2. CHAD

Regional Economic Community: Economic Community of Central African States (ECCAS)
Population: 15,814,345
Internet Penetration: 1,027,932 users i.e. 6.5% of the population.
AUCC Ratification Status: Signed 14/06/2015

2.1. OVERVIEW

DATA PROTECTION: Chad has a data protection law (007/2015). Chad has also acceded to the AUCC. Chad does not have a national policy concerning data protection. Chad does not have an operational data protection authority.

ELECTRONIC TRANSACTIONS: Chad has an electronic transactions law (08/2015). Chad also subscribes to the OHADA Uniform Law, 2010 which validates electronic transactions in the Republic. Chad does not have a policy or strategy concerning electronic transactions/commerce. The National Agency of IT Security and Electronic Certification is responsible for electronic transactions in Chad.

CYBERCRIME AND CYBERSECURITY: Chad has a cybercrime and cybersecurity law (009/2015). Chad does not have an official National Cybersecurity Strategy. Chad does not have an official CERT, however, it operates an anti-cybercrime unit under the ANSICE.

2.2. DATA PROTECTION

2.2.1. Overview of Data Protection Legislation

The primary law relating to data protection in Chad is Law No. 007/PR/2015 of 10 February 2015 (“Law 007/2015”) on the Protection of Personal Data.

Law 007/2015

Law 007/2015 aims to provide for the protection of private and professional life following the collection, processing, transmission, storage and use of personal data (Mwamba, 2016).

Article 5 of Law 007/2015 establishes a public supervisory authority - the National Agency for Computer Security and Electronic Certification “ANSICE”. Law 007/2015 provides for the establishment of alert systems, a code of conduct, sanctions and remedies established by the National Agency for Computer Security and Electronic Certification (ANSICE).

Articles 6, 7 and 8 of Law 007/2015 bestow upon ANSICE the responsibility for personal data protection in Chad. The ANSICE must be consulted for an opinion regarding any legislative or regulatory act concerning the protection of personal data. The ANSICE can issue warnings against data controllers for failure to comply with their obligations under Law 007/2015. The ANSICE can also issue formal notices with several penalties (interruption of processing locking of certain personal data processed).

Law 007/2015 provides several safeguards to prevent attacks on individual and private freedoms. Under Title III of Law 007/2015, data subjects have the following rights:

- The right to information – Articles 35 – 37;
- The right of access - Articles 38 - 44;
- The right to object - Article 45;
- The right of rectification/erasure - Article 46 and 47; and
- The right of recourse – Chapter IV.

Title V sets out the statutory obligations on data controller/processors. These include:

- Articles 59 - 62 impose confidentiality and security obligations; and
- Storage and sustainability obligations on Personal Data Controllers are legislated under Articles 63-64.

Other significant provisions of Law 007/2015 include:

- Title II contains the basic principles governing the processing of personal data;
- Formalities for declarations and authorisations – Articles 54 – 58;
- Specific principles governing the processing of Special/ Sensitive data - Articles 16 to 22; and
- Open access/interconnection of Personal Data files and the storage and transmission of data – Chapter VIII.

Chapter VII of Law 007/2015 restricts cross-border transfers of personal information. Cross-Border Transfers Personal information may not be transferred to a country outside the Central African Economic and Monetary Community (CEMAC) and the Economic Community of Central African States (CEEAC) unless that country ensures an adequate level of data protection. Derogations do, however, exist for instances where the receiving country is not considered adequate. In such cases, data subjects must consent to the transfer or another exemption, such as contractual necessity, must apply.
2.2.2. Data Protection Policy Developments

Whilst Chad’s Law No. 12/PR/2014 provides for the formation of a National ICT strategy, to-date, a strategy has not yet been put in place.

2.2.3. Data Protection Institutional Measures

The primary institutional measures relating to data protection in Chad are:

- The Ministry of Posts and New Information and Communication Technologies: responsible for developing and implementing policies as well as maintaining a regulatory framework in the telecommunication, information technology, and postal sectors in the Chad;

- The Directorate for the Protection of Privacy and Freedoms in the Cyberspaces under the ANSICE (ANSICE, 2019). The Directorate is responsible for:
  - Protecting the privacy of citizens;
  - Ensuring the right to forget is protected; and
  - Popularising the culture of protection of personal data.

- The ICT Development Agency (ADETIC): responsible for developing and monitoring the implementation of the national ICT development strategy.

2.3. CYBERCRIME AND CYBERSECURITY

2.3.1. Overview of Cybercrime and Cybersecurity Legislation

The primary laws relating to cybercrime and cybersecurity in Chad are:

- Law 009/PR/2015 on Cyber Security and the Fight against Cybercrime – adopted by Parliament on 16 December 2014; and


Law 009/PR/2015

The Law 009/PR/2015 governs the security framework for electronic information services, electronic communications services and networks, as well as to define and repress offences related to the use of information and communication technologies. Significant provisions are listed hereunder.

Articles 66-68 address the confidentiality and integrity of computer systems;

Article 69 deals with the fraudulent introduction of data into a system;

Articles 70-76 highlights falsification and use of forged data;

Article 77 regulating the abuse of devices. In terms of national security; and

Article 105 addresses attacks on national defence.

Law 009/PR/2015 set out these offences related to the new information and communication technology are punishable by imprisonment from one (01) year to five (05) years and a fine of one (01) million to ten (10) million francs, or only one of these two penalties.

Anyone who intentionally commits such offences with no lawful excuse or justification will be behind bars. Among these penalties, property offences are characterized as aggravated offences whose sentences are increased to a greater degree.

An aggravated offence is punishable by imprisonment of five (05) years to ten (10) years and a fine of (10) to fifty (50) million francs, or one of these two punishments only, the act for any person who, either by making use of false names or false qualities, or by employing any fraudulent manoeuvres, has been given or delivered, or attempted to be handed over or to deliver funds, furniture or bonds, notes, promises, landfill receipts through a computer system or an electronic communications network and will, by any means, have defrauded or attempted to defraud part or all of the assets of others. Prosecution of perpetrators of cybercrime offences is facilitated by judicial police officers and authorized agents of ANSICE.

Law 14/PR/2014

Law 14/PR/2014 regarding electronic communications provides, in Chapter VII, criminal law provisions in cases of computer crime.
2.3.2. Cybercrime and Cybersecurity Policy Developments

Chadian authorities have been cited as indicating that cybersecurity development in the country is in its infancy (African Union, Symantec, 2016). In this regard, there is no officially recognised National Cybersecurity Strategy in Chad as of writing. There have, however, been in-country notifications that a National Cybersecurity Strategy is in draft.

Despite Chad not operating an official CERT, according to a 2019 ANSICE presentation, under the body of ANSICE there is “an anti-cybercrime unit, under the supervision of the Security Directorate of Electronic Communications Networks and Information Systems” (translated) (ANSICE, 2019). This is known as the Chadian Cybercrime Cell.

Chad has also participated in the G5 Sahel Country Regional Workshop on cybercrime/cyber-terrorism. Chad signed a decree in August 2018 implementing the police component of the Joint Force on its territory (by the Joint Force’s eastern zone of operations) (UNODC, 2019).

2.3.3. Cybercrime and Cybersecurity Institutional Measures

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

- The National Agency for Computer Security and Electronic Certification (ANSICE): ANSICE is the independent national administrative authority responsible for ensuring compliance with the provisions of Law No. 09/PR/2015. ANSICE designs and implements policies to combat cybercrime, regulate and control national information systems’ security and e-communication networks. It coordinates national cybersecurity actions to ensure the security of government systems and critical state infrastructure;

- The Directorate on the Security of Electronic Communications Networks and Information Systems under the ANSICE: responsible for the fight against cybercrime and cybersecurity (ANSICE, 2019); and

- The Directorate of Expertise and Security Technology Watch, under the ANSICE (ANSICE, 2019).

- The National State Security Agency.

The Chadian government does not operate an official cybersecurity emergency response team (CERT) with national-level responsibilities (African Union, Symantec, 2016).

2.4. ELECTRONIC TRANSACTIONS

2.4.1. Overview of Electronic Transactions Legislation

The primary legal instrument regulating electronic transactions in Chad is Law No. 08/PR/2015 of 10 February 2015 on Electronic Transactions (“Law 08/2015”). Various important provisions are listed below:

- Article 25 provides that electronic writing is valid under law and has equal probative value to manuscript - subject to:
  - the identification of the person whose identity it is;
  - the preservation and guarantee of the integrity of the writing;
  - the authenticity of the origin of the data it contains, and the integrity of its contents must also be guaranteed.

- Electronic commerce transactions are secured via electronic signatures referred to in Article 20 of the Law.

- Article 44 states that all advertising accessible by electronic communication must be clearly identifiable as such. However, it must make clearly identifiable the physical person on whose behalf it is carried out.

- Chapter IV concerns electronic contracts, setting out various requirements for their use in electronic commerce. Specifically, Article 55 gives legal validity to electronic contracts, whilst Article 58 sets out with more specificity the formalities/obligations required when dealing with electronic contracts. These obligations require that online service providers shall at the very least, provide the information specified in the contract in a clear, comprehensible and unequivocal manner.

- Article 168 imposes sanctions on service providers who fail to comply with the provisions of Law 08/2015, or who prevent or hinder the performance of contractual obligations.

Implementing Decrees

Alongside Law 08/2015, there are two implementing Decree’s that regulate electronic transaction activities in Chad. ANSICE will oversee the practical aspects of the following Decree’s:

- Decree No 078 / PR / 2019 of 21 January 2019 setting the terms and conditions for providing services and means of cryptology; and

- Decree No 079 / PR / 2019 of 21 January 2019 laying down the conditions and procedures for granting the authorization to carry out the electronic certification activity).
**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.

**African Union Convention on Cybersecurity and Personal Data**

Chad signed the African Union Convention on Cybersecurity and Personal Data in June 2015.

**2.4.2. Electronic Transactions Policy Developments**

**2.4.3. Electronic Transactions Institutional Measures**

The primary institutions responsible for electronic transactions in Chad are:

- The National Agency of IT Security and Electronic Certification – established under Law 006/PR/2015; and

- The Regulatory Authority for Electronic Communications and Post (ARCEP); and

- The Directorate of Electronic Transaction Security and Electronic Certification, under the ANSICE; responsible for the security of electronic transactions (ANSICE, 2019).

The ARCEP is a public institution with administrative status, legal personality, financial autonomy and management. ARCEP is responsible for the regulation of electronic communications and postal activities under the supervision of the Ministry in charge of Posts and New Technologies of Information and Communications. ARCEP’s exclusive competence is to regulate the control and monitoring of the activities of operators and operators in the electronic communications and postal sector (ARCEP, 2019).

The powers of ARCEP in relation to e-commerce include:

- enforcement of electronic communications laws and their implementing regulations under objective, transparent and non-discriminatory conditions;

- To develop, at the request of the Minister, the draft legislative and regulatory texts aimed at changing the legal, economic and security framework in which communications activities are carried out;

- To ensure compliance by the operators of the obligations resulting from the authorizations they hold for international agreements of the national regulations for electronic communications;

- To ensure contractual compliance obligations by operators, regulation competition and pricing between operators;

- To draw up the specifications of the operators in accordance with the provisions of the law on electronic communications;

- To receive advance declarations for the provision of electronic communications services and positions;

- To approve rates for electronic communications services and positions and ensure compliance with the terms and conditions of the rates;
Arbitrate disputes arising between the operators of the electronic communications networks and/or the associated service providers, on the one hand, and their subscribers or users,

Penalize electronic communications service providers in accordance with the law or propose to the Minister the application of sanctions that fall within its jurisdiction;

Participate in meetings of regional and international organizations dealing with issues related to electronic communications and positions;

To monitor and respect the implementation of the universal access and service policy;

To issue an advisory opinion on all draft laws and regulations relating to electronic communication activities and to propose to the Government any draft legislative or regulatory text aimed at changing the legal, economic and security framework of the sectors;

To create and make available a database on information and communication technologies; and

To guarantee the protection of consumers etc.
2.5. 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 which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures</strong>&lt;br&gt;No National Cybersecurity Policy.</td>
<td><strong>Data Protection Laws and Regulations</strong>&lt;br&gt;Law No. 007/PR/2015 on the Protection of Personal Data&lt;br&gt;<strong>Electronic Commerce Laws and Regulations</strong>&lt;br&gt;Law No. 08/PR/2015 of 10 February 2015 on Electronic Transactions.</td>
<td><strong>Data Protection Authority whose responsibilities in regulating data protection include authorisation of data processing, authorisation of cross border transfers of personal data</strong>&lt;br&gt;No Data Protection Authority. However, there is a Directorate for the Protection of Privacy and Freedoms in the Cyberspaces.</td>
</tr>
<tr>
<td><strong>National Cybersecurity strategy to implement the Policy</strong>&lt;br&gt;The National Cybersecurity Strategy is being drafted.</td>
<td><strong>Cybercrime Laws and Regulations</strong>&lt;br&gt;Law 009 / PR / 2015 of 10 February 2015 on Cyber Security and the Fight against Cybercrime</td>
<td><strong>Electronic Signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications</strong>&lt;br&gt;The Directorate of Electronic Transaction Security and Electronic Certification.</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>&lt;br&gt;N/A</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;N/A</td>
<td><strong>State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;</strong>&lt;br&gt;The Directorate of Electronic Transaction Security and Electronic Certification.</td>
</tr>
</tbody>
</table>

**Table 9: Chad National Assessment Overview**

- **Data Protection Laws and Regulations**
- **Electronic Commerce Laws and Regulations**
- **Cybercrime Laws and Regulations**
- **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**

- **Data Protection Authority whose responsibilities in regulating data protection include authorisation of data processing, authorisation of cross border transfers of personal data**
- **No Data Protection Authority. However, there is a Directorate for the Protection of Privacy and Freedoms in the Cyberspaces.**
- **Electronic Signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications**
- **State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;**
- **The Directorate of Electronic Transaction Security and Electronic Certification.**
- **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**
- **The Regulatory Authority for Electronic Communications and Post**
- **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**
- **The Security Directorate of Electronic Communications Networks and Information Systems (ANSICE) operates an anti-cyber crime unit.**
- **The Directorate of Expertise and Security Technology Watch**
- **Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.**
- **The National State Security Agency.**
- **Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)**
- **The Security Directorate of Electronic Communications Networks and Information Systems (ANSICE)**
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 AU-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.

AU-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 AU-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.