerce. The Guichet Unique Des Operations Transfrontalieres (GUOT) is the root Certification Authority in Congo responsible for all electronic transaction related activities.

CYBERCRIME AND CYBERSECURITY: The Republic of Congo has draft laws on Cybersecurity and Cybercrime. The Republic of Congo does not have a National Cybersecurity Strategy. The Republic of Congo has a National Agency of Information Security but has yet to establish a CERT.

3.2. DATA PROTECTION

3.2.1. Overview of Data Protection Legislation

The primary legal instrument relating to data protection in the Republic of Congo is Law No 29/2019 of 13 August 2019 concerning the Protection of Personal Data ("Law 29/2019").

Law 29/2019 forms part of the Legal Framework for Cyberspace, Security and the Protection of Personal Data. Previously, the right to privacy was only addressed by the Constitution and The Framework Law 013/2002 on Telecommunications.

Law No 29/2019

Significant provisions under Law 29/2019 include:

- Chapter 2, dealing with the general principles governing the processing of general and specific categories of personal data;
- Article 5, denoting the basic principles governing the processing of all personal data;
- Article 14, providing that the collection and processing of personal data relating to ethnic and geographic origin, religious and philosophical convictions, political affiliation, trade union membership, genetic data and medical history is prohibited;
- Article 15, listing exemptions and authorisations for the processing of personal data;
- Articles 26 to 30, relating to open access and interconnection of personal data;
- Article 40, requiring the establishment of a National Personal Data Protection Commission;
- Article 46, entranching the data subject’s right to information, and Articles 50 and 59 providing for the data subjects right of access and right to object respectively;
- Article 63, imposing confidentiality obligations on personal data controllers;
- Article 64, concerning the security obligations of personal data controllers; and
- Articles 65 and 66, covering the storage and sustainability obligations on data controllers.

Law No. 29/2019 is, however, not in force yet. Law 29/2019 has been criticised for being outdated and in need of an update.

Draft Law on Fighting Cybercrime

Chapter 6 of the Draft Law on Fighting Cybercrime creates offences for unlawful processing of personal data between Articles 11 – 23. Chapter 8 also lists special measures concerning the protection of personal data (orders of judges).

3.2.2. Data Protection Policy Developments

The Republic of Congo does not have a dedicated data protection policy. However, the Congo Digital Strategy 2025 envisions data protection guarantees (Ecofin Agency, 2019). The strategy was published via Decree N/2019/150 of June 17th, 2019. The Strategy was officially presented in Brazzaville on August 9, 2019 by the Director-General of the Development of the Digital Economy (DGDE) under the Ministry of Posts, Telecommunications and the Digital Economy (Djoyum, 2019).
3.2.3. Data Protection Institutional Measures

The primary institutional measures relating to data protection and privacy in the Republic of Congo are:

- The Ministry of Posts, Telecommunications and the Digital Economy; and
- The National Personal Data Protection Commission.

3.3. CYBERCRIME AND CYBERSECURITY

3.3.1. Overview of Cybercrime and Cybersecurity Legislation

The primary legal instruments relating to cybercrime and cybersecurity in the Republic of Congo are:

- The Draft Law on Cybersecurity;
- The Draft Law on Fighting Cybercrime; and

Both draft laws have been positively voted for in the National Assembly but are yet to be promulgated.

Draft Law on Cybersecurity

The Draft Cybersecurity Law (the “Cybersecurity Bill”) identifies the risks facing the use of new information technologies. Article 1 of the Cybersecurity Bill sets out its objectives to:

- organize and reinvigorate the computer security needed to strengthen the confidence of citizens, businesses and public authorities in information and communication technologies;
- set the general rules for the protection of computer systems and electronic communications networks; and
- define the rules applicable to the means, methods and systems of cryptography and repress the related offences.

Important provisions from the Cybersecurity Bill are set out below:

- Chapter 3 of Title I sets out the general principles of cyber-security;
- Title II sets out provisions relating to activities to be conducted by owners of information systems and electronic communication networks. These activities include mandatory audits, ‘listening’, disturbance reporting, protection of electronic communication networks and the protection of information systems; and
- Title III regulates cryptology in the Republic of Congo:
  - Chapter 1 sets out the legal regimes of means and services of cryptology.
  - Chapter 2 regulates organisations who perform cryptology services. Thereunder, Article 34 requires that organisations performing cryptology be approved by the National Information Systems Security Agency.
  - Chapter 3 sets out the responsibility of cryptology service providers. Penal Sanctions are provided for in Chapter 5.

Draft Law on Fighting Cybercrime

The Draft Law on Fighting Cybercrime (the “Cybercrime Bill”) deals with the fight against cybercrime. Considering the lack of criminal legislation in the field of digital crime, the Congolese government intends to add offences committed through information communication technologies and adapt traditional offences to those committed using information communication technologies. Chapter 20 (Title II) of the Cybercrime Bill creates criminal liability for committing any offence laid out under the Bill.

Title II of the Bill contains numerous Chapters on various cyber offences. These include:

- Infringements of the confidentiality of information systems;
- Attacks on the integrity of information systems;
- Fraudulent introduction of data into an information system;
- Fraudulent interception of data from an information system;
- Damages to the integrity of data in an information system;
- Offences relating to personal data;
- Abuse of Devices and the Association with Computer Criminals;
- Child pornography;
- Xenophobia through an information system;
- Offences related to the activities of electronic communication service providers;
- Offences Relating to Electronic Advertising;
- Offences related to direct prospecting;
- Offences relating to cryptology;
- Offences committed by any means of public dissemination;
- Digital Identity Theft;
- Denial of assistance; and
- Attacks on National Defence.

Chapter 14 of Title II adapts property offences to information and communication technologies, whilst Chapter 16 of Title II provides for cyber infringements on Copyright and Neighbouring Rights. Chapter 21 adapts certain sanctions to information and communication technologies.
Title IV relates to international judicial cooperation and assistance. Article 104 states that “the procedures for establishing cooperation agreements on cybersecurity and the fight against cybercrime shall be determined by regulation”, whilst Articles 105 - 106 detail the procedures for mutual legal assistance between the Republic of Congo and foreign judicial authorities.

**Law 30/2019**

Law No. 30/2019 of 10 October 2019 forms part of the Legal Framework for Cyberspace, Security and the Protection of Personal Data and serves the sole function of establishing and regulating the National Information Systems Security Agency. Thereunder:

- Articles 1 and 2 provide for the establishment of the National Information Systems Security Agency and vest it with legal authority;
- Article 3 sets out the Agency’s duties and obligations;
- Article 4 delineates its powers which include the power to apply sanctions and penalties for infractions;
- Article 5 makes provision for funding of the Agency; and
- Article provides that the Agency should be led by a Director-General appointed by Ministerial decree.

### 3.3.2. Cybercrime and Cybersecurity Policy Developments

Currently, the Republic of Congo does not have a National Cybersecurity Strategy. However, the government of the Republic of Congo plans to adopt a National Cybersecurity Strategy after the promulgation of the draft cyberlaw and draft cybersecurity law. The government has furthermore noted that cybersecurity awareness training is a priority (Poaty, 2019).

In establishing its National Cybersecurity Agency, the Republic of Congo will be training its police force on cybersecurity and cybercrime.

### 3.3.3. Cybercrime and Cybersecurity Institutional Measures

The primary institutions relating to cybercrime and cybersecurity in the Republic of Congo are:

- The Ministry of the Interior who oversees cybersecurity issues; and
- A special branch within the National Police tasked with investigating cybercrimes and enforces crime laws.
- Centre for Computing and of Research of the Army and of Security (CIRAS) – the Institution researching cybersecurity and national defence under the Presidency;
- The National Intelligence Agency; and

Congo has not established a national cybersecurity emergency response team (CERT) as of writing.

### 3.4. Electronic Transactions

#### 3.4.1. Overview of Electronic Transactions Legislation

The primary legal instruments governing electronic transactions and commerce in the Republic of Congo is the Electronic Transactions Bill, 2018.

**The Electronic Transactions Bill, 2018**

In August 2019 the lower house of the Parliament of the Republic of Congo adopted the draft law on Electronic Transactions. It was initiated by the Minister of Posts, Telecommunications and the Digital Economy (Bombo, 2019).

**OHADA Uniform Law, 2010**

The Organization for Harmonization of Business Law (OHADA) is the French Commercial Law common to all Francophone countries and serves as the country's commercial law - subject to specific Congolese laws. The Republic of Congo has ratified OHADA Treaty of October 17, 1993 on May 28, 1997. Insofar as electronic commerce/transactions are concerned, the Republic of Congo relies on the 2010 revised OHADA Uniform Law on General Commercial Law which became effective in Member States in 2011.

Under the 2010 revised OHADA Uniform Law on General Commercial Law, Book V contains Chapters pertaining to the 'Computerization Of The Register Of Commerce And Securities, The National And Regional Registries'. These Chapters include provisions on general principles for use of electronic procedures; the validity of electronic documents and electronic signatures; use and conservation of electronic documents; use of electronic means for the transmission of documents; and publicity and electronic dissemination of registers information.
Important provisions stemming from the Chapter on the validity of electronic documents include:

- Article 82 recognising the legal equivalence between electronic documents, electronic transmissions and paper documents - when such transmissions are established and kept in a reliable technique and which guarantee, at any time, the origin of the electronic document and its integrity during electronic processing and transmissions;

- Article 83 providing that electronic authentication and electronic signatures are given legal validity and may be lawfully utilised to identify a person/s. Article 83 also makes provision for the formation of electronic contracts consisting of intentions and obligations – providing for contractual liability for providers of goods or services by electronic means; and

- Article 84 regulates the use of electronic certificates to link signature-verification data to a person and confirm the identity of such persons. Article 84 also sets out the particulars that must be contained within an electronic certificate.

3.4.2. Electronic Transactions Policy Developments

The primary strategy/policy relating to electronic transactions and electronic commerce in the Republic of Congo is the Congo Digital Strategy 2025. The strategy was published via Decree 2019/150 of June 17th, 2019. The Strategy was officially presented in Brazzaville on August 9, 2019 by the Director-General of the Development of the Digital Economy (DGDEN) under the Ministry of Posts, Telecommunications and the Digital Economy.

The core pillars of the strategy are e-Citizen; e-Government and e-Commerce with precise axes. The goal of Congo Digital 2025 is to "build Congo into a true information and knowledge society".

In an effort to increase financial inclusion and bolster the use of mobile money, Terra Pay was presented to the Minister in charge of the digital economy Léon Juste Ibonbo on September 18, 2019. Terra Pay, which will be deployed in Congo, will unite telephone operators as well as banks and micro-finance by freely circulating money electronically between mobile money accounts from one operator to another across the country (Bombo, 2019).

3.4.3. Electronic Transactions Institutional Measures

The core institutions relating to electronic transactions in the Republic of Congo are:

- Ministry of Posts and Electronic Communications;

- The Regulatory Agency for Post and Electronic Communications of the Republic of Congo (ARPCE). The ARPCE was established by Law n° 11/2009 of 25 November 2009. ARPCE is an administrative public institution, with legal personality and financial autonomy. The ARPCE is the Congolese Authority for control, monitoring and regulation of the Posts and Electronic Communications sectors;

- The Autorité De Certification Des Echanges Electroniques Au Congo - The Guichet Unique Des Operations Transfrontalières (GUOT). The GUOT is the root Certification Authority in Congo, empowered by Decree 596 of November 03, 2014. The GUOT is responsible for ensuring, on behalf of the Republic of Congo, the regulation, control and monitoring of all activities related to electronic certification, as described in the aforesaid Decree (GUOT, 2019); and

- Under the leadership of ARPCE, an association called the Congolese branch of Congo Internet naming (ACNIC), was established on June 9, 2011. The new structure is responsible for managing the Internet domain naming of Congo.
### 3.5. 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><strong>Cybersecurity Policy</strong> which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures</td>
<td><strong>Data Protection Laws and Regulations</strong>&lt;br&gt;Data protection Law No 29/2019&lt;br&gt;Electronic Commerce Laws and Regulations&lt;br&gt;Draft law on Electronic Transactions</td>
<td><strong>Data Protection Authority</strong> whose responsibilities in regulating data protection include authorisation of data processing, authorisation of cross border transfers of personal data&lt;br&gt;National Personal Data Protection Commission.</td>
</tr>
<tr>
<td><strong>National Cybersecurity strategy to implement the Policy</strong></td>
<td><strong>Cybercrime Laws and Regulations</strong>&lt;br&gt;The Draft Law on Cybersecurity; The Draft Law on Cybercrime; and Law 30/2019 establishing the National Agency of Information Security.</td>
<td><strong>Electronic Signature Accreditation Authority</strong> that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications&lt;br&gt;Autorite De Certification Des Echanges Electroniques Au Congo.</td>
</tr>
<tr>
<td><strong>Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture</strong></td>
<td><strong>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</strong>&lt;br&gt;State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;&lt;br&gt;The State Department should regulate vulnerability and security assessments of suppliers of ICT products, including ensuring mandatory disclosure of vulnerabilities and solutions to these suppliers</td>
<td><strong>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</strong>&lt;br&gt;National Information Systems Security Agency - a special branch within the National Police tasked with investigating cybercrimes and enforces crime laws.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.</strong>&lt;br&gt;The National State Security Agency.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</strong>&lt;br&gt;National Cybersecurity Agency of the Republic of Congo; Centre for Computing and of Research of the Army and of Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>(No CERT)</strong></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.