5. GUINEA

Regional Economic Community: Economic Community of West African States (ECOWAS)
Population: 13 398 180
Internet Penetration: 2 411 672 users i.e. 18% of the population
AUCC Ratification Status: Signed 31/07/2018

5.1. OVERVIEW

DATA PROTECTION: Guinea has a data protection law (2016/037). Guinea has also acceded to the AUCC and will be subject to the ECOWAS Supplementary Act A/SA.1/01/10. Law 2016/037 makes provision for the Guinean Data Protection Authority however it is not yet operational. The Authority for Regulation of Post and Telecommunications is also relevant to data protection in Guinea.

ELECTRONIC TRANSACTIONS: Guinea has an electronic transactions law (2016/035). Guinea has also acceded to the AUCC and will be subject to the ECOWAS Supplementary Act A/SA.2/01/10. The National Economic and Social Development Plan is applicable to electronic commerce in Guinea. Decree D/2018/175/PRG/SGG bestows obligations on the Ministry of Posts Telecommunications and Digital Economy relating to electronic transactions. The Regulatory Authority of Posts and Telecommunications is responsible for the security of electronic transactions in the Republic of Guinea.

CYBERCRIME AND CYBERSECURITY: Guinea has a cybercrime and cybersecurity law (2016/037). Guinea has also acceded to the AUCC and will be subject to the ECOWAS Directive 1/08/11 on cybercrime. Guinea does not yet have a national cybersecurity strategy. The primary institutions relating to cybercrime and cybersecurity are the National Agency for the Security of Information Systems, the National Agency for Electronic Governance and State Computerisation and the Regulatory Authority of Posts and Telecommunications. Law No.2016/037 provides for the establishment of a CERT which has not yet been established.

5.2. DATA PROTECTION

5.2.1. Overview of Data Protection Legislation

At a Constitutional level, Article 151 of the Constitution of Guinea requires that international law takes precedence over domestic law. Accordingly, Guinea is a signatory to the Universal Declaration of Human Rights (‘UDHR’) and party to the International Covenant on Civil and Political Rights (‘ICCPR’). Article 17 of the ICCPR protects individuals against arbitrary interference with privacy, family, home and correspondence.

Law 2016/037 on cybersecurity and the protection of personal data

The primary law relating to data protection and privacy in Guinea is Law 2016/037 on cybersecurity and the protection of personal data (“Law 2016/037”). Part 2 of Law 2016/037 is dedicated to data protection and transposes the ECOWAS Supplementary Act A/SA/1/01/10 in terms of the processing of data, rights of the data subject and authorisation for sensitive data files. (Greenleaf & Cottier, 54).

Law 2016/037 requires the processing of personal data to be subject to a prior declaration by data controllers to the designated competent authority (a data protection authority in Guinea is yet to be established) (Greenleaf, 2019). Further, certain categories of personal data (listed under Article 7 of Part 2 of Law 2016/037) require prior authorisation from the Competent Authority before processing may commence.

Chapter VI of Part 2 sets out the guiding principles for the lawful processing of personal data. These include (translated):

- lawful bases for processing (consent; the fulfilment of a legal obligation; public interest; performance of a contract and safeguarding the interests of data subjects (Article 18));
- Collection, recording, processing, storage, transmission and interconnection of personal data files, must be to do so lawfully and fairly;
- Personal data must be collected for specified, explicit and legitimate purposes and cannot be subsequently inconsistent with those purposes;
- The data collected must be accurate and, if necessary;
- Transparent: The principle of transparency implies mandatory and clear information on behalf of the data controller; and
- Personal data must be processed in a way that confidentiality and be protected, especially where the treatment of these data comprises data transmissions in a network

Confidentiality and storage obligations on data controllers and data processors (sub-contractors) are specified under the general principles (Articles 23 and 24, respectively). Articles 41 - 43 provide further confidentiality and security obligations on data controllers.
Data subject rights are contained under Chapter IX of Part 2

- The right to information (Article 30-31);
- The right to oppose and object (Article 32-33);
- The right to erasure (Article 35);
- The right to copies of one’s data processed via automated means (Article 40).

Cross-border transfers are considered under Article 28. Thereunder, any transfers of personal to a third country will only be permitted if:

- the third country provides a higher level of protection or equivalent of privacy, fundamental freedoms and rights of individuals/data subjects; and
- prior authorisation must have been received from the Data Protection Authority.

The interconnection of personal data files is considered under Article 29.

Lastly, Article 47 states that the Authority responsible for the protection of personal data will be established by way of Regulation. Article 48 sets out the roles and responsibilities of the Guinean Data Protection Authority. To reiterate, the Guinean Data Protection Authority is not yet established as of writing (Greenleaf, 2019).

**ECOWAS Supplementary Acts**

The Economic Community of West African States (ECOWAS) has an ICT legal framework revolving around: e-transactions (Supplementary Act A/SA.2/01/10); cybercrime (Directive 1/08/11) and personal data protection (Supplementary Act A/SA.1/01/10). The legal framework has yet to be implemented by its Member States (UNCTAD, 2019), Guinea being one of such member states.

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


**5.2.2. Data Protection Policy Developments**

**5.2.3. Data Protection Institutional Measures**

The following institutions are relevant to Data Protection in Guinea:

- The Ministry of Posts, Telecommunications and Digital Economy (MPTEN);
- The Authority for the Regulation of Post and Telecommunications (ARPT); the ARPT has several units related to Data Protection, these include:
  - The Office of the Legal Adviser (BJC);
  - International Cooperation and External Relations (CIRE);
  - The Communication Service; and
  - The Information System Service.

### 5.3. CYBERCRIME AND CYBERSECURITY

#### 5.3.1. Overview of Cybercrime and Cybersecurity Legislation

Cybersecurity and crimes associated therewith in Guinea are primarily governed by Law 2016/037 on cybersecurity and the protection of personal data (‘Law 2016/037’).

**Law 2016/037**

Law 2016/037 introduces provisions on substantive criminal law, including illegal access, illegal interception, data and system interference, computer-related fraud and forgery and child online protection. Chapters III – XIV set out various cyber offences.

Title II of Law 2016/037 sets out the various cyber offences and electronic communications. The Title consists of the following chapters and the following types of offences:

- Chapter III: Unauthorized Access and Retention In Systems Computer;
- Chapter IV: Operating of Systems Computers And Fraudulent Introduction Of Data In Computer Systems;
- Chapter V: Fraudulent Interception, Modification and Falsification of Computer Data;
- Chapter VI: Computer Fraud, Fraudulent Treatment Of Personal Data And Use Of Falsified Data;
- Chapter VII: Detention Of Equipment To Commit Cybercriminal Infractions And Commission Of Infractions Through Associations Specifically Formed For This Purpose Or By Prior Agreement;
- Chapter VIII: Production, Import or Export, Possession, And Facilitation Of Access To Images Or Representations Of A Pornographic Character;
- Chapter IX: Disposition of Images Or Writings Of A Racist Or Xenophobic Nature Through A Computer System, Injuries, Threats, And Negations Through The Computer System;
- Chapter X: Attacks and Threats To Public Order And Security: Security, Integrity And Dignity Individuals Through A Computer System; and
- Chapter XI: Classic Infringements Of Common Law Committed On Or Through Systems, Software And Computer Programs;
- Chapter XII: Offences Concerning Personal Data Committed To Or Through Computer Systems And In The Field Of Cryptology;
- Chapter XIII: Offences In The Field Of Intellectual Property In And Through Computer Systems; and
- Chapter XIV: Offences in Matters Of Games, Money Transfers And Other Illegal Acts On Electronic Communications Networks.
Chapter XIX sets out the institutions responsible for fighting cybercrime. The National CERT of Guinea is established under Article 89 of Law 2016/037. Article 89 further specifies that the modalities and functioning of the CERT will be defined by a regulatory text. The Ministry of Posts, Telecommunications and the Digital Economy are responsible for operationalising the Guinea National CERT (Article 92).

National co-operation between the Ministry of Justice, the Ministry of Security, the Ministry of Posts, Telecommunications and the Digital Economy, as well as the Regulatory Authority of Posts and Telecommunications, is mandated under Article 106 of Law 2016/037. Furthermore, International co-operation on combating cybercrime is also mandated under Article 106 of Law 2016/037.

Decree No. 266

Decree No. 266 establishes the National Agency for Information Systems Security and sets out its functions. Article 4 of the Decree sets out its powers and duties of the Agency which include:

- Cybersecurity risk evaluation;
- Auditing of cybersecurity systems and risk simulation;
- Investigation and prevention of cyber-attacks;
- Management of cybersecurity emergencies;
- Provision of a centralised/coordinated response to requests for assistance where cyberattacks occur;
- The sharing and exchanging of information, and learning from and liaising with other countries on cybersecurity; and
- Cooperation with service providers, CERTs in other countries, researchers and other stakeholders in matters of cybersecurity.

African Union Convention on Cybersecurity and Personal Data


ECOWAS Supplementary Acts

The Economic Community of West African States (ECOWAS) has an ICT legal framework revolving around: e-transactions (Supplementary Act A/SA.2/01/10); cybercrime (Directive 1/08/11) and personal data protection (Supplementary Act A/SA.1/01/10). The legal framework has yet to be implemented by its Member States (UNCTAD, 2019), Guinea being one of such member states.

5.3.2. Cybercrime and Cybersecurity Policy Developments

Guinea does not have a national cybersecurity strategy. According to the ITU’s 2014 ‘cyber-wellness profile of Guinea’, a committee had been established to develop a cybersecurity strategy (ITU, 2014). However, a United Nations Initiative for Disarmament Research (UNIDIR) cyber profile of Guinea from 2018 indicates that Guinea has yet to launch its National Cybersecurity Strategy (UNIDIR, 2018).

The Agence Nationale de la Gouvernance Electronique et de l’Informatisation de l’Etat (ANGEIE) is the officially recognised agency that will be responsible for implementing Guinea’s National Cybersecurity Strategy, Policy and Roadmap (ITU, 2014).

Article 1 of Decree D/2018/175/PRG/SGG on the Powers and Functions of the Ministry of Posts Telecommunications and Digital Economy sets out certain functions on this Ministry to:

- Promote cybersecurity; and
- Participate in international cooperation efforts (including treaties, conventions etc) and overseeing their implementation within the Republic of Guinea.

5.3.3. Cybercrime and Cybersecurity Institutional Measures

The primary institutional measures relating to cybercrime and cybersecurity in Guinea are:

- The Ministry of Posts, Telecommunications and Digital Economy (MPTEN);
- The National Agency for Electronic Governance and State Computerization - Agence Nationale de la Gouvernance Electronique et de l’Informatisation de l’Etat (ANGEIE);
- The National Agency for the Security of Information Systems (ANSSI): established by way of Decree D/266/PRG/SGG of 29 August 2016. This law enforcement agency, under the technical supervision of the MPTEN, is the national structure responsible for cybersecurity in Guinea; and

Other relevant institutions are the:

- Ministry of Justice;
- Ministry of Security; and the
- Regulatory Authority of Posts and Telecommunications.
5.4. ELECTRONIC TRANSACTIONS

5.4.1. Overview of Electronic Transactions Legislation

Electronic communications and transactions (in the context of electronic commerce) in Guinea are primarily governed by the Law No. 2016/035 on Electronic Transactions ("Law 2016/035").

The purpose of Law 2016/035 is to regulate electronic transactions in the Republic of Guinea, in particular by defining the implementation and securing of these transactions, offences, penalties, and evidence in the matter.

A summary of the contents of Law 2016/035 insofar as electronic transactions and electronic commerce are concerned, is provided below:

• Chapter III of Title II (Articles 5 – 9) set out various requirements for electronic commerce activities in Guinea.

• Chapter V sets out various provisions relating to the conclusion of contracts via electronic means.
  • Articles 16-17 validates the conclusion of contracts electronically;
  • Article 19 provides for contractual liability for providers who provide goods/services by electronic means, by requiring various contractual terms and conditions to be provided to consumers; and
  • Article 20 sets out the conditions for a valid electronic contract.

• Electronic writing is given legal validity and equal probative value to manuscript under Article 21. Article 21 also provides for exceptions whereby its provisions do not apply to private agreements, issues related to family law and rights under the law of succession. The provisions also do not apply to agreements related to personal sureties except where a natural person or legal entity enters into an agreement by virtue of his professional duties.

• Articles 33 to 36 guarantee the security of electronic transmissions. In particular:
  • Articles 33-34 gives electronic certificates legal validity and authenticity. Article 33 provides that in the case of electronic transactions, electronic certificates confirm the intentions and obligations between the parties to an electronic transaction. Electronic signatures that are created by a reliable measure/device, and which is secured by way of an electronic certificate, are granted the same legal validity as a manuscript signature under Article 34; and
  • Article 35 provides that an electronic certificate issued by a service provider established outside Guinea has the same juridical value as one within Guinea where there is a multilateral or bilateral agreement between Guinea and that country or where the service provider satisfies the requirements of this law.

Chapter IX provides for entrusts, under the Regulatory Authority of Posts and Telecommunications in the Republic of Guinea, a body responsible for the regulation of electronic transactions or the control of the application and observance of the provisions of Law 2016/035. The Authority is responsible for the security of electronic transactions, as well as networks and computer systems.

Electronic advertising is considered under Chapter 4 (Articles 10 to 14):

• Article 10 provides that all digital advertising in whatever form, must be unambiguously identified as advertising;

• Article 11 provides that the terms and conditions of any promotional offer or advertisement must be clearly presented in a means easily accessible to the public;

• Articles 12 to 14 regulate the transmission of digital advertisements via direct communication (SMS etc) to consumers; and

• Articles 15 to 20 provide contractual rules applicable to providers of goods and services by electronic means. These include contractual liability for service providers.

ECOWAS Supplementary Acts

The Economic Community of West African States (ECOWAS) has an ICT legal framework revolving around: e-transactions (Supplementary Act A/SA.2/01/10); cybercrime (Directive 1/08/11) and personal data protection (Supplementary Act A/SA.1/01/10). The legal framework has yet to be implemented by its Member States (UNCTAD, 2019), Guinea being one of such member states.
5.4.2. Electronic Transactions Policy Developments

The following policies and strategies apply to electronic commerce and electronic transactions in Guinea:

- National Economic and Social Development Plan (PNDES), 2016-2020:

  - The PNDES states an objective to make Guinea’s telecommunication infrastructures and services more durable and dependable. Quoting from the strategic option cited:

    “The government’s strategic choice to achieve the expected result during 2016-2020 is “to make ITC an engine of economic and social development in Guinea.” The authorities view telecommunications and the digital economy as indispensable factors of development and a cross-cutting sector with direct multiplier effects on all other sectors of economic activity. The PNDES reflects this view by drawing on the six main levers of telecommunications development in Guinea: (i) the development of broadband networks, (ii) increasing the supply of energy, (iii) the sharing of infrastructures, (iv) strengthening of regulations through a “strong and effective regulatory authority,” (v) strengthening the capacities of telecommunications and ITC sector managers, and (vi) the emergence of a telecommunications/ITC ecosystem.” (Ministry of Planning and International Cooperation, 2016).

Article 1 of Decree D/2018/175/PRG/SGG on the Powers and Functions of the Ministry of Posts Telecommunications and Digital Economy sets out certain functions on this Ministry which include:

- Developing digital networks for public and private;
- Development and implementation of the national digital strategy;
- Promotion of the digital economy;
- Supporting and promoting the creation of incubators for small and medium enterprise development in ICT;
- Developing public ICT resources to implement e-government services; and
- Ensuring sustainable development of the ICT sector.

5.4.3. Electronic Transactions Institutional Measures

The primary institution relating to electronic transactions and commerce in Guinea is the Regulatory Authority of Posts and Telecommunications. The Authority is responsible for the security of electronic transactions in the Republic of Guinea.

The relevant Ministries relating to electronic transactions and commerce in Guinea are:

- The Ministry of Posts, Telecommunications and Digital Economy (MPTEN); and
- The Ministry of Planning and International Cooperation.
5.5. 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>
</table>
| **Cybersecurity Policy which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures** | **Data Protection Laws and Regulations**  
Law 2016/037. | **Data Protection Authority whose responsibilities in regulating data protection include authorisation of data processing, authorisation of cross border transfers of personal data** |
| **The National Cybersecurity Strategy, Policy and Roadmap.** | **Electronic Commerce Laws and Regulations**  
Law 2016/035 on Electronic Transactions. | **Electronic Signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications** |
| **National Cybersecurity strategy to implement the Policy** | **Cybercrime Laws and Regulations**  
Governed by Law 2016/037. | **State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;** |
| Guinea does not have a strategy yet, but a committee has been established to develop one. | **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** | **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** |
| **Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture** | | **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 Authority for the Regulation of Post and Telecommunications (ARPT).** |
| | | **Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.** |
| | | **The Ministry of Planning and International Cooperation.** |
| | | **Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)** |
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.