The emergence of a global and borderless information society brings new opportunities to all countries worldwide as technologies play an even more important role in social and economic development. Services in the health, educational, business, finance and public administration sectors are possible thanks to ICT applications.

ICTs also bring new challenges which must be addressed if we are to securely conduct e-health transactions, enable citizens to access e-government services, provide the necessary trust for online commercial and business transactions and maintain the integrity of our information technology systems and resources. Despite the low level of ICT development and the low Internet penetration, Africa is experiencing rapid growth of cybercrime; cybercriminals have found ways to take advantage of the weak ICT infrastructure and turn Africa into a haven for operating illegally with impunity. Cybersecurity is still considered a luxury rather than a necessity in many African economies and its importance has not yet been sufficiently appreciated or recognized. Cybersecurity budgets in many organizations are reported to be less than 1% and many organizations have no budget allocated to Cybersecurity.

Cybersecurity has become even more important with the emergence of the COVID 19 pandemic, which has imposed the use of ICTs for all aspects of daily life. Computer attacks and digital scams have increased alarmingly during these times of uncertainty. It is therefore becoming crucial for countries and organisations to have frameworks in place to govern data protection and the security of electronic transactions. Putting in place adequate security and trust solutions is therefore one of the main challenges that must be addressed.

This Cybersecurity Assessment Report provides an overview of the various legislative and legal measures taken by African governments in selected countries to ensure the protection of personal data, the security of electronic transactions and the fight against cybercrime. It compares these measures to those defined by the African Union Convention on Cybersecurity and Personal Data Protection (AUCC), a credible framework for Cybersecurity in Africa. The study reveals that institutional measures relating to cybercrime and cybersecurity, as well as policy measures and institutional strategies relating to electronic transactions, are the areas lagging the furthest behind in the implementation activities of the member states studied.

The report has been developed to contribute to the advancement of cybersecurity in Africa and to strengthen the legal framework within which electronic transactions and the transfer of personal information take place on the continent. Building on the findings and recommendations of this report, AUDA-NEPAD will work to support member states in the development of policies and laws and in the implementation of institutional measures as required by the African Union Convention on Cybersecurity and Personal Data Protection.

Ibrahim Assane Mayaki
AUDA-NEPAD CEO
CYBERSECURITY ASSESSMENT REPORT

TABLE OF CONTENTS

LIST OF ABBREVIATIONS ............................................................................................................................................. 4
LIST OF TABLES ................................................................................................................................................................ 7
LIST OF FIGURES ............................................................................................................................................................ 7
EXECUTIVE SUMMARY.................................................................................................................................................. 8
INTRODUCTION ............................................................................................................................................................... 9
THE AFRICAN UNION CONVENTION ON CYBERSECURITY AND PERSONAL DATA PROTECTION (AUCC) ......................... 9
  Objective and Scope
  Overview of the requirements
  Impact of the AUCC
  Current Status of the AUCC – Ratification and Amendment
  Data Protection Measures
  Electronic Transaction And E-Commerce Measures
  Cybercrime And Cybersecurity Measures
  International Co-Operation Measures
  Checklist Of Requirements
ANALYSIS FRAMEWORK .................................................................................................................................................. 14
  Defining Cybersecurity
  Methodological Process
  Country Selection
  Assessment Criteria And Data Sources
  Data Collection Methods
ANALYSIS ........................................................................................................................................................................... 15
  Cybersecurity Policy And Strategic Objectives
  Public-Private Partnerships
  Laws And Regulations
  Institutional Measures
  Emergency Response Measures
  International Cooperation
RECOMMENDATIONS .......................................................................................................................................................... 22
  National Level
  Regional Level
  Continental Level
MEMBER STATE NATIONAL ASSESSMENTS .................................................................................................................. 25
  Introduction
  Structure of the National Assessment Reports
BENIN ............................................................................................................................................................................. 26
CHAD ............................................................................................................................................................................. 31
REPUBLIC OF CONGO .................................................................................................................................................... 37
DEMOCRATIC REPUBLIC OF CONGO .......................................................................................................................... 42
## LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFAPDP</td>
<td>Association francophone des autorités de protection des Données Personnelles (Association of Data Protection Authorities)</td>
<td>Morocco</td>
</tr>
<tr>
<td>ANC</td>
<td>Agence Nationale de Certification (National Certification Agency)</td>
<td>Tunisia</td>
</tr>
<tr>
<td>ADIE</td>
<td>Agence De l'Informatique de l'Etat (State Computer Agency)</td>
<td>Senegal</td>
</tr>
<tr>
<td>ADETIC</td>
<td>Agence de Développement des Technologies de l'Information (ICT Development Agency)</td>
<td>Chad</td>
</tr>
<tr>
<td>ANSICE</td>
<td>Agence Nationale de Sécurité Informatique et de Certification Electronique (National Agency for Computer Security and Electronic Certification)</td>
<td>Chad</td>
</tr>
<tr>
<td>ANSI</td>
<td>Agence Nationale de Sécurité Informatique (National Agency for Computer Security)</td>
<td>Tunisia / Mauritania</td>
</tr>
<tr>
<td>ANSSI</td>
<td>Agence Nationale des Systèmes d'information de Sécurité (National Agency for Security Information Systems)</td>
<td>Benin / Guinea</td>
</tr>
<tr>
<td>APDP</td>
<td>Autorité de Protection des Données à caractère Personnel (the Personal Data Protection Authority)</td>
<td>Benin</td>
</tr>
<tr>
<td>ARCEP</td>
<td>Autorité de Régulation de la Poste et des Communications Electroniques (Regulatory Authority for Electronic Communications and Post)</td>
<td>Chad</td>
</tr>
<tr>
<td>ARPCE</td>
<td>Autorité de Régulation de la Poste et des Communications Electroniques du Congo (Regulatory Agency for Post and Electronic Communications of the Republic of Congo)</td>
<td>Republic of Congo</td>
</tr>
<tr>
<td>ARPT</td>
<td>Autorité de Régulation de la Poste et des Télécommunications (Authority for the Regulation of Post and Telecommunications)</td>
<td>Guinea</td>
</tr>
<tr>
<td>ARPTC</td>
<td>Autorité de Régulation de la Poste et des Télécommunications du Congo (Authority of the Post and Telecommunications of Congo)</td>
<td>Democratic Republic of Congo</td>
</tr>
<tr>
<td>BEF</td>
<td>Financial and Economic Brigade</td>
<td>Benin</td>
</tr>
<tr>
<td>BjCSIRT</td>
<td>Benin Computer Security Incident Response Team</td>
<td>Benin</td>
</tr>
<tr>
<td>CA</td>
<td>Communications Authority</td>
<td>Kenya</td>
</tr>
<tr>
<td>CBM</td>
<td>Confidence Building Measures</td>
<td>Benin</td>
</tr>
<tr>
<td>CEEAC</td>
<td>Communauté économique des États de l’Afrique centrale (Economic Community of Central African States)</td>
<td>Chad</td>
</tr>
<tr>
<td>CEMAC</td>
<td>Central African Economic and Monetary Community</td>
<td>Chad</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
<td>Benin</td>
</tr>
<tr>
<td>CIRAS</td>
<td>Centre d'Informatique et de Recherche de l’Armée et de la Sécurité (Centre for Computing and of Research of the Army and of Security)</td>
<td>Republic of Congo</td>
</tr>
<tr>
<td>CIRE</td>
<td>Coopération Internationale et Relations Extérieures (International Cooperation and External Relations)</td>
<td>Guinea</td>
</tr>
<tr>
<td>CNC</td>
<td>Commission Nationale de Cryptologie (National Cryptology Commission)</td>
<td>Senegal</td>
</tr>
<tr>
<td>CNDP</td>
<td>Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (National Control Commission for the Protection of Personal Data)</td>
<td>Morocco</td>
</tr>
<tr>
<td>CNIL</td>
<td>Commission Nationale de l'informatique et des Libertés (National Commission for Computing and Liberties)</td>
<td>Benin</td>
</tr>
</tbody>
</table>
## LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>COP</td>
<td>Online Child Protection Initiative</td>
<td>Tunisia</td>
</tr>
<tr>
<td>CPD</td>
<td>Commission de Protection des Données Personelles (Data Protection Authority)</td>
<td>Senegal</td>
</tr>
<tr>
<td>CRL</td>
<td>Commission on Rights and Liberties</td>
<td>Tunisia</td>
</tr>
<tr>
<td>DeG</td>
<td>Directorate of e-Government</td>
<td>Kenya</td>
</tr>
<tr>
<td>DGDEN</td>
<td>Director-General of the Development of the Digital Economy</td>
<td>Republic of Congo</td>
</tr>
<tr>
<td>DGITC</td>
<td>Director General of Information Technology and Communications</td>
<td>Mauritania</td>
</tr>
<tr>
<td>DGSSI</td>
<td>The Directorate-General for Information Systems Security</td>
<td>Morocco</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
<td>Mauritania</td>
</tr>
<tr>
<td>EAC</td>
<td>East African Community</td>
<td>Kenya</td>
</tr>
<tr>
<td>ECCAS</td>
<td>Economic Community of Central African States</td>
<td>Kenya</td>
</tr>
<tr>
<td>ECOWAS</td>
<td>Economic Community of West African States</td>
<td>Kenya</td>
</tr>
<tr>
<td>FIRST</td>
<td>Forum of Incident Response and Security Teams</td>
<td>Tunisia</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
<td>Kenya</td>
</tr>
<tr>
<td>ICTA</td>
<td>ICT Authority</td>
<td>Kenya</td>
</tr>
<tr>
<td>INAI</td>
<td>l’Instance Nationale d’Accès à l’Information (Tunisian Access to Information Authority)</td>
<td>Tunisia</td>
</tr>
<tr>
<td>INPDP</td>
<td>l’Instance Nationale de Protection des Données à Caractère Personnel (National Authority for the Protection of Personal Data)</td>
<td>Tunisia</td>
</tr>
<tr>
<td>GCA</td>
<td>Government Certification Authority</td>
<td>Kenya</td>
</tr>
<tr>
<td>GUOT</td>
<td>Guichet Unique Des Operations Transfrontalières (Cross Border Operations)</td>
<td>Republic of Congo</td>
</tr>
<tr>
<td>ma-CERT</td>
<td>The Moroccan Computer Emergency Response Team</td>
<td>Morocco</td>
</tr>
<tr>
<td>MAURIPOST</td>
<td>The Mauritanian Post Corporation</td>
<td>Mauritania</td>
</tr>
<tr>
<td>MDN</td>
<td>Ministry of Interior and Decentrilization</td>
<td>Mauritania</td>
</tr>
<tr>
<td>MEFPNT</td>
<td>The Mauritanian Ministry of Employment, Vocational Training and New Technologies</td>
<td>Mauritania</td>
</tr>
<tr>
<td>MoICT</td>
<td>Ministry of ICT</td>
<td>Kenya</td>
</tr>
<tr>
<td>MPTEN</td>
<td>Ministère des Postes, Télécommunications et Economie Numérique (Ministry of Posts, Telecommunications and Digital Economy)</td>
<td>Guinea</td>
</tr>
<tr>
<td>NCS</td>
<td>National Communications Secretariat</td>
<td>Kenya</td>
</tr>
<tr>
<td>NCACCC</td>
<td>National Computer And Cybercrimes Co-Ordination Committee</td>
<td>Kenya</td>
</tr>
<tr>
<td>NDC</td>
<td>National Data Centre</td>
<td>Mauritania</td>
</tr>
<tr>
<td>NSMAI</td>
<td>The National Strategy of Modernization of Administration and Information and Communication Technologies</td>
<td>Mauritania</td>
</tr>
<tr>
<td>OCRC</td>
<td>Office Central de Répression de la Cybercriminalité (Central Office for the Suppression of Cybercrime)</td>
<td>Benin</td>
</tr>
<tr>
<td>OHADA</td>
<td>Organisation pour l’Harmonisation en Afrique du Droit des Affaires (Organization for Harmonization of Business Law)</td>
<td>Senegal</td>
</tr>
<tr>
<td>PDPC</td>
<td>Personal Data Protection Commission system</td>
<td>Senegal</td>
</tr>
<tr>
<td>PNDES</td>
<td>Plan National de Développement Economique et Social (National Economic and Social Development Plan)</td>
<td>Guinea</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
<td>Location</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>PSE</td>
<td>Le Plan Sénégal Emergent (The Emergent Senegal Plan)</td>
<td>Senegal</td>
</tr>
<tr>
<td>STCC</td>
<td>Services Techniques Centraux des nombres et de la sécurité des systèmes d'information (Central Technical Services of Numbers and Security of Information Systems)</td>
<td>Senegal</td>
</tr>
<tr>
<td>TunCERT</td>
<td>Tunisian Computer Emergency Response Team</td>
<td>Tunisia</td>
</tr>
<tr>
<td>Tuntrust</td>
<td>National Electronic Certification Agency</td>
<td>Tunisia</td>
</tr>
<tr>
<td>RCA</td>
<td>Root Certification Authority</td>
<td>Kenya</td>
</tr>
<tr>
<td>RCEF</td>
<td>Les Règles Contraignantes d'Entreprise Francophones (Binding Corporate Rules)</td>
<td>Morocco</td>
</tr>
<tr>
<td>RCI</td>
<td>Le Référentiel Commun d'Interopérabilité (The Common Repository of Interoperability)</td>
<td>Mauritania</td>
</tr>
<tr>
<td>UDHR</td>
<td>Universal Declaration of Human Rights</td>
<td>Kenya</td>
</tr>
<tr>
<td>UMA</td>
<td>Union of Arab Maghreb</td>
<td></td>
</tr>
<tr>
<td>UNIDIR</td>
<td>United Nations Initiative for Disarmament Research</td>
<td></td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Cybersecurity is of rising significance on the African continent, whether in response to opportunities in the digital economy or rising incidents of cybercrime. In Kenya, between April and June 2019 alone, Kenya’s Director of Criminal Investigation issued warrants of arrest against one hundred and thirty (130) suspected hackers and fraudsters for alleged banking fraud – showing that financial losses to cyber insecurity are a growing concern on the continent (Muendo, 2019). In 2018, the Malawian government announced it would require businesses to offer options for digital payments in an effort to expand the digital economy and tax base. Countries such as Malawi are seeking out the benefits of digital innovation for economic prosperity but will have a dependence on securing national information systems.

The African Union’s Convention on Cyber Security and Personal Data Protection (AUCC/Convention) was drafted in 2011 to establish a credible framework for cybersecurity in Africa through organization of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime. Working documents prefacing the AUCC note that the objective of such a Convention was to address the cybercrime related legislative challenges in the African Continent in a compatible and harmonised manner. As such the Convention promotes, in the main, for African states to establish policy, strategic, institutional and legal frameworks for cybersecurity in the context of credible digital environment. The AUCC encompasses in cybersecurity, three main areas: (1) electronic transactions, (2) personal data protection, (3) cybersecurity and cybercrime. The Convention will enter into force thirty (30) days after the 15th instrument of ratification or accession is deposited. The current status is five (5) ratifications out of fifty-five (55) AU member States (Ghana, Guinea, Mauritius, Namibia and Senegal), while fourteen (14) more Member States have signed the Convention.

According to the International Telecommunication Unions’ (ITU) 2018 Global Cybersecurity Index, thirty eight (38) out of the forty-four (44) participating African countries had enacted cybercrime legislation, whilst as at October 2019, twenty-five (25) of Africa’s fifty-four (54) countries have passed data protection laws (Sylla and Ford-Cox, 2019).

This Report analyses and compares the policy and regulation in ten (10) African Union member states - Benin, Chad, Republic of Congo, Democratic Republic of Congo, Guinea, Kenya, Mauritania, Morocco, Senegal and Tunisia. Whilst this Report is limited to the aforementioned ten (10) African Union member states, the study is intended to be rolled out to the rest of the fifty-five (55) Africa Union member states in the future.

The methodology for the study included developing a questionnaire for the purposes of information gathering, as well as the collection and analysis of the data. Information gathering in accordance with the methodology, including the distribution of the questionnaire to the select African member states (government, private sector and academic representatives) and the exchange of information on national legislation, was conducted between July 2019 and January 2020. The analysis points to several common approaches. There are however significant differences between the approaches. The analysis compares the approaches to the provisions of the AUCC. The observations lead to a set of conclusions which policy makers may find relevant in understanding how their national approaches compare with the provisions of the AUCC and the measures taken by other countries. In particular, the Report provides recommendations at the national, regional and continental level.

At the national level, the Report recommends African Union member states to consider: (i) drafting or reviewing outdated the legislative and regulatory frameworks; (ii) implementing institutional frameworks provided for in legislative and regulatory frameworks; and (iii) balancing interests in cybersecurity and human rights. The Report recommends that African Union consider supporting harmonisation of laws and policies at the African Union member state level. Finally, at the continental level, the Report recommends: (i) harmonising definitions of cybersecurity; (ii) gathering baseline and annual statistics; (iii) promoting dialogues with national and regional stakeholders on the significance of the Convention and concerns pertaining to the ratification of the Convention; (iv) comparing the AUCC with global models and conventions and moving towards compatibility with these models and conventions; (v) promoting cybersecurity in the context of cyber stability; and (vi) broadening co-operation with African Union member states.

1 The African Union (AU), formed in 2002 to replace the Organisation of African Unity, consists of 55 African states, and its broad objectives include establishing peace and security, and fostering development and socio-economic integration on the African continent.
INTRODUCTION

The realisation of the importance that developing countries in general and African countries in particular take cybersecurity seriously inspired the UN General Assembly to produce a resolution as early as 2002, which mandated the International Telecommunication Union (ITU) “to facilitate the transfer of information technology and capacity-building to [those] countries, in order to help them to take measures in cybersecurity” (United Nations General Assembly Resolution 57/239 on the creation of a global culture of cybersecurity). In this regard, the preamble of the African Union Convention on Cybersecurity and Personal Data Protection (AUCC) considers that the “protection under criminal law of system of values is a necessity prompted by security considerations; that are reflected primarily by the need for appropriate criminal legislation in the fight against cybercrime in general, and money laundering in particular” (AUCC, 2014). Furthermore, the preamble recalls that the AUCC “aims at defining the objectives and broad orientations of the Information Society in Africa and strengthening existing legislations on Information and Communication Technologies (ICTs) of Member States and the Regional Economic Communities (RECs)” (AUCC, 2014) and considers that “the goal of [the] Convention is to address the need for harmonized legislation in the area of [cybersecurity] in Member States of the African Union...” (AUCC, 2014). The ITU’s 2018 Cybersecurity Index provides various insights into the current cybersecurity stance of the African Region. In particular, it indicated that the African region has the least National Cybersecurity Strategies – only fourteen (14) out of forty-four (44) African Union member states that participated in the study had National Cybersecurity Strategies (ITU, 2018). Furthermore, the African region was shown to have the least national CERTs – only thirteen (13) out of the forty-four (44) African Union member states that participated in the study had national CERTs, whilst only seventeen (17) African Union member states provide professional training in cybersecurity (ITU, 2018).

Objective and Scope

Considering the above, the objective of this study was to assess the laws, policies and regulations of selected African Union member states in order to develop tailored guidelines and interventions for implementation of the AUCC in these selected African Union member states. In turn, the study aimed to contribute to the advancement of Africa’s cybersecurity posture, and the strengthening of the legal framework within which electronic transactions and the transfer of personal information take place on the continent.

To date, a number of African Union member states have developed and published policies, legislation and established institutions meeting the requirements in the provisions of the AUCC (see Table 1 below where the main elements of the AUCC provisions are compared with the data collected from the African Union member states under study). Of the ten (10) African Union member states under study, Benin, Chad, Mauritania and Tunisia have signed the AUCC, Guinea and Senegal have ratified the Convention and DRC, Kenya and Morocco have neither ratified nor signed the Convention.

This report, albeit only considering a sample of African countries, fills a gap in available information on whether measures that African states (through the sample) have established or are in the process of establishing align with the requirements of the AUCC.

THE AFRICAN UNION CONVENTION ON CYBERSECURITY AND PERSONAL DATA PROTECTION (AUCC)

The African Union Cybersecurity Convention and Personal Data Protection (AUCC/Convention) was adopted at the 23rd Ordinary Session of the Assembly of the Union, Malabo, on the 27th June 2014. Primarily the Convention is concerned with the establishment of a Legal Framework for Cyber-security and Personal Data Protection that embodies the existing commitments of African Union Member States at sub-regional, regional and international levels to build the Information Society and address the need for harmonized legislation in the area of cyber security in Member States of the African Union. As a third dimension, the AUCC provides for regulatory measures to support growth and development of electronic transactions on the continent.

Overview of the Requirements

At a glance, the Convention requires member states to:

- Develop an enabling environment to facilitate electronic commerce and transactions;
- Develop a national cyber security Framework;
- Develop a Policy, strategy and legislation on cybercrime and ancillary regulations;
- Ensure the protection of critical information infrastructure;
- Enact personal data protection laws; and
- Establish a Data Protection regulatory institution.
The Convention encompasses several aspects of cybersecurity governance at the level of African Countries. Chapter 3 of the Convention address the promotion of cybersecurity and the combating of cybercrime. Article 24 of the Convention requires member states to undertake and develop a national cybersecurity policy that recognise the Importance of Critical Information Infrastructure in Identifying risks faced by the member state. Moreover, the cybersecurity policy should be developed in collaboration with relevant stakeholders and how the objective outlined in the policy will be achieved, should be clearly stipulated in the respective cybersecurity policies. Furthermore, Article 24(2) requires member states to adopt national strategies adequate to implement the national cybersecurity policy. Again, the national strategy should clearly stipulate the organisational structures, objectives and timelines for successful implementation of the cybersecurity strategy. Furthermore, according to Article 25 member states should have legal measures in place, such as legislation against crime, national regulatory authorities, protection of critical Infrastructure and establishment of citizens’ rights in the area of cybersecurity. Article 26, goes further to require the establishment of national cybersecurity systems by creating a culture of cybersecurity among stakeholders, educate and train relevant stakeholders so as to develop the national capacity with regard to cybersecurity, as well as, develop public-private partnerships as a model to engage with the relevant stakeholders. Article 27 also requires that national monitoring structures and an Institutional framework be put in place to provide for cybersecurity governance. Moreover, Article 28 provides that there should be International cooperation between the member states within the region, exchange of information between the member states and International, Inter-government or regional or based on public-private partnerships, so as combat the risk of cybersecurity threats within a member state.

Impact of the AUCC

The Convention is a positive step for the continent to the extent that a standardised approach to the regulation of (1) electronic transactions, (2) personal data protection and (3) cyber security and cybercrime is provided - regulatory areas that several governments on the continent have not adequately responded to. Additionally, the call for adherence to national constitutions and international human rights law when implementing the Convention at the national level promotes further harmonisation and standardisation with international approaches facilitating international co-operation. In its dealing with cybersecurity specifically, the AUCC represents the culmination of considerable effort to establish an African response. The Convention intends to:

- Facilitate the establishment of relevant structures to implement cybersecurity defences and mitigate cybersecurity threats and vulnerabilities;
- Foster cooperation and coordination between government and the private sector;
- Promote and strengthen international cooperation in cybersecurity; and
- Build capacity and promote a culture of cybersecurity.

Table 1: AUCC STATUS TABLE

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SIGNED</th>
<th>RATIFIED / ACCEDED</th>
<th>DEPOSITED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benin</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Chad</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Comoros</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Congo</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Ghana</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Guinea</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Guinea Bissau</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Mozambique</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Mauritania</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Mauritius</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Namibia</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Rwanda</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Sao Tome &amp; Principe</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Senegal</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Sierra Leone</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Togo</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Tunisia</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Zambia</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

Current Status of the AUCC – Ratification and Amendment

The Convention is open to all Member States of the Union for signature, ratification or accession, in conformity with their respective constitutional procedures. It shall enter into force thirty days after the date of receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification. As of January 2020, there have been fourteen (14) signatures, five (5) ratifications/accessions and five (5) deposits (African Union, 2020). A full list of the fifty-five (55) African Union member states is available in Annexure “A” of this Report.

The Convention may be amended or revised upon proposals from African Union member states in accordance with due process.
DATA PROTECTION MEASURES

The Preamble of the AUCC stresses that the protection of personal data and private life constitutes a major challenge to the ambitions of the information society. The Convention acknowledges that achieving the requisite protection requires a balance between the use of information and communication technologies and the protection of the privacy of citizens in their daily or professional lives, while guaranteeing the free flow of information.

Chapter II of the Convention, which deals with personal data protection, requires Member States to provide for the following:

- **establish a legal framework that strengthens the fundamental rights and freedoms of citizens, particularly the protection of their personal data and provide penalties for the violation of privacy whilst balancing against the need to ensure the free flow of data** (Article 8.1);

- **ensure that specific activities related to the processing of personal data are subject to the authorisation of an administrative authority** (Article 10.4);

- **institutional framework for personal data protection**, by inviting States Parties to establish an independent administrative authority in charge of protecting personal data in their national mechanism (Article 11);

- **obligations relating to conditions governing personal data processing**, thus making it possible, on the one hand, to lay down the basic principles governing the processing of personal data (Article 13) and, on the other hand, specific principles (Article 14) for the processing of sensitive data, as well as the supervision of personal data files interconnection;

- **data subjects’ rights**, namely the right to information, right of access, right to object and the right of rectification or erasure, which enable natural persons whose data is being processed to maintain control over same (Articles 16 to 19); and

- **obligations of the personal data controller**, namely the confidentiality obligations, security obligations, storage obligations and sustainability obligations which reflect the rights of the persons concerned and are consistent with personal data processing principles.

ELECTRONIC TRANSACTION AND E-COMMERCE MEASURES

The Preamble consolidates the barriers to electronic commerce in Africa as including in particular, gaps and weaknesses in:

- **Regulation of the legal recognition of data communications and electronic signatures**;
- **Legal rules that protect consumers, intellectual property rights, personal data and information systems**;
- **Legislation regulating electronic services**;
- **The rules applicable to cryptology**;
- **The regulation of online advertising**; and
- **Fiscal and custom legislation that apply to electronic commerce**.

Member states are called on to establish a regulatory framework to address the abovementioned and in so doing provide for the information security and legal framework that facilitates e-commerce in Africa. The framework must address:

- **the principle of free exercise of electronic commerce activities** (Article 2.1) with a framework for information disclosures by e-commerce providers to consumers (Article 2.2) and contractual liability of such providers (Article 3), as well as regulate advertising by electronic means (Articles 4.1 and 4.2); the prohibition of direct marketing to any individual who has not consented to the use of their particulars (Article 4.3);

- **contractual obligations in electronic form**, by laying down the general rules applicable to the legal validity and formation of electronic contracts (Article 5), and define the legal basis for the recognition of written documents in electronic form (Article 6); require tax invoices pertaining to e-services to maintain readability, integrity and sustainability of the contents of the invoice (Article 5);

- **security of electronic transactions**, through the introduction of electronic payment methods in electronic transactions (Article 7.1a), the institution of rules of evidence in electronic transactions (Article 7.1 b) and the admissibility of the electronic signature (Article 7.4).
The Convention emphasises the importance of cybersecurity for the well-being of society. Aware of the risks associated with information and communication technologies, the Convention requires that measures are taken to secure critical information infrastructure, deal substantively and procedurally with cybercrime, and improve capacity and enhance the resilience to threats to cybersecurity.

Member states are called on to develop a holistic approach to promoting cybersecurity and combatting cybercrime by:

- **Defining the national cyber security framework:** Defining a logical framework is a prerequisite for cyber security promotion at national level. The most important measures to be taken at this level concern the elaboration and adoption, by each Member State, of a national cyber security policy (Article 24.1). However, the effective implementation of these cyber security policies will be ensured only through a precise definition of relevant strategies (Article 24.2) in the light of the regional goals defined in the Convention.

- **Defining cybercrime offences:** Article 29 states in no indeterminable terms, Member Countries to take the necessary legislative and regulatory measures to establish the identified criminal offences. Article 29 states in no indeterminable terms, State Parties shall take the necessary legislative and/or regulatory measures to make the offences provided for the Convention provided for the Convention provided for the Convention.

- **Establishing a national cyber security system** (Article 26): The Convention invites African Countries to build their national cyber security system on four basic pillars. These are, in the order proposed by the text of the African Union, as follows:
  - promoting a culture of cyber security (Article 26.1) among all stakeholders in the cyberspace;
  - the role of governments (Article 26.2), which must be to provide leadership for developing a culture of security within their borders, notably through sensitisation, as well as provision of education and training;
  - developing Public-Private Partnership (Article 26.3) as a model to engage industry, the civil society and academia in the promotion and enhancement of a culture of cyber security; and
  - capacity-building through education and training (Article 26.4), through the adoption of capacity-building measures for the benefit of the various stakeholders in the Information Society, including the establishment of training programmes in all areas of cyber security.

**INTERNATIONAL CO-OPERATION MEASURES**

The Convention calls on Member States to provide for co-operation with regional and interactional stakeholders particularly for the purposes of harmonising and reconciling approaches to advancing cybersecurity. Member States are called on to:

- **Adequately interpret Convention** (Article 33). The Convention requires that the provisions of the Convention shall not be interpreted in a manner that is inconsistent with the relevant principles of international law, including international customary law. Hence Member States implementing the Convention are called upon to adequately interpret the provisions to avoid conflicts with international law and international customary law. Furthermore, the Preamble requires consideration of internationally recognised best practices and affirms a commitment to freedoms and rights in instruments of the AU and the United Nations. Again Member States are called upon to interpret the provisions of the Convention in light of various other rights instruments.
Table 2: Checklist of Requirements under the AUCC

<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>- 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></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 and 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 cybersecurity incidents, co-ordination and co-operation for (cybersecurity) restorative justice, forensic investigations, cybersecurity prosecution</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>
</tbody>
</table>
ANALYSIS FRAMEWORK

DEFINING CYBERSECURITY

Cybersecurity can be defined to include the tools, policies, guidelines, training, best practices, assurances and technologies that can be used to protect the cyber-environment, organisation, and users’ assets and cybersecurity governance measures. These can include technical protection measures, development of organisational or institutional capacities, policy and legal measures that aim to promote cybersecurity and prohibit acts that violate the security or integrity or availability of computer data and systems or networks and attacks against critical information infrastructure (Oriji, U.J, 2012).

METHODOLOGICAL PROCESS

Considering the purpose of this study, the methodological process undertaken was as follows:

1. Determine the assessment criteria for the study against the legal and regulatory, policy, and institutional requirements of the AUCC across the themes of data protection, electronic transactions and cybersecurity and cybercrime;
2. Define the purpose and scope of the National Assessments;
3. Clarify the data collection methods for the National Assessments;
4. Selection of the countries for study;
5. Develop the questionnaire to follow when assessing the cybersecurity standing of the ten African Union member states that sets out the relevant assessment criteria and the key sources of data (evidence) for the assessment;
6. Assess the legislation, regulation, policies, strategies and institutions across the ten (10) selected African Union member states; and
7. Conduct interviews with stakeholders (government, academia and legal experts) for further data collection and validation of desktop findings where possible.

ASSESSMENT CRITERIA AND DATA SOURCES

For the purposes of this Report, we considered whether the selected African Union member states have in place the legislative/regulatory, policy and institutional measures in the areas of data protection, cybersecurity and cybercrime and electronic transactions called for by the AUCC. In particular, high-level considerations were:

- What are the data protection legislative measures?
- What are the data protection policy developments?
- What are the data protection institutional measures?
- What are the cybercrime and cybersecurity legislative measures?
- What are the cybercrime and cybersecurity policy developments?
- What are the cybercrime and cybersecurity institutional measures?
- What are the electronic transactions legislative measures?
- What are the electronic transactions policy developments?
- What are the electronic transactions institutional measures?

Information gathering in accordance with the methodology, including the distribution of a questionnaire (Annexure “C”) to the select African Union member states (government, private sector and academic representatives) and including the exchange of information on national legislation, was conducted between July 2019 and January 2020.

COUNTRY SELECTION

The ten (10) African Union member states studied were selected based on several factors including:

- Countries that have signed and/or ratified the AU Convention;
- Countries with representatives in the PAP Committee on Transport, Industry, Telecommunications, Energy, Science and Technology which is collaborating with AUDA-NEPAD on the Cybersecurity project;
- Countries that are recognised ICT leaders within their respective regions (for benchmarking); and
- Regional and geographic balancing.

DATA COLLECTION METHODS

The collection of data involved a mixed methods approach with an embedded design, incorporating (a) documentary analysis; and b) expert stakeholder analysis.

National policies and legal documents were collected via desktop research and supplemented by focal points and/or stakeholders in each sub-region/member state. Study of the documentation took place to gain insight on cybersecurity governance measures followed by documentary analysis of primary and secondary sources relevant to cybersecurity policies and programmes in the African Union member states. To enhance interpretation and validate these findings, in-depth interviews with relevant expert stakeholders were conducted. The data collected supported our analysis of how the national measures of the ten (10) African Union member states compare with the provisions of the AUCC.
ANALYSIS

CYBERSECURITY POLICY AND STRATEGIC OBJECTIVES

The Convention recognises the principle of national sovereignty of member states in cybersecurity governance and provision is made for member states to establish national legal, institutional and policy measures i.e. the Convention does not call for uniformity at the national level.

**Article 8:** Each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of personal data, and punish any violation of privacy without prejudice to the principle of free flow of personal data

Stakeholders consulted suggest differences in the governing motivation or stimulus for cybersecurity measures implemented. African Union member states may be motivated by economics, national security, or military defence. Another major difference is the scope of cyber security measures: whilst the majority of countries prioritised policy and legislation, strategies to implement policies and institutions to support implementation of policies and strategies are not as widespread.

The Convention also provides that member states should have a Cybersecurity Policy which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures, as well as, a National Cybersecurity strategy to implement such policy.

**Article 24 (1):** Each Country shall undertake to develop, in collaboration with stakeholders, a national cyber security policy which recognises the importance of Critical Information Infrastructure (CII) for the nation identifies the risks facing the nation in using the all-hazards approach and outlines how the objectives of such policy are to be achieved.

**Article 24 (2):** State parties shall adopt the strategies they deem appropriate and adequate to implement the national cyber security policy, particularly in the area of legislative reform and development, sensitisation and capacity building, public-private partnership, and international cooperation, among other things. Such strategies shall define organizational structures, set objectives and timeframes for successful implementation of the cyber security policy and lay the foundation for effective management of cyber security incidents and international cooperation.

Guinea, Kenya, Mauritania, Morocco and Tunisia have a Cybersecurity Policy that recognises Critical Information Infrastructure, identifies the national security interests in cyberspace and recognises the need for mitigation measures. Kenya, Morocco and Tunisia have a national Cybersecurity Strategy to implement the Policy.

<table>
<thead>
<tr>
<th>Countries</th>
<th>Benin</th>
<th>Chad</th>
<th>Congo</th>
<th>DRC</th>
<th>Guinea</th>
<th>Kenya</th>
<th>Mauritania</th>
<th>Morocco</th>
<th>Senegal</th>
<th>Tunisia</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cybercrime and Cybersecurity</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Policy which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures Art 24(1)</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>National Cybersecurity strategy to implement the Policy Art 24(2)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture Art 26</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
</tbody>
</table>
PUBLIC-PRIVATE PARTNERSHIPS

The Convention recognises public-private partnerships as a means by which international and regional cooperation can be achieved.

**Article 26 (3):** Each State Party shall develop public-private partnerships as a model to engage industry, the civil society, and academia in the promotion and enhancement of culture of cyber security. **Article 28 (4):** State Parties shall make sure existing means for international cooperation with a view to responding to cyber threats, improving cyber security and stimulating dialogue between stakeholders. These means may be international, intergovernmental or regional, or based on private and public partnerships.

Benin, Morocco and Tunisia have implemented public-private partnerships to engage a range of stakeholders such as industry, civil society and academia on cooperation in the interests of cybersecurity.

LAWS AND REGULATIONS

Articles 3 to 7 of the Convention requires member states to enact Electronic Commerce laws and regulations that cater for contractual liability for providers providing goods/services by electronic means, advertising by electronic means, electronic contracts, electronic writing/signatures and guaranteeing the security of electronic transactions.

Additionally, Articles 10 to 23 of the Convention require member countries to have Data Protection laws and Regulations that provide for, amongst other things, the exemption or authorisation of the processing of personal data the composition, organisation, duties and powers of a National Personal Data Protection Authority, basic principles governing the processing of personal data, as well as, specific principles governing the processing of special/sensitive personal data and providing the data subjects with certain rights to their information and corresponding obligations on the data controllers.

Furthermore, the Convention stipulates that Cyber-crime laws and regulations should be provided for by member states. Such laws and regulations should provide for the criminalisation of cyber-crime (Article 25(1), 29), adaption of certain offences and sanctions for information and communication technologies infringements (Article 30); the conferring of statutory authority and legal capacity on a national regulatory authority responsible for all aspects of national cyber security (Article 25 (2) ), as well as, the protection of critical infrastructure (Article 25(4) ) and enhancement of regional harmonisation and international cooperation (Article 28).

Eight (8) countries (Benin, Chad, Guinea, Kenya, Mauritania, Morocco, Senegal and Tunisia) have enacted electronic transactions regulation and two (2) countries Congo and DRC have draft laws pending enactment.

On the subject of cybercrime laws and regulations eight (8) countries (Benin, Chad, Guinea, Kenya, Mauritania, Morocco, Senegal and Tunisia) have enacted cybercrime laws. Tunisia has progressed with a cybercrime draft law to supplement its penal code that is not yet available to the public and Congo and DRC have draft laws awaiting enactment.

From the above (visualised in Table 4 below), the majority of member states under study have prioritised the introduction of laws and regulations in the areas of data protection, cybercrime and electronic transactions. However, of the African Union member states that have laws and regulations in place, three member states have data protection, cybercrime and cybersecurity, and electronic transaction laws that are all outdated (dating from 2000 - 2008):

**Morocco:**
- Law 09/08 relating to the protection of individuals with respect to the processing of personal data;
- Law 53/05 relating to the electronic exchange of legal data;
- Law No. 07/03 supplementing the Penal Code with respect to offenses relating to automated data processing systems.

**Senegal:**
- Law No 2008/12 on the protection of personal data;
- Law No. 2008-08 on Electronic Transactions;
- Law No. 2008/11 on Cybercrime for the substantive and procedural aspects of cybercrime.

**Tunisia:**
- Law 2004/63 of 27th July 2004 relating to personal data protection;
- Law 2000/83 regarding electronic commerce;
- Law No. 2004/5 relating to electronic security and on the organisation of the field of computer security and setting the general rules for the protection of computer systems and networks.

Where member states have not enacted a law, draft laws are available (visualised in Table 5 below).

Of the ten (10) Country studied, nine (9) countries (Benin, Chad, Congo, Guinea, Kenya, Mauritania, Morocco and Senegal) have enacted data protection regulation and Tunisia has partial implementation. Only DRC is yet to enact a data protection law.
### Table 4: Member States Implementation Of Legislative And Regulatory Measures Required By The AUCC

<table>
<thead>
<tr>
<th>Countries</th>
<th>Benin</th>
<th>Chad</th>
<th>Congo</th>
<th>DRC</th>
<th>Guinea</th>
<th>Kenya</th>
<th>Mauritania</th>
<th>Morocco</th>
<th>Senegal</th>
<th>Tunisia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection</td>
<td>🟢</td>
<td>🟢</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data Protection Laws and Regulations</td>
<td>Arts 10-23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Transactions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Electronic Transactions/ Commerce Laws and Regulations</td>
<td>Arts 3-7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybercrime and Cybersecurity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cybercrime Laws and Regulations</td>
<td>Arts 25-30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<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>Art 25(4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 5: Draft Laws, Policies & Strategies Across The Member States

<table>
<thead>
<tr>
<th>Member State</th>
<th>Law/Policy/Strategy in Draft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benin</td>
<td>National Cybersecurity Strategy</td>
</tr>
<tr>
<td>Chad</td>
<td>National Cybersecurity Strategy</td>
</tr>
</tbody>
</table>
| Congo | The Draft law on Electronic Transactions  
The Draft Law on Cybersecurity  
The Draft Law on Cybercrime |
| DRC | Draft Electronic Transactions Bill  
Draft Telecommunications and ICT Bill  
Draft Decree establishing a CERT has been submitted for examination and adoption by the Council of Ministers |
| Kenya | Draft Policy Framework for the Protection of Critical Infrastructure  
Draft Information and Communications (Electronic Transactions) Regulations 2016  
Draft Information Communications (Cyber- security) Regulations 2016  
Draft Critical Infrastructure Bill, 2015 |
| Mauritania | National Strategy guideline for cyber security is under consideration |
| Tunisia | Cybersecurity Strategy (2020-2024)  
Draft Basic Law No. 2016/25 on the protection of personal data  
Draft Digital Code  
Draft Cybercrime Law |
INSTITUTIONAL MEASURES

To provide for enforcement of the aforementioned laws and regulation, in 3.3 above, the Convention requires that member states provide for institutional support. In terms of Article 12 member states are required to have a data protection authority whose responsibilities in regulating data protection include authorisation of data processing and authorisation of cross border transfers of personal data. Article 7 (3) (a) requires a member state to have an electronic signature accreditation authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications. Also, Article 7 provides that the member state is required to have a state department that is empowered to regulate and approve electronic commerce payment methods, whereby only approved payment methods may be validly used in the member state territory.


Benin, Chad, Congo, Guinea, Kenya, Morocco and Tunisia have established Electronic Signature Accreditation Authorities that regulate what constitutes a qualified electronic signature for the purpose of authenticating electronic records and other applications.

Benin, Chad, Congo, Guinea, Kenya, Mauritania, Morocco, Senegal and Tunisia have some institutional structures with the legal capacity to respond to cybersecurity incidents and facilitate cybersecurity coordination and cooperation.

Figure 1: African Union member states under study with established Cybersecurity Emergency Response Teams (CERT’s)
<table>
<thead>
<tr>
<th>Countries</th>
<th>Benin</th>
<th>Chad</th>
<th>Congo</th>
<th>DRC</th>
<th>Guinea</th>
<th>Kenya</th>
<th>Mauritania</th>
<th>Morocco</th>
<th>Senegal</th>
<th>Tunisia</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Protection</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Protection Authority whose responsibilities in regulating data protection include: authorisation of data processing, authorisation of cross border transfers of personal data. Arts 11-12</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Electronic Transactions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications. Art 7(3)(a)</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory. Art 7</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Cybercrime and Cybersecurity</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<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. Art 2.2</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<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. Art 25(2)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Countries</td>
<td>Benin</td>
<td>Chad</td>
<td>Congo</td>
<td>DRC</td>
<td>Guinea</td>
<td>Kenya</td>
<td>Mauritania</td>
<td>Morocco</td>
<td>Senegal</td>
<td>Tunisia</td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>------</td>
<td>-------</td>
<td>-----</td>
<td>--------</td>
<td>-------</td>
<td>------------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Cybercrime and Cybersecurity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation. Art 28</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs) Art 28</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
EMERGENCY RESPONSE MEASURES

Article 25 (2) of the Convention requires a member state to have an institution with the statutory authority and legal capacity to respond to cyber security incidents, co-ordination and co-operation for (cybersecurity) restorative justice, forensic investigations and cybersecurity prosecution. Moreover, Article 28 provides that there is a need for member states to have institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs).

Africa has had both successes and failures in the area of CERTs/ CIRTs. Tunisia, Egypt and Morocco have built effective CERTs. Sub-Saharan African countries were slower to join the progression. South Africa, Nigeria and Kenya are further examples of success. A measure of success is the ability of the newly created CERT to be accepted as a full member at the Forum for Incidence Response Teams (FIRST). The process has rigour. In addition to an application, the country applying requires two sponsors and to go through a review process to prove a certain level of competence. Tunisia was the first country in Africa to receive FIRST membership followed by Egypt, Morocco and three CERTs (associated with financial institutions) in South Africa. In 2015, Nigeria and Kenya became official members. Out of the 326 teams belonging to FIRST, so far, Africa has eight.

In this study and sample, five (5) of the ten (10) countries (Benin, Chad, Kenya, Morocco and Tunisia) have operational CERTs/CIRTs.

INTERNATIONAL COOPERATION

In terms of Article 28 of the Convention, member states should have institutions responsible for, not only national, but cross-border co-ordination of cyber-crime. Article 28 (1) provides that member states should ensure that there are legislative measures to provide for regional and international cooperation and harmonisation.

In 2009 the Beninese government drafted a Decree No. 200/MISP/DC/SGM/DGPN/SERCT/DER/SA related to the creation of a division responsible for the fight against cybercrime. The decree stipulates that the victims of internet crime can approach Interpol or the local authorities regarding the incidence of cybercrime. Further, Article 624 within Book Six of Benin’s Digital Code sets out mechanisms of international cooperation.

In Chad, Article 104 of its Draft Law on Fighting Cybercrime states that “the procedures for establishing cooperation agreements on cybersecurity and the fight against cybercrime shall be determined by regulation”, whilst Articles 105 – 106 of the same Draft Law details the procedures for mutual legal assistance between the Republic of Congo and foreign judicial authorities.

In Guinea, international cooperation on combatting cybercrime is mandated under Article 106 of Law 2016/037 on cybersecurity and the protection of personal data, whilst 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 participate in international cooperation efforts (including treaties, conventions etc) and overseeing their implementation within the Republic of Guinea.

In Kenya, provision for international cooperation in tackling cybercrimes is made under Part V of the Computer Misuse and Cybercrimes Act of 2018.

Mauritania is required to co-operate with any international country in the investigation/prosecution of cyber-criminal offences in terms of national reciprocal legislation and/ or international legal instruments under Article 50 of Law No. 2016/007 on cybercrime.

In Morocco, its National Cybersecurity Strategy (Stratégie nationale en Sécurité des Systèmes d’Information) considers the promotion of national and international cooperation as one of its strategic objectives.

---

4 ITU (2018) Global Cybersecurity Index (GCI)
Concerning data protection, six of ten (6/10) member states have a policy or strategy that considers data protection (Benin, Republic of Congo, Kenya, Mauritania, Morocco and Senegal), nine of ten (9/10) member states have instituted a law concerning data protection (Benin; Chad; Republic of Congo; Guinea; Kenya; Mauritania; Morocco; Senegal; and Tunisia), and seven of ten (7/10) member states have established a Data Protection Authority (Benin; Republic of Congo; Kenya; Mauritania; Morocco; Senegal; and Tunisia) – of the seven (7) Data Protection Authorities, only four (4) appear to be operational at the time of writing.

Concerning cybercrime and cybersecurity, five of ten (5/10) member states have a policy or strategy concerning cybercrime and cybersecurity (Kenya, Mauritania, Morocco, Senegal and Tunisia), eight of ten (8/10) member states have instituted a law concerning cybercrime and cybersecurity (Benin; Chad; Guinea; Kenya; Mauritania; Morocco; Senegal; and Tunisia), and five of ten (5/10) member states have established a Cybersecurity Emergency Response Team (CERT) (Benin, Chad, Kenya, Morocco and Tunisia) – however, all member states under study (with the exclusion of the DRC) have one or more alternative institutional measures in place responsible for responding to cybercrime and cybersecurity. Concerning electronic transactions, nine of ten (9/10) member states have a policy or strategy concerning electronic transactions (Benin; Congo; DRC; Guinea; Kenya; Mauritania; Morocco; Senegal and Tunisia), eight of ten (8/10) member states have instituted a law concerning electronic transactions (Benin; Chad; Guinea; Kenya; Mauritania; Morocco; Senegal; and Tunisia), and six of ten (6/10) member states have established an institution for electronic transactions (electronic signature and certification providers) (Benin; Chad; Republic of Congo; Morocco; Senegal and Tunisia).

The recap above (as visualised in Figure 3 below), indicates that cybercrime and cybersecurity institutional measures, as well as electronic transaction institutional measures, policies and strategies, are the weakest areas of implementation for the member states under study.
Of the African Union member states that have laws, policies & strategies in place, the analysis pointed to three (3) member states whose data protection, cybercrime and cybersecurity, and electronic transaction laws are all outdated (dating from 2000 - 2008) and require revision. Additionally, of the African Union member states that have laws, policies & strategies in place, Table 5 above indicated that seven (7) of the member states have laws, policies and/or strategies that are in draft.

RECOMMENDATIONS

NATIONAL LEVEL

Countries can accelerate the ratification and implementation of the Convention protection through for instance: developing the national strategies on cybersecurity and an operational action plan for combating cybercrime and cyber terrorism – several countries have guiding policies or policy statements.

- **Drafting or reviewing outdated legislative and regulatory frameworks:** Several countries laws on data protection, electronic transactions and cybercrime may be outdated;

- **Implement institutional frameworks provided for in legislative and regulatory frameworks:** Countries may have provisioned for a national protection authority but not implemented such an institution; and

- **Balanced interests in cybersecurity and human rights:** Countries should ensure that African citizens, represented by the continent’s civil society organisations, are part of the process and that all legislation adopted at the domestic level includes provisions on the rule of law and human rights.

Accordingly, at the national level we furthermore recommend that:

- **Member states prioritise strengthening weaker areas of implementation (policies, strategies and institutions), especially when considering that such areas are integral to the enforcement of laws that have already been enacted;**

- **Member states whose laws and regulations are outdated implement review procedures to assess the compatibility of their outdated laws and regulation against current data protection, cybercrime, cybersecurity and electronic transaction issues, as well as consider adaptability for the evolving cybersecurity landscape in emergent technologies;**

- **Member states whose laws, regulations, policies, strategies are in draft prioritise the passing of such laws; and**

REGIONAL LEVEL

- **Support legislative harmonisation at member state level:** At the regional level, several initiatives have focussed on developing regional model legislation in the three focus areas of the AUCC, related to data protection, electronic transactions and cybercrime. These include the ECOWAS Cybersecurity guidelines, the ECCAS Model Law/CEMAC Directives on Cybersecurity and the SADC Model Law on data protection, e-transactions and cybercrime. Regional support for national implementation of legislation including drafting of legislation, regulation that give effect to legislation and capacity building for institutions that have oversight of the legislation are needed.

CONTINENTAL LEVEL

- **Harmonised definitions of cybersecurity:** Global studies show that in developed and developing worlds, harmonised definitions of cybersecurity is a transversal issue. France for instance defines cybersecurity as “an information system allowing to resist likely events resulting from cyber space which may compromise the availability, the integrity or confidentiality of data stored, processed or transmitted and of the related services that Information and Communication (ICT) systems offer” (Luijff, Besseling & Spoelstra et al, 2013), whilst the UK views cybersecurity as “[embracing] both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers” (Luijff, Besseling & Spoelstra et al, 2013). The above comparison shows a distinction in where cybersecurity is located, a priority at the information system level or a priority at the national security level. Harmonised definitions of cybersecurity are needed at the continental level.

- **Baseline and Annual Statistics:** Both baseline data on cybersecurity legislative, policy and institutional measures and annual updates will be valuable in assessing successes and challenges and targeted support (at the continental level) for advancing such cybersecurity measures in Africa. The AUCC refers to monitoring and evaluation mechanisms to assess implementation – such mechanisms may provide the baseline and annual research needed.

---

7 SADC Model Law on data protection, e-transactions and cybercrime (2010).
It is recommended that at the continental level, guidance is provided to African Union member states on how to deal with competing requirements from the various regional, continental and instruments, particularly where such requirements may be in conflict with one another.

**Promote cybersecurity in the context of cyber stability:**

Cyber stability has been defined as “a geo-strategic condition whereby users of the cyber domain enjoy the greatest possible benefits to political, civic, social, and economic life, while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels” (Oriji, U.J. 2012). Continental bodies must promote cybersecurity in the context of its geostrategic character encompassing the many facets of benefits and harms permeating the various areas of life.

**Compatibility and Comparison with Other Models and Conventions:**

Over the course of the study, African Union Member States raised concerns relating to the compatibility of the provisions of the AUCC with the provisions of the Budapest Convention on Cybercrime, as well as compatibility with regional model laws and treaties.

In total, seven member countries have signed and ratified the Budapest Convention (Benin, Cabo Verde, Ghana, Mauritius, Morocco, Nigeria and Senegal). The Budapest convention was the first international effort to provide guidelines for countries to develop their national legislation and establish a framework for international cooperation.

Regional models include the ECOWAS Cybersecurity guidelines, the ECCAS Model Law/CEMAC Directives on Cybersecurity and the SADC Model Law on data protection, e-transactions and cybercrime.

[ banging ]

It is recommended that at the continental level, guidance is provided to African Union member states on how to deal with competing requirements from the various regional, continental and instruments, particularly where such requirements may be in conflict with one another.

**Promote cybersecurity in the context of cyber stability:**

Cyber stability has been defined as “a geo-strategic condition whereby users of the cyber domain enjoy the greatest possible benefits to political, civic, social, and economic life, while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels” (Oriji, U.J. 2012). Continental bodies must promote cybersecurity in the context of its geostrategic character encompassing the many facets of benefits and harms permeating the various areas of life.

**Compatibility and Comparison with Other Models and Conventions:**

Over the course of the study, African Union Member States raised concerns relating to the compatibility of the provisions of the AUCC with the provisions of the Budapest Convention on Cybercrime, as well as compatibility with regional model laws and treaties.

In total, seven member countries have signed and ratified the Budapest Convention (Benin, Cabo Verde, Ghana, Mauritius, Morocco, Nigeria and Senegal). The Budapest convention was the first international effort to provide guidelines for countries to develop their national legislation and establish a framework for international cooperation.

Regional models include the ECOWAS Cybersecurity guidelines, the ECCAS Model Law/CEMAC Directives on Cybersecurity and the SADC Model Law on data protection, e-transactions and cybercrime.

---

MEMBER STATE NATIONAL ASSESSMENTS

Introduction

The National Assessments assess National Cyber Security policy, regulation and frameworks of select African Union member states. The primary aim of the assessment is to analyse and compare the different cyber security policy, legislative and institutional approaches outlined in the respective countries with the approaches in the African Union Cybersecurity Convention and Personal Data Protection (AUCC), in order to better understand the gaps between the country’s cybersecurity governance and the requirements of the Convention.

Ten (10) National Assessment Reports on selected African Union member states were compiled during this study. These African Union member states include:

1. Benin;
2. Chad;
3. Republic of Congo;
4. Democratic Republic of Congo;
5. Guinea;
6. Kenya;
7. Mauritania;
8. Morocco;
9. Senegal; and
10. Tunisia.

Annexure “A” of this Report sets out a list of the fifty-five (55) African Union member states with which we selected to first ten (10) African Union member states for study. The selected member states were chosen based on several factors including:

 países that have signed and/or ratified the AU Convention;
 países with representatives in the PAP Committee on Transport, Industry, Telecommunications, Energy, Science and Technology which is collaborating with AUDA-NEPAD on the Cybersecurity project;
 países that are recognised ICT leaders within their respective regions (for benchmarking); and
 países Regional and geographic balancing.

Structure of the National Assessment Reports

The structure for the National Assessment Reports that follow was developed in accordance with the scope of the AUCC. Accordingly, each National Assessment is divided into three sections, namely:

1. Data Protection;
2. Cybercrime and Cybersecurity; and
3. Electronic Transactions.

Under cover of each of the above sections, the Laws and Regulations; Policies and Strategies; and Institutional Measures were assessed.
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 (bjCSIRT).

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
Articles 425 and 426, respectively, set out confidentiality and security obligations on data controllers. Storage obligations on data controllers are laid out under Article 433.

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 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 Book 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/DGPN/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:

1. The Government of Benin launched a cyber security campaign focused on the country’s youth – known as the Internet of Sensitization to Youth;”
2. The Government of Benin works with various Non-Governmental Organizations (NGOs) and civil society organizations in order to increase overall cyber security awareness.”
3. 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.”
4. “The Government of Benin also takes part in a number of Confidence Building Measures (CBM) through international meetings and cooperates in international cyber security 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:

1. 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.
2. 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:

1. Book Two governs ‘electronic writing’ (Title I) and ‘electronic signatures’ (Title III); and
2. 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:

1. Electronic writing is given legal validity under Article 266;
2. Electronic signatures are regulated under Title III, including provisions on qualified electronic signatures (Article 287) and qualified validation services electronic signatures (Article 291); and
3. 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] development 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 8: Benin National Assessment Overview

<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;The Digital Code (Book 5).</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;Autorité de Protection des Données à caractère Personnel (APDP).</td>
</tr>
<tr>
<td><strong>National Cybersecurity strategy to implement the Policy</strong></td>
<td><strong>Electronic Commerce Laws and Regulations</strong>&lt;br&gt;The Digital Code (Book 2 and 4).</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;National Signing Certification Authority (L’autorité de certification signataire nationale).</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>Cybercrime Laws and Regulations</strong>&lt;br&gt;The Digital Code (Book 6).</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 Ministry of Digital and Digitalization</td>
</tr>
<tr>
<td>Benin has engaged in various public-private partnerships to enhance cybersecurity awareness.</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;The Digital Code.</td>
<td><strong>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</strong>&lt;br&gt;National Agency for Security Information Systems (ANSSI)</td>
</tr>
<tr>
<td><strong>No dedicated Cybersecurity policy.</strong></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 Agency for Security Information Systems (ANSSI)</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 bjCSIRT</td>
</tr>
<tr>
<td><strong>National Cybersecurity strategy to implement the Policy</strong></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;The bjCSIRT</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 bjCSIRT</td>
</tr>
</tbody>
</table>
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 electric 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).
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.

The African Union Convention on Cybersecurity and Personal Data

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

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></td>
<td><strong>Data Protection Laws and Regulations</strong>&lt;br&gt;Law No. 007/PR/2015 on the Protection of Personal Data</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</td>
</tr>
<tr>
<td><strong>National Cybersecurity strategy to implement the Policy</strong></td>
<td><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>No Data Protection Authority. However, there is a Directorate for the Protection of Privacy and Freedoms in the Cyberspaces</strong></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>Cybercrime Laws and Regulations</strong>&lt;br&gt;Law 009 / PR / 2015 of 10 February on Cyber Security and the Fight against Cybercrime</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</td>
</tr>
<tr>
<td><strong>N/A</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></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>;</td>
</tr>
<tr>
<td><strong>N/A</strong></td>
<td><strong>Law 006/PR/2015 About the Creation of the National Agency for Computer Security and Electronic Certification</strong></td>
<td><strong>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</strong></td>
</tr>
<tr>
<td><strong>N/A</strong></td>
<td><strong>State Department to regulate vulnerability and security assessments of suppliers of ICT products, including ensuring mandatory disclosure of vulnerabilities and solutions to these suppliers</strong></td>
<td><strong>The Regulatory Authority for Electronic Communications and Post</strong></td>
</tr>
<tr>
<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></td>
<td><strong>The Security Directorate of Electronic Communications Networks and Information Systems (ANSICE) operates an anti-cyber crime unit.</strong></td>
<td><strong>The Director of Expertise and Security Technology Watch</strong></td>
</tr>
<tr>
<td><strong>Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.</strong></td>
<td><strong>The Director of Electronic Transaction Security and Electronic Certification.</strong></td>
<td><strong>The National State Security Agency.</strong></td>
</tr>
<tr>
<td><strong>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</strong></td>
<td><strong>The Security Directorate of Electronic Communications Networks and Information Systems (ANSICE)</strong></td>
<td><strong>The Security Directorate of Electronic Communications Networks and Information Systems (ANSICE)</strong></td>
</tr>
</tbody>
</table>
3. REPUBLIC OF CONGO

Regional Economic Community: Economic Community of Central African States (ECCAS)
Population: 5 542 197
Internet Penetration: 650 000 users i.e. 11.7% of the population.
AUCC Ratification Status: Signed 12/06/2015

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 TRANSACTIONS: 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, entrenching 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 (DGDEN) 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 cryptology 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 Ibombo 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 Transfrontalieres (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>
</table>
| **Cybersecurity Policy which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures** | **Data Protection Laws and Regulations**  
Data protection Law No 29/2019  
Electronic Commerce Laws and Regulations  
Draft law on Electronic Transactions..  
**Cybercrime Laws and Regulations**  
The Draft Law on Cybersecurity;  
The Draft Law on Cybercrime; and  
Law 30/2019 establishing the National Agency of Information Security. | Data Protection Authority whose responsibilities in regulating data protection include authorisation of data processing, authorisation of cross border transfers of personal data  
National Personal Data Protection Commission.  
Electronic Signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications  
Autorite De Certification Des Echanges Electroniques Au Congo.  
The State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;  
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 |
| **National Cybersecurity strategy to implement the Policy** | **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** | 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  
National Information Systems Security Agency - a special branch within the National Police tasked with investigating cybercrimes and enforces crime laws.  
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)  
National Cybersecurity Agency of the Republic of Congo;  
Centre for Computing and of Research of the Army and of Security  
(No CERT) |
4. DEMOCRATIC REPUBLIC OF CONGO

Regional Economic Community: Economic Community of Central African States (ECCAS)
Population: 86 727 537
Internet Penetration: 745 917 users i.e. 8.6% of the population.
AUCC Ratification Status: N/A

4.1. OVERVIEW

DATA PROTECTION: The DRC does not have a dedicated data protection law. The DRC does not have a national policy on data protection. The DRC does not have a dedicated data protection authority.

ELECTRONIC TRANSACTIONS: The DRC does not have a dedicated national electronic transaction law in force but relies on the revised OHADA Uniform Law, 2010. A draft E-Transactions Bill exists. The DRC has drafted the policy “Digital Horizon 2025” which applies to electronic commerce.

CYBERCRIME AND CYBERSECURITY: The DRC does not have specific legislation for cybercrime and cybersecurity. The DRC does not have a National Cybersecurity Strategy. The institution responsible for cybercrime and cybersecurity in the DRC is the Ministry of Telecommunications and New Technologies. A CERT has not been established.

4.2. DATA PROTECTION

4.2.1. Overview of Data Protection Legislation


The 2006 Constitution

Article 31 of the DRC’s Constitution guarantees the right to privacy to every DRC citizen:

“Everyone has the right to respect for privacy and confidentiality of correspondence, telecommunications or any other form of communication. This right cannot be infringed only in cases provided by law.”

The 2002 Framework Law

The 2002 Framework Law contains various provisions concerning the protection of personal data. These are described hereunder:

Article 21 (b) of the 2002 Framework Law requires that telecom operators are subject to confidentiality and neutrality regarding the content of messages exchanged by their clients.

Articles 52 and 53 of the 2002 Framework Law concern the secrecy/confidentiality of correspondences emitted by way of telecommunications:

- Article 52 provides for confidentiality protections on correspondence transmitted through communications in the DRC. The confidentiality of correspondence can only be lifted in cases where it is strictly in the public interest as provided by the law.

- Article 53 reinforces confidentiality of communications. “The public operator, operators of utility, telecommunications and other providers of telecommunications services and members of their staff are required to respect the confidentiality of communications.”

Articles 54 (Section A) and 55 of the 2002 Framework Law: prohibits any form of surveillance on citizens’ communication, even by security agents, without prior authorisation from the General Prosecutor of the Republic. However, Articles 54(a) and 55 provides for the interception of communications in two scenarios:

- In the context of judicial cases where authorisation has been granted by the Attorney General of the Republic (“Attorney General”); and

- Interceptions authorised by the Minister of the Interior concerning national security, protection of the essential elements of the scientific, economic and cultural potential of the country, or the prevention of crime and organised crime.

Article 54(a) prohibits the interception, phone-tapping, recording, transcription and disclosure of correspondence issued via telecommunications without the prior permission of the Attorney General. Article 55 addresses evidence and states that for the purpose of providing evidence in a court of law, the Attorney General must order the interception, recording and transcription of correspondence transmitted through telecommunications.

Article 59 of the 2002 Framework Law requires that interceptions authorised by the Minister of the Interior must have a purpose to: (i) seek information relating to national security; (ii) protect the essential elements of the cultural, scientific or economic potential of DRC; or (iii) prevent crime and organized crime.

**Law 14/2002 on the Regulator**

The Law 14/2002 on the Regulator establishes the regulatory body - Autorite de Regulation de la Poste et des Telecommunications du Congo known as the Authority of the Post and Telecommunications of Congo (ARPTC) - grants the right for the government, specifically the legislature, to “conduct site visits, conduct investigations and studies, and collect all the necessary data” from telecom service providers. This Law authorises the government to “collect all necessary data” from telecommunications companies when needed.

**The Telecommunications and ICT Bill**

Notably, a Telecommunications and ICT Bill (the “ICT Bill”) exists in draft which is aimed at revamping the Framework Law. The Telecommunications and ICT Bill will be known as the Telecommunications and ICT Framework when passed. In September 2019, the Telecommunications and ICT Bill was sent back from the office of the President for a further reading to remedy certain provisions.

Whilst the ICT Bill is not limited to data protection, it provides for the protection of the confidentiality of personal data, as stated in paragraph 1 of Article 125. Criticisms of the Bill, insofar as data protection and privacy are concerned, have included:

- The lack of “written consent” required from data subjects regarding the processing of their personal information; and
- Exclusions allowing the State to derogate from the confidentiality of correspondence under the Bill for reasons of internal and/or external security of the State, national defence or public order.

The ICT Bill also includes protections for the privacy of users in cases of cyber-attacks.

**Other Draft Laws in Existence**

Apart from the Telecommunications and ICT Bill, a Bill amending the Act that set up the regulator – the Authority of the Post and Telecommunications of Congo (ARPTC) - is in existence but is yet to be passed (CIPESA, 2017).

4.2.3. Data Protection Institutional Measures

4.3. Cybercrime and Cybersecurity

4.3.1. Overview of Cybercrime and Cybersecurity Legislation

There is currently no specific legislation for cybercrime and cybersecurity in force. However, the Democratic Republic of Congo has drafted the Telecommunications and Information Communications Bill (The “ICT Bill”).

**The Telecommunications and ICT Bill**

The ICT Bill exists in draft and is aimed at revamping the Framework Law. The Telecommunications and ICT Bill will be known as the Telecommunications and ICT Framework when passed. In September 2019, the Telecommunications and ICT Bill was sent back from the office of the President for a further reading to remedy certain provisions.

Whilst the ICT Bill is not limited to cybercrime and cybersecurity, its provisions define cybercrime and provide for sanctions against the perpetrators of cybercrimes. Under the ICT Bill, ‘cybercrime’ is broadly defined as the set of offences committed employing computers or targeting them. It is also the set of offences committed against or by a computer system carried out through a telecommunications network. More simply, cybercrime is conceived as an act of intrusion for the theft, control or destruction of computer systems or databases. These may include methods of forcing access to a remote computer, modifying data and files, or implementing malicious programs on servers.

The ICT Bill has, however, been criticised for lacking enough provisions regarding cybercrime and cybersecurity.

4.3.2. Cybercrime and Cybersecurity Policy Developments

The Democratic Republic of Congo does not have a National Cybersecurity Strategy in place. A workshop was, however, organized in Kinshasa in August 2015 that assisted the country in raising awareness of cybercrime. To date, the government has not been greatly involved in working with the private sector on cybersecurity issues (African Union, Symantec, 2016).

Quoting from the Report:

“One of the biggest obstacles facing cyber security advancement in the DRC is that training remains a major obstacle. In addition, the authorities noted, computers and an internet connection are not accessible to most of the population in the first place” (African Union, Symantec, 2016, 67).
4.3.3. Cybercrime and Cybersecurity Institutional Measures

The primary institution relating to cybercrime and cybersecurity in the DRC is the Ministry of Telecommunications and New Technologies. This Ministry is responsible for cybersecurity and cybercrime-related efforts in the DRC.

At the time of writing, the DRC does not have any institutional mechanisms for responding to cyber incidents, including a CERT or other national-level cybersecurity infrastructure. Saying that, the establishment of a CERT has nonetheless been evaluated in the DRC (African Union, Symantec, 2016) and a draft decree establishing a CERT has been submitted for examination and adoption by the Council of Ministers. The strategies, operation and effective implementation of the CERT are already the subject of two bills under discussion in Parliament.

There is a plan to set up a national strategy as well as a roadmap for the effective implementation and actual operation of this centre. As at March 2019 according to the ITU, there is still no CIRT established (ITU, 2019).

4.4. ELECTRONIC TRANSACTIONS

4.4.1. Overview of Electronic Transactions Legislation

The Democratic Republic of Congo does not have a dedicated national electronic transactions law in place. Instead, it primarily relies on the revised OHADA Uniform Law, 2010 to regulate its electronic transactions and e-commerce sphere.

**OHADA Uniform Law, 2010**

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.

The OHADA (Organization for Harmonization of Business Law) is the French Commercial Law common to all Francophone countries and serves as the country’s commercial law - subject to specific Congolese laws. 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.

**The Telecommunications and ICT Bill**

Notably, a Telecommunications and ICT Bill (the “ICT Bill”) exists in draft which is aimed at revamping the Framework Law (No. 013/2002 of 16 October 2002). The Telecommunications and ICT Bill will be known as the Telecommunications and ICT Framework when passed. In September 2019, the Telecommunications and ICT Bill was sent back from the office of the President for a further reading to remedy certain provisions. The ICT Bill is unavailable for public consumption as of writing and cannot be assessed further.

**Law No 86/033**

Law No. 86/033 of 5 April 1986 on the Protection of Copyright and neighbouring Rights provides the basis for the protection of e-commerce Intellectual Property Rights (IPR).

**Draft E-Transactions Bill**

4.4.2. Electronic Transactions Policy Developments

A validation Workshop was concluded on 5 September 2019 for the Digital National Plan of the Democratic Republic of Congo (DRC) – known as "Digital Horizon 2025", which constitutes the primary policy relating to electronic transactions and electronic commerce in the Democratic Republic of Congo.

The workshop aimed to "modernize the administration and pool resources and infrastructure to achieve significant gains in terms of efficiency and effectiveness; enable citizens and businesses to interact online with the public administration and partners; to provide users with better quality services that reduce costs and deadlines with the additional guarantee of maximum transparency" (H2T, 2019).

The National Plan was validated by various stakeholders in the DRC’s digital sector. The closing ceremony was attended by the Minister of Posts, Telecommunications and New Information Technologies and Communication, Emery Okudji, who represented the Head of State in the DRC, Felix Tshisekedi (H2T, 2019).

The national digital plan will be comprised of four core pillars, namely:

- infrastructure;
- production and hosting of content;
- application uses; and
- governance and regulation.

4.4.3. Electronic Transactions Institutional Measures
4.5. COMPARISON WITH THE AUCC PROVISIONS ON LAWS, POLICIES AND INSTITUTIONS FOR DATA PROTECTION, CYBERCRIME AND ELECTRONIC TRANSACTIONS.

Table 11: DRC National Assessment Overview

<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></td>
<td><strong>Data Protection Laws and</strong></td>
<td><strong>Data Protection Authority</strong> who regulates data protection include authorisation of data processing, authorisation of cross border transfers of personal data</td>
</tr>
<tr>
<td>which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures</td>
<td><strong>Regulations</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>No Cybersecurity Policy.</td>
<td><strong>Electronic Commerce Laws and</strong></td>
<td><strong>Electronic Signature Accreditation Authority</strong> who regulates qualified electronic signature for the purposes of authenticating electronic records and other applications</td>
</tr>
<tr>
<td><strong>National Cybersecurity strategy to implement the Policy</strong></td>
<td><strong>Regulations</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>The Democratic Republic of Congo does not have a National Cybersecurity Strategy in place.</td>
<td><strong>Cybercrime Laws and</strong></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></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>Regulations</strong></td>
<td><strong>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</strong></td>
</tr>
<tr>
<td>No dedicated data protection law.</td>
<td><strong>Legislative and regulatory</strong></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></td>
</tr>
<tr>
<td><strong>Electronic Commerce Laws and</strong></td>
<td>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><strong>Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.</strong></td>
</tr>
<tr>
<td><strong>Regulations</strong></td>
<td>N/A</td>
<td>The Ministry of Telecommunications and New Technologies is responsible for cyber security and cybersecurity-related efforts in the DRC.</td>
</tr>
<tr>
<td><strong>Cybercrime Laws and</strong></td>
<td><strong>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</strong></td>
<td>A draft decree establishing a CERT has been submitted for examination and adoption by the Council of Ministers.</td>
</tr>
<tr>
<td><strong>Regulations</strong></td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
5. GUINEA

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):

1. 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));

2. Collection, recording, processing, storage, transmission and interconnection of personal data files, must be to do so lawfully and fairly;

3. Personal data must be collected for specified, explicit and legitimate purposes and cannot be subsequently inconsistent with those purposes;

4. The data collected must be accurate and, if necessary;

5. Transparent: The principle of transparency implies mandatory and clear information on behalf of the data controller; and

6. 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 relating to information and communications technology 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.

**Data Protection**

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).
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/SSG/2016 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 telecommunication 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 telecommunication 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 12: Guinea National Assessment Overview

<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&lt;br&gt;Law 2016/037.</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>The National Cybersecurity Strategy, Policy and Roadmap.</td>
<td>Electronic Commerce Laws and Regulations&lt;br&gt;Law 2016/035 on Electronic Transactions.</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>National Cybersecurity strategy to implement the Policy</td>
<td>Cybercrime Laws and Regulations&lt;br&gt;Governed by Law 2016/037.</td>
<td>The Authority for the Regulation of Post and Telecommunications (ARPT).</td>
</tr>
<tr>
<td>Guinea does not have a strategy yet, but a committee has been established to develop one.</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 electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;</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></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>The Authority for the Regulation of Post and Telecommunications (ARPT).</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>The Ministry of Planning and International Cooperation.</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>
</tbody>
</table>
6. KENYA

Regional Economic Community: East African Community (EAC)
Population: 52,214,791
Internet Penetration: 46,870,422 users i.e. 89.9% of the population
AUCC Ratification Status: N/A

6.1. OVERVIEW

DATA PROTECTION: Kenya has a data protection law (the Data Protection Act, 2019). Kenya has a Policy and Regulatory Framework for Privacy and Data Protection, as well as various other ICT Policies. The Office of the Kenyan Data Commission has been established.

ELECTRONIC TRANSACTIONS: Kenya has a law governing electronic data (The Kenya Information and Communications Act, 2015 – as amended), Electronic Transactions Regulations, 2016 and a draft Information and Communications (Electronic Transactions) Bill, 2018. Kenya has a Whitepaper on Facilitation And Adoption of E-Commerce Via The Postal/Courier Networks and a National ICT Policy and Masterplan. The Communications Authority of Kenya is empowered to authorise an entity to provide electronic certification services in Kenya. Kenya also has an ICT Authority and a Root Certification Authority.

CYBERCRIME AND CYBERSECURITY: Kenya has a cybercrimes law (The Computer Misuse and Cybercrimes Act of 2018), as well as a Draft Critical Infrastructure Bill, 2015. Kenya has a National Cyber Security Strategy (2014) and a Critical Infrastructure Information Policy, 2016 in addition to other policies. Kenya has a CERT (KE-CIRT/CC), a National Computer and Cybercrimes Co-Ordination Committee and a ICT Authority. A Critical Infrastructure Protection Committee and a Critical Infrastructure Protection Unit will be established under the Draft Critical Infrastructure Bill.

6.2. DATA PROTECTION

6.2.1. Overview of Data Protection Legislation

At a Constitutional level, Article 31 of the Kenyan Constitution specifically protects the right to privacy. Thereunder, all persons have the right to privacy, including the rights not to have information relating to their family or private affairs unnecessarily required or revealed (Section 31(c)); or the privacy of their communications infringed (Section 31(d)).

Previously (up until November 2019), personal data protection in Kenya was not governed by a dedicated data protection law (despite two Data Protection Bills having been submitted to Kenya’s Senate, and Parliament, respectively). Instead, the confidentiality of data was catered for under a patchwork of sectoral laws. For example (KICTAnet, 2019):

- Personal financial information is protected through confidentiality requirements under the Kenya Banking Act, Credit Reference Bureau Regulations and Capital Markets Act;
- The Kenya Access to Information Act and the Public Archives and Documentation Service Act also have internal protections for the safeguarding of personal information; and
- The Kenya Information and Communications Act (KICA); the Kenyan Information and Communications (Amendment) Bill, 2019; Private Security Regulation Act; and the Elections (Technology) Regulations, 2017 also cater for protection of personal data in certain instances.

The Data Protection Act, 2019

It is positive to note that on 8 November 2019 the Kenyan Data Protection Act, 2019 was signed into law (“the DPA”). The DPA codifies the right to privacy enshrined under Article 31 of the Kenyan Constitution.

The Office of the Kenyan Data Commission is established under Section 5 of the DPA, whereas its functions and powers are set out under Sections 7 and 8. Interestingly, unless an exception applies under the DPA, all Data Controllers and Data Processors are to be registered with the Kenyan Data Commissioner – as per Section 21 of the DPA.

Obligations on Data Controllers are listed under Part IV of the DPA and include:

- a duty to notify under (Section 29);
- mandatory data protection impact assessments under certain circumstances (Section 31); and
- the implementation of appropriate technical and organisational measures which are designed to implement the data protection principles effectively, and to integrate necessary safeguards for that purpose into the processing.
The DPA does not, however, contain a direct confidentiality obligation for Data Controllers and Data Processors. Instead, confidentiality and security obligations are contained indirectly under the duty to notify where data controllers are required to provide data subjects with “a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data”. Further, Section 25(a) of the Bill requires every data controller and data processor to “process personal data in accordance of the right of privacy of the data subject”.

Data retention requirements are provided for under Section 39.

The basic principles governing the processing of personal data are listed under Section 25 and require that personal data be:

- (a) processed in accordance with the right to privacy of the data subject;
- (b) processed lawfully, fairly and in a transparent manner;
- (c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- (d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
- (e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
- (f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
- (g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
- (h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

The general principles and obligations for processing personal data are contained within Chapter IV of the DPA. Thereunder, data collection requirements, notification duties, lawful bases for the processing of personal data, and conditions for consent and regulated amongst other things.

The appointment of a data protection officer is envisaged under the DPA; however, it is voluntary and not mandatory.

Data Subject rights provided for under the DPA include:

- The right to be informed - Section 26(a);
- The right of access - Section 26(b);
- The right to object - Section 26(c);
- The right to correction of false or ‘misleading’ data - Section 26 (d);
- The right to deletion of false or ‘misleading’ data - Section 26 (3);
- The right to request the restriction on the processing of data – Section 34;
- The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affecting the data subject – Section 35; and
- The right to data portability (sustainability of data) – Section 38.

Worryingly, the right to correction and deletion of data is limited to ‘misleading’ data. This may be argued to confer an unreasonable onus on Data Subject’s to prove that data is ‘misleading’.

The processing of special/sensitive personal data is regulated under Chapter V (Sections 44-47). Thereunder, a general prohibition on the processing of sensitive personal data exists. However, the prohibition ceases to exist where any of the grounds for lawful processing under Section 25 of the DPA are present, or where permitted grounds for the processing of sensitive personal data exist under Section 45.

Furthermore, Section 33 of the DPA regulates the processing of personal data belonging to children, requiring that:

- consent is given by the child’s parent or guardian – Section 33(1)(a);
- the processing is in such a manner that protects and advances the rights and best interests of the child – Section 33(1)(b); and
- appropriate mechanisms for age verification and consent in order to process personal data of a child be incorporated – Section 33(2)-(3).

Finally, exemptions for the processing of personal data are contained under Part VII (Sections 51-55):

- General exemptions are provided for under Section 51;
- Journalism literature and art under Section 52;
- Research, history and statistics under Section 53;
- Exemptions by the Data Commissioner under Section 54; and
- Data-sharing code under Section 55.

International Conventions

Kenya has signed/ratified the following internal legal instruments:

- the Universal Declaration of Human Rights (UDHR) (signed); and
- the International Covenant on Civil and Political Rights (ICCPR) (ratified).
6.2.2. Data Protection Policy Developments

The Cabinet Secretary, Ministry of Information, Communications and Technology through Gazette Notice Number 4367 of 11th May 2018 constituted a Taskforce to develop the Policy and Regulatory Framework for Privacy and Data Protection in Kenya. The proposed Policy will give effect to Article 31 of the Constitution of Kenya, by presenting legislative proposals and recommendations for stakeholder consultation with the object of developing the draft policy and legislation for privacy and data protection. (Privacy International, 2019). The primary objectives of the policy are to:

- inform the development of Privacy and Data Protection laws and facilitate statutory and regulatory compliance, and enhance the effective application of the proposed laws in Kenya;
- comply with the international good practice and ensure consistency in practices and procedures in developing and administering the Privacy and Data Protection laws;
- ensure effective protection and management of Personal Data by identifying, assessing, monitoring and mitigating privacy risks in programs and activities involving the collection, retention, use, disclosure and disposal of Personal Data;
- establish the required institutional framework for privacy and data protection; and
- protect children and vulnerable groups.

Other notable policy instruments relating to data protection and privacy are:

- ICT Authority Strategic Plan (2013-2018) – Roadmap for the transformation of Government ICT services;
- National ICT Masterplan (2014-2017) – Blueprint towards transforming Kenya into a digital economy and regional ICT hub; and
- The National ICT Policy.

6.2.3. Data Protection Institutional Measures

The following institutions are relevant to Data Protection in Kenya:

- The Kenyan Data Protection Commissioner: The Commissioner will be responsible for enforcing the provisions of Kenya’s future data protection law.
- The Data Protection Taskforce: The Taskforce was appointed by the Cabinet Secretary to formulate the Kenyan Privacy and Data Protection Policy.

6.3. CYBERCRIME AND CYBERSECURITY

6.3.1. Overview of Cybercrime and Cybersecurity Legislation

Cyber security and crimes associated therewith in Kenya are primarily governed by the following laws/legal instruments:

- The Computer Misuse and Cybercrimes Act of 2018 (the “Cybercrimes Act”);
- The Draft Information Communications (Cyber-security) Regulations 2016 (“the Cybersecurity Regulations”);
- The Draft Critical Infrastructure Bill, 2015 (the “CIB”)
- The Kenya Information Communication Act, 2012 (the “KICA”) and the Regulations thereto; and
- The Kenyan Penal Code.

The KICA Act

The KICA and its regulations had criminalised several cybercrimes. Its provisions have been now been superseded by the Cybercrimes Act.

The Cybercrimes Act

The Cybercrimes Act was introduced as the primary legislation establishing a statutory cyber authority and criminalising cyber offences. The Act repealed various provisions from the KICA. Before detailing its provisions below, it is imperative to note that on 29 May 2018, the High Court of Kenya issued a conservatory order suspending the entry into force of 26 sections of the Cybercrimes Act – these are Sections: 5, 16, 17, 22, 23, 24, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 48, 49, 50, 51, 52 & 53. The judgment on the constitutionality of the Computer Misuse and Cybercrimes Act 2018 was initially set to be heard on 30th January 2020 (Itimu, 2019). However, judgment in the matter was postponed for a second time to 20 February 2020. On 20 February 2020, Judge James Makau of the Kenyan High Court declared the Cybercrimes Act constitutional in its entirety (Shiwalo and Vilita, 2020).

Part II of the Cybercrimes Act establishes the National Computer And Cybercrimes Co-Ordination Committee (the “NCACCC”) whose functions include designating certain systems as ‘critical infrastructure’ (Section 9) under certain circumstances - listed in Section 9(2). The NCACCC is also responsible for regulating the minimum physical and technical security measures that must be implemented to protect critical information infrastructure. The NCACCC has statutory authority and legal capacity to conduct investigations and enforce the provisions of the Cybercrimes Act – in terms of Part IV of the Cybercrimes Act.
Part III of the Cybercrimes Act sets out a vast range of cyber offences between Sections 14-46 (32 cyber offences in total). The range of offences adapts certain sanctions and offences to Information and Communication Technologies – these include:

- The fraudulent use of electronic data (Section 37) which is wide enough to include the causing of damage to intellectual property in an electronic form;
- Issuance of false e-instructions (Section 39);
- Employee responsibilities to relinquish access codes (Section 41); and
- Cybersquatting (Section 27) and Cyber Harassment (Section 28).

Lastly, Part V of the Cybercrimes Act lays the ground for international cooperation in tackling cyber-crimes. And it sets up a crime reporting database. Any person who has information about a threat, attempt or actual cyber-attack is now legally obliged to share this with the database within 24 hours of the incident. If they don’t, they’re liable for a fine or could be jailed for up to two years.

The Cybercrimes Act has been criticised for having the potential to prejudice citizens and curb freedom of expression due to poorly defined offences such as that of ‘fake publications’.

**The Cybersecurity Regulations**

The Cybersecurity Regulations provides for various cyber offences and cyber penalties. However, in light of the Cybercrimes Act, the 2016 Cybersecurity Regulations have been superseded.

**The CIB**

On 27th March 2015, the then Cabinet Secretary in the Ministry of Information and Communications Dr Fred Matiang’i appointed a task force to formulate the Critical Infrastructure Policy, 2016 and the CIB. The CIB is a dedicated Bill providing for the protection of critical infrastructure in Kenya.

**6.3.2. Cybercrime and Cybersecurity Policy Developments**

The primary policy developments relating to cybersecurity and cybercrime in Kenya are:

- The Critical Infrastructure Information Policy, 2016; and
- Vision 2030;
At the outset, it is interesting to highlight that the term ‘electronic transaction’ is not defined under the KICA. However, the terms “data”, “electronic” and “electronic form” are defined which may be coupled to cater for electronic transactions.

Part II of the KICA establishes the Communications Authority of Kenya (the “CA”). Part VI-A of the KICA contains provisions relating to electronic transactions. Thereunder, the CA has statutory functions to guarantee the security of electronic transactions which include:

- “facilitate electronic transactions… by ensuring the use of reliable electronic records” - Section 83C(1)(a);
- “facilitate electronic commerce and eliminate barriers to electronic commerce such as those resulting from uncertainties over writing and signature requirements” - Section 83C(1)(b); and
- “[fostering] the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium” - Section 83C(1)(d).

Electronic Contracts: Section 83J of KICA states that an offer and acceptance may be expressed by means of electronic messages. Thus, where electronic messages are used in the formation of a contract, the contract shall not be denied validity or enforceability solely on the ground that an electronic message was used.

Importantly, Section 83B states that the creation or execution of a will; negotiable instruments; and documents of title may not be concluded electronically.

Electronic Certificates and Signatures: Section 83E of the KICA empowers the CA to authorise an entity to provide electronic certification services. On this note, electronic writing is given legal recognition under Section 83G of the KICA. Electronic signatures are given legal recognition under Section 83P and electronic messages and the parties to these messages are given legal recognition under Section 83K.

Electronic Advertising: Electronic advertising is partially catered for under the KICA. Thereunder, responsibilities on ‘broadcasters’ (TV/Radio providers) include “[ensuring] that advertisements, either in terms of content, tone or treatment, are not deceptive or are not repugnant to good taste”.

Contractual liability for providers who provide goods/services by electronic means is established under the ET Regulations. Unfortunately, a copy of these Regulations is not available in the public domain at the time of writing.

Direct marketing is not regulated under the KICA. Instead, the DPA regulates direct marketing under Section 37.

The following policies and strategies apply to electronic commerce and electronic transactions in Kenya.

- ICT Authority Strategic Plan (2013-2018) – Roadmap for the transformation of Government ICT services;
- National ICT Masterplan (2014-2017) – Blueprint towards transforming Kenya into a digital economy and regional ICT hub; and
- The National ICT Policy.

The Whitepaper On Facilitation And Adoption Of E-Commerce Via The Postal/Courier Networks was developed by the Kenyan CA in 2015. The Whitepaper was developed with a view to developing an appropriate framework that will promote the adoption of e-commerce via the post (Communication Authority, 2015). The Whitepaper canvassed the concept of e-commerce, looked at various case studies, identified lessons learnt and inhibiting growth factors in Kenya, and provided intervention measures to promote the adoption of e-commerce in Kenya.

The Digital Economy Blueprint: seeks to provide a conceptual framework adopted by Kenya in its quest towards the realisation of a successful and sustainable digital economy. The Blueprint acknowledges e-commerce as a rationale for digital business and considers actions to be taken to grow and streamline the adoption of e-commerce in Kenya.
6.4.3. Electronic Commerce Institutional Measures

The following institutions play a fundamental role in Kenya’s e-commerce:

- The Ministry of ICT (MoICT): which is responsible for formulating, administering, managing and developing information, communications and broadcasting policies in Kenya;

- The National Communications Secretariat (NCS): which advises the MoICT on ICT policy;

- The Directorate of e-Government (DeG);

- The Parliamentary Committee on Communications Information and Innovation;

- The Communications Authority of Kenya; and

- The Root Certification Authority (RCA);

- The Government Certification Authority (GCA); and

- The ICT Authority (ICTA): responsible for the management of the mainstream government ICT services, and which operates the GCA.

<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;The Data Protection Act, 2019.</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;The Kenyan Data Protection Commissioner.</td>
</tr>
<tr>
<td>The Critical Infrastructure Information Policy, 2016; In draft is a Policy Framework for the Protection of Critical Infrastructure.</td>
<td><strong>Electronic Commerce Laws and Regulations</strong>&lt;br&gt;Primarily governed by The Kenya Information and Communications Act, 2015; And&lt;br&gt;The Data Protection Act, 2019.</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;The Communications Authority of Kenya (the “CA”).</td>
</tr>
<tr>
<td><strong>National Cybersecurity strategy to implement the Policy</strong>&lt;br&gt;The primary policy developments are National Cyber Security Strategy (2014); and Vision 2030.</td>
<td><strong>Cybercrime Laws and Regulations</strong>&lt;br&gt;Primarily governed by the Computer Misuse and Cybercrimes Act of 2018; And&lt;br&gt;The Kenya Information Communication Act, 2012; The Kenyan Penal Code.</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>;</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>In draft is the Draft Information and Communications (Electronic Transactions) Regulations 2016.</strong>&lt;br&gt;<strong>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</strong>&lt;br&gt;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&lt;br&gt;The National Computer and Cybercrimes Co-Ordination Committee; and&lt;br&gt;The Kenyan ICT Authority (ICTA).</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 Kenya Computer Incidence Response Team and Coordination Centre (KE-CIRT/CC)</td>
</tr>
<tr>
<td><strong>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</strong>&lt;br&gt;The Kenya Computer Incidence Response Team and Coordination Centre (KE-CIRT/CC)</td>
<td><strong>If passed as law, the Draft Critical Infrastructure Bill, 2015 (the “CIB”) will create the Critical Infrastructure Protection Committee and a Critical Infrastructure Protection Unit.</strong></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;The Kenya Computer Incidence Response Team and Coordination Centre (KE-CIRT/CC)</td>
</tr>
</tbody>
</table>
7. MAURITANIA

Regional Economic Community: Union of Arab Maghreb (UMA)
Population: 4,661,149
Internet Penetration: 969,519 users i.e., 20.8% of the population
AUCC Ratification Status: Signed 26/02/2015

7.1. OVERVIEW

DATA PROTECTION: Mauritania has a data protection law in the form of Law 2017/020. Mauritania will also be bound by the ECOWAS Supplementary Act on the Personal Data Protection. Mauritania has a National Strategy of Modernization of Administration and ICTs 2012-2016 including data protection provisions. The Mauritanian Data Protection Authority is yet to be established.

ELECTRONIC TRANSACTIONS: Mauritania has electronic transaction laws (2013/025 and 2018/022). The National Strategy of Modernization of Administration and ICTs 2012-2016 considers electronic transactions and commerce in Mauritania. The Mauritanian Post Corporation is tasked with the provision of electronic certification services.

CYBERCRIME AND CYBERSECURITY: Mauritania has a cybercrime and cybersecurity Law (2016/007). Mauritania is contemplating a national cybersecurity strategy. Mauritania has a Computer Security Service tasked with investigating cybercrimes. There is no official operational CERT in Mauritania.

7.2. DATA PROTECTION

7.2.1. Overview of Data Protection Legislation

Personal data protection in Mauritania is governed by Law No. 2017/020 of July 22, 2017 on the protection of personal data (“Law 2017/020”). Law 2017/020 has been officially adopted by Mauritania’s Parliament. The purpose of Law 2017/020 is to establish a legal framework for the processing of personal data. Law 2017/020 lays down the conditions under which personal data may be processed.

Law No. 2017/020

The basic principles governing the processing of personal data are set out under Articles 4-11 whilst Articles 12-16 set out the principles for the processing of sensitive/special personal data.

Data Subject Rights are contained within Chapter V of Law 2017/020. The basic rights of data subjects are set out as follows:

- Right to Information: Section I (Articles 50-52);
- Right to Access: Section II (Articles 53-58);
- Right to object: Section III (Articles 59-60); and
- Right to Rectification: Section IV (Articles 61-63).

The obligations upon Data Controllers are set out between Articles 46-49. Security obligations are laid down under Articles 47 and 49, whilst retention obligations are set out under Article 48. It is worth noting that Law 2017/020 imposes requirements between data processors and data controllers to be governed by a written contract clearly defining each party’s respective obligations and responsibilities (Article 46).

Exemptions for the processing of Personal Data are contained within Article 4 and 17, whilst Articles 37-45 set out provisions relating to authorisations for the processing of personal data.

Law 2017/020 makes provision for a Mauritanian Data Protection Authority (“DPA”) in Chapter VI. Under Articles 64 – 72, the DPA is established, composed and organised. Article 73 sets out the duties of the DPA whilst Articles 74-83 set out administrative and pecuniary controls and penalties that the DPA may impose. The Mauritanian DPA has not been established as of writing (Greenleaf & Cottier, 54). It is furthermore noted that the DPA will become operational by way of a Decree to be passed by the Mauritanian Government.

Lastly, Law 2017/020 makes provision for the interconnection of personal data files under Articles 26-31, whilst the cross-border transfers of personal data are regulated under Articles 22-25.

Notably, Law 2017/020 fails to include provisions on the portability of data, breach notifications, privacy by design or the requirement for in-house Data Protection Officers (in certain instances), the Convention too falls in this regard.

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). Law 2017/020 is predicated to a large extent on the Supplementary Act on Personal Data Protection of the Economic Community of West African States (ECOWAS) (Mauritania is an associated member of ECOWAS) (Greenleaf & Cottier, 54). However, this Regional Instrument has not yet been adopted by ECOWAS member states (UNCTAD, 2019).
7.2.2. Data Protection Policy Developments

The National Strategy of Modernization of Administration and ICTs 2012-2016 (“NSMAI”) is the primary source of data protection policy in Mauritania. The NSMAI has, since its implementation in 2012, acknowledged legal loopholes in Mauritanian law, creating an increased risk of privacy invasions and breaches of personal data. The NSMAI acknowledges the need for data subject rights (confidentiality, security of data, access to information concerning it, rectification or opposition) and other protective rules, in a democratic state. The NSMAI furthermore acknowledges the need for trust and trust as an enabler of technology adoption in Mauritania.

“Issues related to the privacy of citizens and the confidentiality of privacy data the company are critical.” (NSMAI, Section 2.4.2.5).

The NSMAI lists actions relating to data protection and privacy as:

- Establishing a law on the protection of freedoms and personal data – Project 222;
- Defining the Common Repository of Interoperability (RCI) of information systems and protection of information – Project 421; and
- Establishing a National Data Centre (NDC) – Project 433.

7.2.3. Data Protection Institutional Measures

The Mauritanian Data Protection Authority (Autorité de protection des Données) is not yet operational (Greenleaf & Cottier, 54).

7.3. Cybercrime and Cybersecurity

7.3.1. Overview of Cybercrime and Cybersecurity Legislation

Cyber security and crimes associated therewith in Mauritania are governed by Law No. 2016/006, of January 20, 2016, providing for the orientation of the Information Society, as read with Law No. 2016/007, of 20 January 2016, on cybercrime (“Law 2016/007”).

**Law 2016/007**

Cybercrimes are criminalised under Chapter II of Law 2016/007, titled “Offenses Against the Confidentiality, Integrity And Availability Of Data And Computer Systems” (translated). Articles 4 – 13 make provision for various cyber offences including offences related to: (i) a breach of the confidentiality of a data computer and/or the data stored thereon; (ii) a breach of the integrity and availability of a data computer; and (iii) the use/distribution of technologies/devices that may be used to commit cyber offences. Offences related to intellectual property and related rights are adapted to apply to those committed by way of a computer system under Chapter III of Law 2016/007. Furthermore, various sanctions for cyber offences are provided for between Chapters I – VII (Articles 4 – 39) of Law 2016/007 in the form of both monetary fines as well as imprisonment. Importantly, offences against the safety and security of the Islamic Republic of Mauritania are provided for under Chapter V (Articles 32 and 33). Secret information of the state and other aspects of national security are protected under Article 32, whilst the ICT systems of Mauritania that are sensitive to its national security and public order are deemed critical infrastructure and are protected by way of sanctions under Article 32.

Insofar as the enforcement of its provisions are concerned, Chapter IX of Law 2016/007 provides Mauritania’s courts with the judicial authority and jurisdiction to hear and decide on violations provided for under Law 2016/007. Throughout the Act, Law 2016/007 refers to the ‘judicial authority’ (translated) as being capable of granting searches and seizures, confiscations, injunctions, appointments of qualified persons to protect computer systems, and, handing down sentences for offences set out under the Act.

Finally, Article 50 of Law 2016/007 places an obligation on Mauritania to co-operate with any international country in the investigation/prosecution of cyber-criminal offences in terms of national reciprocal legislation and/or international legal instruments.

7.3.2. Cybercrime and Cybersecurity Policy Developments

The National Strategy of Modernization of Administration and ICTs 2012-2016 (“NSMAI”) is the primary source of cyber policy in Mauritania. The NSMAI has, since its implementation in 2012, acknowledged a deficiency of legal provisions on cybercrime that ought to be addressed in order to reduce the cyber and ICT risks Mauritania faces. The NSMAI acknowledges the need to leverage successful international experiences for the deployment of cyber strategies and has listed the enactment of the Cybercrimes Act and the establishment of a State IT Security Service or Agency as actions to be completed (note: the Cybercrimes Act is now promulgated).

Furthermore, on the cybersecurity front, the Mauritanian government is contemplating the development of a national strategy guideline for cyber security (African Union & Symantec, 79).
7.3.3. Cybercrime and Cybersecurity Institutional Measures

The Mauritania government agency which has the primary responsibility for cybersecurity is referred to as the ‘ICT Branch’ (African Union & Symantec, 79). The Ministry ‘Emploi, de la Formation Professionnelle et des Technologies de l'Information et de la Communication (MEFPTIC) and the Ministry of Interior and Decentrilization (MDN) are other imperative government institutions in the cybersecurity space. The Government of Mauritania has also appointed the Computer Security Service, part of the Director General of Information Technology and Communications (DGITC), which is specifically tasked with investigating cybercrimes (African Union & Symantec, 79).

“Mauritania has established mechanisms for responding to cyber incidents, but the government does not yet operate an official CERT with national level responsibilities” (African Union & Symantec, 79).

7.4. Electronic Transactions

7.4.1. Overview of Electronic Transactions Legislation

Electronic communications and transactions (in the context of electronic commerce) in Mauritania are governed by Ordinance 2006/031 ‘concerning the instruments of payment and e-commerce transactions’ (“Order 2006/031”) and Law No. 2018/022 on Electronic Transactions.

Ordinance 2006/031

Ordinance 2006/031 provides for, amongst other things, the admissibility of electronic writing/data as evidence (Article 4); retention of electronic records (Article 5); electronic signatures (Article 6); the security of electronic signatures and guarantees on the security of electronic signatures (Article 8); the provision of electronic certificates (Article 10); the establishment of certification service providers (Article 11) and contractual liability for providers who provide goods/services by electronic means (Articles 53-61).

Law No. 2018/022

Law No. 2018/022 regulates electronic transactions in Mauritania. Thereunder:

Chapter VI regulates electronic advertising. Article 46 thereunder governs electronic advertising and provides that it must be clearly identified as such.

Section 2 of Chapter VII requires a written electronic agreement to be entered into in the context of online transactions, and furthermore sets out conditions to be inserted into these agreements.

Chapter VIII regulates the security of electronic transactions. Thereunder:

- Electronic signatures are considered under Section 2 of Chapter VIII. Article 83 provides legal validity to electronic signatures which may be utilised for authentication;
- Electronic certificates are considered under Section 3 of Chapter VIII. Article 88 states that electronic certification service providers may be registered in accordance with the requirements set out in Article 92. Article 89 sets out the requirements for a valid electronic certificate.

Chapter VIII regulates the security of electronic transactions. Section 5 (Articles 69 – 75) of Chapter VII consider the execution of contracts electronically and provides for consumer rights in the context of online transactions.

Chapter VIII regulates the security of electronic transactions. Section 1 of Chapter VIII provides for the security of electronic transactions and electronic evidence, whilst Section2 recognises electronic signatures and provides that nobody may be compelled to sign electronically.

7.4.2. Electronic Transactions Policy Developments

The National Strategy of Modernization of Administration and ICTs 2012-2016 (“NSMAI”) is the primary source of electronic communications and transactions policy in Mauritania.

The NSMAI envisages, amongst other things:

- The establishment of an electronic certification provider – Project 435; and
- The creation of an electronic document archiving system.

The NSMAI furthermore sets out general principles of online service development under Guideline 47.

Mauritania has recently drafted its National Strategy Cybersecurity 2020-2024.

7.4.3. Electronic Transactions Institutional Measures

The Mauritanian Ministry of Employment, Vocational Training and New Technologies (MEFPNT) is currently responsible for piloting the Mauritanian e-government project (as per the NSMAI) and is responsible for overseeing the development of an electronic certification service (building upon current infrastructure in Mauritania). The Mauritanian Post Corporation (MAURIPOST) has been described (in the NSMAI) as being an ideal candidate to provide electronic certification services.
7.5. 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></td>
<td><strong>Data Protection Laws and Regulations</strong></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></td>
</tr>
<tr>
<td>The National Strategy of Modernization of Administration and ICTs 2012-2016 (&quot;NSMAI&quot;) is the primary source of cyber policy in Mauritania.</td>
<td>Personal data protection in Mauritania is governed by Law No. 2017/020 of July 22, 2017 on the protection of personal data (“Law 2017/020”).</td>
<td>Law 2017/020 makes provision for a Mauritanian Data Protection Authority (&quot;DPA&quot;) in Chapter VI. Under Articles 64 – 72, the DPA is established, composed and organised</td>
</tr>
<tr>
<td><strong>National Cybersecurity strategy to implement the Policy</strong></td>
<td><strong>Electronic Commerce Laws and Regulations</strong></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></td>
</tr>
<tr>
<td>On the cybersecurity front the Mauritanian government is contemplating the development of a national strategy guideline for cyber security</td>
<td>Electronic communications and transactions (in the context of electronic commerce) in Mauritania are governed by the Electronic Transactions Act 2013/025 ‘Focusing on Electronic Communications’ and Law No. 2018 / 022 on Electronic Transactions.</td>
<td>The Mauritanian Ministry of Employment, Vocational Training and New Technologies (MEFPNT) is currently responsible for piloting the Mauritanian e-government project (as per the NSMAI) and is responsible for overseeing the development of an electronic certification service.</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>Cybercrime Laws and Regulations</strong></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></td>
</tr>
<tr>
<td></td>
<td>Law No. 2016/006, of January 20, 2016, providing for the orientation of the Information Society, as read with Law No. 2016/007, of 20 January 2016, on cybercrime.</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><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></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>ICT systems of Mauritania that are sensitive to its national security and public order are deemed critical infrastructure, and are also protected under Law No. 2016/007.</td>
<td></td>
<td>The Government of Mauritania has also appointed the Computer Security Service, part of the Director General of Information Technology and Communications (DGITC), which is specifically tasked with investigating cyber crimes</td>
</tr>
<tr>
<td></td>
<td><strong>Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.</strong></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><strong>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</strong></td>
<td>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</td>
</tr>
</tbody>
</table>
8. MOROCCO

Regional Economic Community: Union of Arab Maghreb (UMA)
Population: 36,635,156
Internet Penetration: 23,739,581 users i.e. 64.8% of the population.
AUCC Ratification Status: N/A

8.1. OVERVIEW


ELECTRONIC TRANSACTIONS: Morocco has an electronic transactions law (Law 53/05) and multiple Decrees. The Digital Morocco 2013 strategy considers electronic transactions/e-commerce. The Directorate-General for Information Systems Security (DNSSI) is responsible for approving electronic certification service providers (PSCE’s) and the approval of secure electronic certificates.


8.2. DATA PROTECTION

8.2.1. Overview of Data Protection Legislation

At a Constitutional level, Article 24 of the Moroccan Constitution, 2011, expressly guarantees the right to privacy. Thereunder, every person has the right to the protection of his private life. Private communications are considered secret. Encroachments into one’s privacy can only be authorised in cases of justice, under conditions set by law (Makulilo, 2016).

Personal data protection is governed in Morocco primarily by Law 09/08 of 18 February 2009 relating to the protection of individuals with respect to the processing of personal data (“Law 09/08”) and by its implementation, Decree 2-09-165 of 21 May 2009 (“the Decree”). The application of Law 09/08 applies to processing by automatic and non-automatic means whether by juristic/legal and natural persons; whether public or private - Article 2(1).

Law 09/08 has extra-territorial application when the person responsible for the processing uses automated or non-automated means located on Moroccan territory - Article 2(2).

Article 3(1) of Law 09/08 sets out the principles for processing Personal Data and requires that Personal Data must be:

- processed fairly and lawfully;
- collected for explicit and a legitimate aim only;
- not further processed in a way incompatible with the stated purposes;
- adequate, relevant and not excessive in relation to purposes for which they were collected and for which they are further processed;
- accurate and up to date and where inaccurate, incomplete or outdated, all reasonable measures must be taken to ensure that such Personal Data are erased or rectified; and
- kept in a form which permits identification of data subjects for no longer than that which is necessary to achieve the purposes for which they were collected and for which they are further processed.

The processing of Sensitive Data must be in adherence with the processing conditions set out under Law 09/08, failing which prior authorisation must be provided by the National Control Commission for the Protection of Personal Data (CNDP).

Article 4 sets out the requirements for valid consent as a condition for lawful data collection and Articles 5 - 9 set out and grant data subjects with the following rights:

- Information regarding the use of data (Articles 5-6);
- A right to access to data held, as well as their origins and destinations (Article 7);
- A right to rectification, without charge (Article 8);
- A right of appeal to the CNDP; and
- A right to express opposition to the collection of the data (Article 9).
Instances where prior authorisation is required from the CNDP before processing may commence/continue are detailed under Article 12 of Law 09/08 as well as Article 21 (for sensitive data). In terms of Article 22, the processing of health data is subject to a declaration to the CNDP.

Section 3 (Articles 23-36) set out the confidentiality, security and storage obligations of controllers and subcontractors (as defined under Law 09/08).

Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention 108”)

Morocco ratified Convention 108 on 28 May 2019. In addition to providing guarantees concerning the collection and processing of personal data, in the absence of proper legal safeguards, Convention 108 prohibits the processing of “sensitive data” which includes data relating to a person’s race, political views, health, religion, sexual life, and criminal record. The Convention also provides individuals with a right to know that information is stored on him or her and, if necessary, to have it corrected. Restrictions on the rights laid down in the Convention are only possible when overriding interests (e.g. State security, defence, etc.) are at stake.

On 6 June 2013, Morocco adopted a Bill approving Convention 108 (Makuilo, 2016, 37), thereby acceding to Convention 108.

Francophone Binding Corporate Rules

The Kingdom of Morocco is also a member of the French Speaking Association of Data Protection Authorities (Association francophone des autorités de protection des Données personnelles – “AFAPDP”). The Francophone Binding Corporate Rules on transfers of personal data (Les Règles Contraignantes d’Entreprise Francophones (RCEF)) were adopted by Morocco in 2013 and Morocco is bound thereby.

8.2.2. Data Protection Policy Developments

The Digital Morocco 2013 strategy is the core policy document containing policy actions for data protection. Thereunder, Morocco has, amongst other things, strategized to:

- Implement a law relating to data protection (Action 3.1 of Initiative 3) – achieved; and

- Allocate a budget to establish the National Commission for Data Protection (CNDP) (Budget 48) – achieved.

On an international front:

- The EU-Morocco Action Plan (2013-2017) required the Kingdom of Morocco to gradually accede to the relevant Council of Europe conventions on the protection of fundamental rights that are open to participation by non-members of the Council of Europe. In this regard, Morocco has acceded to Convention 108, which enables the Kingdom of Morocco to exchange personal data with Council of Europe members.

8.2.3. Data Protection Institutional Measures

The following institutions are relevant to Data Protection in Morocco:

- Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (“CNDP”) (which translates to the ‘National Control Commission for the Protection of Personal Data’): The CNDP is the independent administrative authority in charge of protecting personal data in Morocco, established by way of Decree 2-11-508. The CNDP is an autonomous authority charged with ensuring that the use of personal data does not prejudice personal privacy. The CNDP has authority over private and public institutions and their conformity with Law 09/08. The CNDP also has the power to take judicial action and apply financial and penal sanctions, in the event of infringements of the Law 09/08.
  
  - In January 2014, the CNDP launched its first large-scale control operation to verify the compliance by Moroccan websites and online businesses with the provisions of Law 09/08. Contravening websites were invited to comply with the law. Past a certain deadline, CNDP warned that non-compliant online businesses could face sanctions, including legal action (CNDP, 2014).
8.3. Cybercrime and Cybersecurity

8.3.1. Overview of Cybercrime and Cybersecurity Legislation

Cyber security and crimes associated therewith in Morocco are primarily governed by the following laws/legal instruments:

- Law No. 07/03 supplementing the Penal Code with respect to offenses relating to automated data processing systems ("Law 07/03");
- Decree 2-15-712: On the protection of sensitive information systems and critical infrastructures; and
- Decree 2-11-509: Completes Decree 2-82-673 on the organisation of the national defence administration with provisions on cybersecurity and information systems security.

Law 07/03

Since November 2003, cybercrime has been deemed a criminal offence in Morocco. Through Law 07/03, the Moroccan Criminal Code was updated to include and define cybercrime as “offenses related to automated data processing systems”. Specifically, the crimes supplemented include:

- Fraudulently modifying/altering all or any part of an automated system (Article 607-3);
- Fraudulently modifying/altering all or any part of an automated system for the purposes of obtaining information relating to the internal or external secrets of the State or the national economy (Article 607-4);
- The intentional hindering or distorting of an automated data processing system (Article 607-5);
- The fraudulent introduction of data in an automated data processing system that deteriorates, removes or modifies the data it contains, their method of processing or transmission (Article 607-6); and
- Forgery or falsification of computerized documents, regardless of form, that is likely to cause prejudice to others (Article 607-7).

Apart from the foregoing, the extent to which Morocco has adapted traditional offences to ICT's (for example, those pertaining to intellectual property), is unclear.

Decree 2-15-712

Decree 2-15-712 on the Protection of Sensitive Information Systems and Infrastructures of Vital Importance regulates the protection of Morocco's critical information systems and infrastructure.

Decree 2-11-509

Decree 2-11-509, as read with Decree 2-82-673, confers statutory authority and legal capacity on a national regulatory authority (the Directorate-General for Information Systems Security – “DGSSI”) which is responsible for all aspects of Morocco’s national cyber security.

8.3.2. Cybercrime and Cybersecurity Policy Developments

In 2012, CSSSI adopted Morocco’s first National Cybersecurity Strategy (Stratégie nationale en Sécurité des Systèmes d’Information) built on the National Strategy for Information Society and Digital Economy (“Digital Morocco 2013 strategy”) and focused on four main strategic priorities, namely:

- evaluating risks to information systems within government and in vital infrastructures;
- protecting the information systems of government agencies, public organizations, and vital infrastructures;
- strengthening the foundations of information systems security (legal framework, sensitization, training, research and development); and
- promoting national and international cooperation.

CSSSI also developed an action plan for DGSSI “to operationalize the guidelines and directives included in the strategy.

Under the Digital Morocco 2013 strategy, the promotion of cyber-confidence is recorded as a priority. The Digital Morocco 2013 strategy also acknowledges the nexus between the security of information systems and the successful uptake and expansion of Morocco’s e-commerce industry.

In 2013 Morocco also introduced the National Security Directive on Information Systems, which, amongst other things, sets out an action plan for the protection of ‘infrastructure of vital important’ (critical infrastructure). One of the core actions of this Directive is to develop and implement a National Directive of Information Systems Security (DNSSI).
8.3.3. Cybercrime and Cybersecurity Institutional Measures

In accordance with its National Cybersecurity Strategy (2013), Morocco has established the following cyber security and cybercrime related institutions in order to “strengthen national capacities as regards the security of the information systems of the administrations, public bodies and infrastructure of vital importance” (Royaume Du Maroc Administration de la Défense Nationale, 2012, 8):

- The Strategic Committee for the Security of Information Systems (CSSSI);
- The DGSSI (as described above);
- The DNSSI: The primary objective of the DNSSI is to raise the level of protection and the level of maturity of the security of all information systems in the Kingdom of Morocco; and
- The Moroccan Computer Emergency Response Team (“ma-CERT”): In 2013 the ma-CERT was established, and it joined the international Forum of Incident Response and Security Teams (FIRST).

In a media statement, the head of the data protection authority CNDP, Said Ihrai, stated that Morocco had put in place 29 units specialized in the fight against cybercrime (CIO Mag, 2018). In February 2016, the Moroccan Ministry of Industry launched the “National Campaign to Fight Cybercrime” - an initiative particularly aimed at supporting the private sector. In July 2016, the Ministry of Justice, together with the Council of Europe, organized an international workshop in the capital Rabat, on best practices regarding cybercrime legislation and electronic evidence.

8.4. ELECTRONIC TRANSACTIONS

8.4.1. Overview of Electronic Transactions Legislation

Electronic communications and transactions (in the context of electronic commerce) in Morocco are primarily governed by:

- Law 53/05 relating to the electronic exchange of legal data (“Law 53/05”);
- Decree 3-88-13 of January 20, 2015 fixing the form and content of the application for prior authorization for import, export, provision, exploitation or use of means or services of cryptography and the accompanying file;
- Decree 3-89-13 of January 20, 2015 setting the model of specifications to accompany the application to be made by the persons not having the accreditation of certification service providers and who intend to provide cryptographic services subject to authorization; and
- Decree 3-90-13 of January 20th, 2015 fixing the model of specifications to accompany the application for approval of electronic certification services.

Law 53/05

Law 53/05 is the foundation for Morocco’s electronic landscape in that it sets out a regime applicable to legal data exchanged electronically, electronic evidence, cryptography and electronic certifications.

Under Article 3 of Law 53/05, electronic mechanisms may be utilised to make public contractual offers and conclude such offers, electronically, thereby establishing a principle of free exercise of electronic commerce activities.

Article 3-4 as read with Articles 26-27 set out obligations on suppliers to provide consumers with information about the characteristics of goods or services and the details of the supplier in order to enable consumers to enforce their rights and opt-out of communications.

Articles 4 - 5 of Law 53/05 maintains that electronic writing has the same probative value as manuscript writing, provided that the person from whom it emanates can be duly identified and that it is established and preserved in conditions to guarantee the ‘integrity’ thereof.

Article 6 provides for the creation and retention of electronic signatures that ensure the validity thereof through certification by accredited electronic certification providers; and

Articles 12 – 14 set out the basis for the usage of cryptography by accredited electronic certification providers to guarantee the security of the exchange and / or the storage of legal data by electronic means.

Section III of Article 3 of Law 53/05 sets out the basis for the validity of electronic contracts, specifying what constitutes a valid electronic offer and acceptance.

Articles 15-16 of Chapter II of Law 53/05 establishes and regulates the National Authority for approval and supervision of electronic certification, whilst Section II of Chapter II regulates electronic certification service providers.
Information Disclosures, Contractual Liability of Service Providers and Advertising by Electronic Means are also provided for under Law 53/05. Specifically, a framework for information disclosures and terms and conditions by e-commerce providers, as well as contractual liability of such providers, is provided for in Article 3 of Law 53/05. Insofar as advertising by electronic means is concerned, the primary source of regulation is not Law 53/05 but rather Law 09/08 and Morocco’s proposed Bill No. 31/08 on consumer protection, including some provisions concerning the remote sales, online advertising and spamming (“Bill 31/08”). That said, within Article 10 of Law 09/08, an e-commerce provider may not direct market to a data subject, via any electronic means (email, fax, SMS, automated calling machines), unless the recipient has affirmatively consented (as defined in Law 09/08) to such prospecting. Article 10 does, however, make an exception for prospecting to a data subject via e-mail when such information was directly collected from a data subject. In addition, under Bill 31/08, rights for consumers (including e-commerce consumers) are sought to be strengthened.

8.4.2. Electronic Transactions Policy Developments

The primary strategy concerning electronic commerce in Morocco is the Digital Morocco 2013 strategy. The strategy recognised that the adoption of, and interaction with e-commerce is still under-developed for both individuals and enterprises in the Kingdom. The strategy furthermore acknowledged that in order for an uptake in e-commerce (by online sellers and consumers) to take place:

- consumer trust will need to be strengthened through legislative interventions – primarily protecting their personal data, and regulating the relationship between online sellers, and the consumer (Initiative 1 of the Digital Morocco Strategy, 2013); and

- support mechanisms to assist social operators on issues related to Information Systems Security should be implemented.

8.4.3. Electronic Transactions Institutional Measures

The following institutions play a fundamental role in Morocco’s e-commerce:

- The DGSSI: their role insofar as electronic commerce is concerned includes approving electronic certification service providers (PSCE’s) and the approval of secure electronic certificates issued by PSCE’s; and

- The CNDP: the role of the CNDP insofar as electronic commerce is concerned, primarily relates to consumer protection (especially in online environments). Where electronic marketing is concerned, In January 2016, the CNDP issued recommendations regarding unsolicited electronic marketing. It called for the creation of a national opt-out list in which consumers would register to stop receiving commercial marketing messages. This raised the question of a potential misuse of databases that could be exploited for uses beyond the original intended purpose/s. The CNDP recommended establishing a permanent working group to ensure the proper implementation of its recommendations (CNDP, 2016).
8.5. COMPARISON WITH THE AUCC PROVISIONS ON LAWS, POLICIES AND INSTITUTIONS FOR DATA PROTECTION, CYBERCRIME AND ELECTRONIC TRANSACTIONS.

Table 15: Morocco National Assessment Overview

<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**  
Personal data protection is governed by Law 09/08 of 18 February 2009 and by its implementation, Decree 2-09-165 of 21 May 2009. | **Data Protection Authority whose responsibilities in regulating data protection include authorisation of data processing, authorisation of cross border transfers of personal data**  
The Decree 2-11-508 establishes the Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel ("CNDP") (which translates to the 'National Control Commission for the Protection of Personal Data') as the authority. |
| National Cybersecurity strategy to implement the Policy | **Electronic Commerce Laws and Regulations**  
Primarily governed by Law 53/05;  
And  
Decree 2-82-673 of 28 Rabi I 1403 (13 January 1983); Decree 3-88-13 of January 20; Decree 3-89-13 of January 20, 2015; and Decree 3-90-13 of January 20th, 2015. | **Electronic Signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications**  
The Directorate-General for Information Systems Security ("DGSSI") is the authority. |
| Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture | **Cybercrime Laws and Regulations**  
Cyber security and crimes are primarily governed by Law No. 07/03;  
And  
Decree 2-15-712; Decree 2-11-509; and Decree 2-82-673. | **State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;** |
| The Ministry of Industry launched the "National Campaign to Fight Cybercrime" - aimed at supporting the private sector. | **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** |
| | | **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 Moroccan Computer Emergency Response Team ("ma-CERT"). |
| | | **Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.**  
The Strategic Committee for the Security of Information Systems (CSSSI);  
The Directorate-General for Information Systems Security ("DGSSI");  
And  
The Moroccan Computer Emergency Response Team ("ma-CERT"). |
| | | **Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)**  
The Moroccan Computer Emergency Response Team ("ma-CERT"). |
9. SENEGAL

Regional Economic Community: Economic Community of West African States (ECOWAS)
Population: 16 743 859
Internet Penetration: 9 749 527 users i.e. 58% of the population.
AUCC Ratification Status: Ratified 03/08/2016

9.1. OVERVIEW

DATA PROTECTION: Senegal has a data protection Law (2008/12) as read with Decree number 2008/721 and also Law 2016/29 modifying the Penal Code. Senegal is a signatory to the African Union Convention on Cybersecurity and Personal Data. Data protection is also considered under the Digital Senegal 2025 strategy. Senegal has a Privacy Protection Commission which was established by Law No. 2008/12. Senegal has a data protection authority (the CPD).

ELECTRONIC TRANSACTIONS: Senegal has an electronic transactions law (2008/08). The Plan for an Emerging Senegal and Digital Senegal 2025 are the policies relevant to electronic transactions and commerce. The regulatory authority responsible for electronic transactions is the State Computer Agency. SenTrust is the primary electronic certification service provider in the Republic.

CYBERCRIME AND CYBERSECURITY: Senegal has various cybercrime and security related laws, with Law 2008/11 on Cybercrime being the primary legal instrument considering substantive and procedural aspects of cybercrime. Senegal is also signatory to several international legal instruments on cybercrime and cybersecurity. Senegal has a Senegalese National Cybersecurity Strategy which constitutes the policy framework for cybersecurity. There are two institutions relevant to cybersecurity, these are the National Commission of Cryptology and the State Computer Agency.

9.2. DATA PROTECTION

9.2.1. Overview of Data Protection Legislation

There are two main laws in Senegal relating to Data Protection:

- Law No 2008/12 on the protection of personal data, dated 25 January 2008 - the Data Protection Act (the “DPA”) - as read with Decree number 2008/721 dated 30 June 2008; and


The DPA, as read with Decree 2008/721 set the conditions for data processing, the obligations for Data Controllers and the rights of Data Subjects. The DPA creates the Data Protection Authority (Commission de Protection des Donnees Personelles) (CPD).

Statutory Authority: The Statutory Authority/Commission for the Protection of Personal Data (the “CPD”) is established under Article 5 of the DPA. Articles 6-15 of the DPA set out the composition of the CPD, whilst Article 16 sets out the functions of the CPD.

Prior Authorisations: Article 18 sets out the conditions under which a form of ‘prior authorisation’ is required to be obtained from the CDP. Article 19 allows the CDP to publish guidelines/standards to exempt certain non-prejudicial processing activities from being reported, whilst Article 20 sets out instances where prior authorisation is a prerequisite before processing of personal data may take place (health research, statistics in the public interest, data relating to convictions/offences, biometric data and identity numbers).

Principles for Lawful Processing: Chapter III of the DPA sets out the principles for lawful processing of personal data. Specific confidentiality (Article 70) and security (Article 71) obligations are imposed on data controllers and processors.

Data Subject Rights: Chapter IV lays out the rights afforded to data subjects which include: the right to information (Articles 58-61); right of access (Articles 62-67); the right to object (Article 68) and; the right to rectification and deletion (Article 69). There is no “right to be forgotten” and no right to data portability in current Senegalese law.

Sensitive Personal Data: Under the DPA, sensitive personal data is a recognised category for data relating to religious, philosophical, political opinions or union activities, sex life, health, race, social measures and prosecutions, and criminal and administrative sanctions. Section II of the DPA sets out the conditions for processing sensitive personal data (Articles 40-43).

Cross-border transfers of personal data are regulated under Article 49, whilst the interconnection of data is regulated under Article 54.
Direct Marketing: Data Subjects have the right to object to the processing of the personal data by direct marketing. Article 47 of DPA and Section 16 of Electronic Communication Law prohibit the sending of marketing communications unless a Data Subject has agreed to it and this applies extra territorially. Article 431-20 of The Criminal Law stipulates the maximum penalties for sending marketing communications in breach of applicable restrictions are 7 years imprisonment or a XOF 1 million and only one of these sentences can be granted.

Apart from the DPA, there is no other general legislation or sector specific legislation that impacts data protection.

Law No 2016/29

Law 2016/29 sets out the criminal offences and sanctions for data processing.

African Union Convention on Cybersecurity and Personal Data

Senegal acceded to the African Union Convention on Cybersecurity and Personal Data in August 2016.

9.2.2. Data Protection Policy Developments

The primary policy development relating to data protection in Senegal is the Digital Senegal 2025 strategy. The Digital Senegal 2025 strategy is a vision, linked to the Emergent Senegal Plan (PSE). Under the Strategy:

- The updating of Senegal’s rules governing personal data protection is acknowledged (Paragraph 96); and
- Under Paragraph 109, digital security is considered a government priority and envisions the creation of a national cyber-security agency to complete the Personal Data Protection Commission system (PDPC), the National Cryptology Commission (CNC) and existing operational defence and security structures.

9.2.3. Data Protection Institutional Measures

The primary institution relating to data protection in Senegal is the CPD. The CPD was established under Law No. 2008/12 of 25 January 2008 on the protection of personal data – it is an Independent Administrative Authority

9.3. CYBERCRIME AND CYBERSECURITY

9.3.1. Overview of Cybercrime and Cybersecurity Legislation

Senegal has a wide range of laws that address cybersecurity:

- Law No. 2008/41 on Cryptology to build a framework for national ICT security (intended to ensure secure e-commerce, e-transaction and cryptology services);
- Law No. 2004/10 of 6 February 2004 establishing a cyber village;
- the Law No. 2008/08 on Electronic Transactions; and
- Law No. 2008/49 establishing a voluntary contribution of one percent (1%) on public procurement of goods and digital services.

Law 2008/11

Law 2008/11 is the primary legal instrument providing for cyber-criminal offences. Part one of Law 2008/11 relates to substantive criminal law, consists of three titles dealing with the establishment of offences specific to information and communication technologies and the adaptation of certain definitions of offences and certain penalties to the context of information and communication technologies.

Part two of Law 2008/11 relates to criminal procedural law, consists of two titles concerning, on the one hand, adjustments to traditional procedures in the light of information and communication technologies and, on the other, the adoption of a procedure specific to offences relating to personal data.

Critical infrastructure is not protected under Law 2008/11. A Cybersecurity authority is not established thereunder either. In this regard, “there is no single ministry or network of ministries responsible for the coordination of critical infrastructure in relation to cybersecurity” (Global Cybersecurity Capacity Centre, 2018, 16).

Law 2008/10

Law No. 2008/10 on the Orientation of the Information Society, amongst others, lays out general principles regarding the security of the ‘information society’, as well as privacy, protection of data and other human rights.

International Conventions

Senegal has acceded to the following international conventions:

- The Budapest Convention on Cybercrime in 2016 through its Demande d’adhérer à la Convention de Budapest, décembre 2016; and
- The African Union Convention on Cybersecurity and Personal Data – August 2016; and
- Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.
9.3.2. Cybercrime and Cybersecurity Policy Developments

Stemming from the creation of a Telecommunication Code, in 2011, a National Commission of Cryptology, attached to the General Secretariat of the Presidency of the Republic, and whose permanent secretariat is provided by the Central Technical Services of Numbers and Security of Information Systems (STCC), was established.

In November 2017, the Ministry of Communications, Telecommunications, Post and the Digital Economy passed the Senegalese National Cybersecurity Strategy (SNC2022) with the following strategic aims:

- strengthen the legal and institutional framework of cybersecurity in Senegal;
- strengthen protection of critical information infrastructures (CII) and government information systems in Senegal;
- promote a cybersecurity culture in Senegal;
- strengthen cybersecurity abilities and technical knowhow in all sectors;
- training and reinforcement programme for national cybersecurity resources; and
- involvement in regional and international cybersecurity work.

A core action put forward in SNC2022 is to “implement the CERT/CSIRT national structure in the shape of a unit within the national cybersecurity structure with precise defined functions and responsibilities, including responding to incidents” – Action 4.1.2.2. Since 2008, none of Senegal’s cybersecurity laws have been amended to reflect the changing environment of cybersecurity.

Senegal is “planning to establish a National Cyber Security Centre and allocate a budget for cyber security” (African Union, Symantec, 2016, 84).

Cybersecurity School

The Senegalese Government, in partnership with the French Foreign Minister, launched a national school for the cybersecurity regional vocation in 2018. The cybersecurity school is an effort to contribute to capacity building and the growing of technical knowledge in cybersecurity through awareness-raising and training (Agence Ecofin, 2018).

9.3.3. Cybercrime and Cybersecurity Institutional Measures

Law enforcement in Senegal is considered to “have some capacity to investigate cybercrime in accordance with domestic law, however this is minimal. Prosecutors and courts are not trained adequately and do not have the capacity to prosecute and preside over cybercrime cases.” (Global Cybersecurity Capacity Centre, 2018, 10).

Other relevant institutions include:

- Cell Investigations Cyber Crime Unit: investigates cybercrimes within the Interior Ministry National Police (African Union, Symantec, 2016);
- The Intelligence Agency: a specialised branch within the National Police that focuses on cybercrime (African Union, Symantec, 2016);
- The National Cryptology Commission (CNC); and

9.4. ELECTRONIC TRANSACTIONS

9.4.1. Overview of Electronic Transactions Legislation

Electronic transactions and electronic commerce in Senegal are primarily governed by Law No. 2008/08 on Electronic Transactions (the “Electronic Transactions Law”).

The Electronic Transactions Law

The Electronic Transactions Law aims to provide a legal framework for the safe expansion of a reliable e-commerce sector. Thereunder:

- The Electronic Transactions Law sets rules and procedures for internet service providers, and supports the development of electronic transactions and contracts - Article 21. Furthermore, Article 24 places various duties upon electronic vendors provide information to online consumers.
- Electronic writing is given legal certainty under Article 19;
- Free engagement in electronic commerce is permitted (subject to certain exceptions – Article 9);
- Section IV also sets out contractual liability for electronic providers of goods or services;
- Advertising by electronic means is set out under Chapter II;
- Mechanisms for securing electronic transactions are provided for under Chapter III – these include the legal validity of electronic writing and contractual requirements to be adhered to during electronic transactions; and
- Chapter III specifies the requirements for electronic evidence and signatures (Article 42).
9.4.2. Electronic Transactions Policy Developments

The primary policies relating to electronic transactions in Senegal are:

- The Plan for an Emerging Senegal (PES)

- The PES is the new five-year Priority Action Plan (2019-2024) for Senegal. Vision 2024 consists of 5 national initiatives – The Youth Plan for Emerging Sector 2035, The Social and Solidarity-Based Economy PSE, The Inclusive Digital Society PSE: The Green PSE, or the Plan For Sustainable Reforestation of the National Territory and The Industrialisation Cap PSE.

The Digital Senegal 2025 Strategy

The primary policy development relating to electronic transactions and electronic commerce in Senegal is the Digital Senegal 2025 strategy.

The fourth pillar of the "Digital Senegal 2016-2025" strategy calls for the diffusion of digital tools and solutions in key economic sectors, including e-commerce. In this area, planned actions include updating the relevant legal framework, setting up interoperability conditions among electronic financial services platforms, launching a programme to promote electronic financial services, and launching a programme to support the creation of e-commerce sites with a focus on local products and offering the possibility of electronic payment.

In order to handle and execute the e-commerce dimension of the "Digital Senegal 2016-2025" strategy, the Ministry of Trade has been working towards establishing a coherent policy for e-commerce. As a result, in addition to the existing institutional framework, a national consultative framework was set up on 26 January 2017 to create a synergy of actions, bringing various stakeholders in the e-commerce space together (Alioune Sarr, 2018).

The Digital Senegal 2025 strategy is a vision, linked to the Emergent Senegal Plan (PSE). Under the Strategy:

- the updating of Senegal's Telecommunications Code and rules governing electronic transactions is acknowledged (Paragraph 96); and

- Under Paragraph 112 of the Strategy, the promotion of the use of secure digital transactions, the fostering of electronic signatures and the building digital trust in cyberspace, is envisioned as key objectives. The Paragraph also indicates that 10,000 electronic certificates will also be issued each year in Senegal.

9.4.3. Electronic Transactions Institutional Measures

The following e-commerce/transactions institutions are in place in Senegal:

- SenTrust: SenTrust is a Senegalese institution established in 2013. In Senegal, SenTrust is the prominent service provider in the field of electronic signatures, digital certificates and data authentication for businesses, organizations and organizations, and administrations.

- The State Computer Agency (Agence De l'Informatique de l'Etat): established in 2004, the State of Senegal created the State Computer Agency (ADIE) to:

  - give more impetus, authority and resources to computerisation activities;
  - provide a quality service to users by providing appropriate solutions based on proximity and responsiveness; and

  - to make the sector more attentive the notion of performance and results.

<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 No 2008/12 - the Data Protection Act - as read with Decree number 2008/721;  
and  
Law No 2016/29 - the Penal Code. | **Data Protection Authority** whose responsibilities in regulating data protection include authorisation of data processing, authorisation of cross border transfers of personal data  
The Data Protection Authority (Commission de Protection des Données Personelles) (CPD). |
| National Cybersecurity strategy to implement the Policy | **Electronic Commerce Laws and Regulations**  
Law No. 2008/08 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  
The Electronic Signature Accreditation Authority. |
| The Senegalese National Cybersecurity Strategy (SNC2022). | **Cybercrime Laws and Regulations**  
Law No. 2008/11.  
And  
Law No. 2008/10; Law No. 2008/41; Law No. 2004/10; Law No. 2008/08; and Law No. 2008/49. | **State Department** to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory; |
| Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture | **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  
The State Computer Agency (Agence De l'Informatique de l'Etat) (ADIE). |
| **Table 16: Senegal National Assessment Overview** | | **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 Cell Investigations Cyber Crime Unit; and The Intelligence Agency. |
| | | **Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.** |
| | | **Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)**  
The State Computer Agency (Agence De l'Informatique de l'Etat) |
Law 2004/63 was the first statutory instrument in Tunisia that established a legal privacy framework. Law 2004/63 was implemented by Decree No. 2007/3004 of 27 November 2007 on the conditions and processing of notification and authorization for the processing of personal data, and Decree No. 2007/3003 of 27 November 2007 on the functioning of the national authority for the protection of personal data: l’Instance Nationale de Protection des Données à Caractère Personnel (“INPDP”). Under these laws, the protection of personal data is regulated across various provisions – these are canvassed below:

**Article 75 of Law 2004/63 establishes a data protection authority whilst sanctions for non-compliance with Law 2004/63 are laid out under Chapter VII.**

Section I (Articles 7 – 8) make provision for notifications to the National Authority for the Protection of Personal Data (“INPDP”) when processing operations are of a personal nature. Prior authorisations for the processing of various categories of personal information are required under Article 14 of Law 2004/63.

The basic principles for the processing of personal data are set out under Chapter II (specifically under Articles 9-14). Some of these principles require that:

- The processing of personal data must be done in the context of respect for human dignity, privacy and public freedoms (Article 9);
- The collection of personal data can only be carried out for lawful purposes, that is ‘determined and explicit’ (Article 10);
- Personal data must be treated fairly and to the extent necessary to the purposes for which they were collected (Article 11);
- Data Controllers must ensure that data are accurate and up to date (Article 11);
- The processing of personal data may not be carried out for purposes other than those for which they were collected except where sanctioned under the Act (Article 12);
- The processing of personal data relating to criminal records of a data subject is prohibited unless subject to an exception contained in the Act (Article 13); and
- The processing of personal data relating to racial or genetic origin, beliefs, religious, political, philosophical or trade unions, or health is prohibited unless subject to an exception contained in the Act (Article 14).
The processing of ‘special’ categories of data is catered for under Chapter V.

Data subject rights are set out in Section III of Law 2004/63 and include the rights to: retract consent (Article 27); the right of access (Article 32) and the right to object (Article 42).

Section II (Articles 9 – 26) sets out various obligations on data controllers and third-party processors. Confidentiality obligations on data controllers are provided for under Article 8 and Article 23, whilst security obligations on data controllers are provided for under Articles 18 – 19. The relationship between data controllers and third-party processors (‘sub-contractors’) is regulated under Articles 18 – 24. Interestingly, data controllers are required to choose sub-contractors ‘carefully’ (Article 20), both data controllers and sub-contracts have obligations to ensure that records are accurate and kept up to date (Article 21), and the obligations that apply to data controllers and sub-contractors also apply to any agents of a sub-contractor (Article 23). Obligations on data controllers relating to the preservation, erasure and destruction of personal data are contained between Articles 44-46.

Whilst Law 2004/63 is comprehensive, it has nonetheless been noted, with caution, that Law 2004/63 has a ‘major derogatory regime for processing of personal data by public authorities. This means that processing of personal data carried out by public persons is generally excluded.’ (Makulilo, 2016, 32)

**Draft Law 2018/25**

The Draft Law 2018/25 has been formally ratified by the Council of Ministers and has officially been referred to the Commission on Rights and Liberties (a specialised parliamentary commission that considers legislation that has the potential to impact or interfere with individual liberties) (Emna Sayadi, Dima Samaro & Klara Longfellow, 2019).

Saying this, it is important to note that the Draft Law 2018/25 has faced ongoing disapproval from civil society and other independent authorities in Tunisia who have criticised aspects of the draft law that have the potential to impact on the right to freedom of expression and the right of access to information. Specifically, Draft Law 2018/25 fails to differentiate between ‘public’ and ‘private’ personal information which falls contrary to both Article 24 (privacy) and Article 32 (access to information) of the Tunisian Constitution (Emna Sayadi, Dima Samaro & Klara Longfellow, 2019). No provisions protecting against surveillance through CCTV exist under Law 2018/25.

**The Draft Tunisian Digital Code**

In October 2018, the Ministry of Communications Technology and the Digital Economy launched public consultations on the draft Code in October 2018.

On 30 December 2019, the Digital Code was approved by the Tunisian Council of Ministers and returned to Parliament.

**Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data**

Tunisia has also acceded to the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"). In addition to providing guarantees concerning the collection and processing of personal data, in the absence of proper legal safeguards, Convention 108 prohibits the processing of “sensitive data” which includes data relating to a person’s race, political views, health, religion, sexual life, and criminal record. The Convention also provides individuals with a right to know that information is stored on him or her and, if necessary, to have it corrected. Restrictions on the rights laid down in the Convention are only possible when overriding interests (e.g. State security, defence, etc.) are at stake.

**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), Tunisia being one of such member states.

**10.2.2. Data Protection Policy Developments**

Tunisia does not have a national ICT policy that makes reference to data protection policy developments.
10.2.3. Data Protection Institutional Measures

The following institutions are relevant to Data Protection in Tunisia:

- The Ministry of Communications Technology and the Digital Economy;

- Tunisian Access to Information Authority (Instance Nationale d’Accès à l’information, INAI): The INAI was established under organic law n° 2016/22 of 24 March 2016 on the right of access to information. It has a mission to guarantee that citizens have access to public information.

- National Authority for the Protection of Personal Data (INPDP): Decree No. 3003 established Tunisia’s data protection body “l’Instance Nationale de Protection des Données à Caractère Personnel” (“INPDP”). The INPDP began to work efficiently since its inception in 2009 and ensures that specific activities related to the processing of personal data are subject to the authorisation of an administrative authority as stipulated in Article 10.4 of the AUCC; and

- The Commission on Rights and Liberties (CRL): the CRL is a specialised parliamentary commission that considers legislation that has the potential to prejudice protected rights and freedoms.

10.3. Cybercrime and Cybersecurity

10.3.1. Overview of Cybercrime and Cybersecurity Legislation

Cyber security and crimes associated therewith in Tunisia are primarily governed by the following laws:

- Articles 199 and 199b of the Tunisian Criminal Code (“TCC”);

- Law No. 2004/5 of 3 February 2004 relating to electronic security and on the organisation of the field of computer security and setting the general rules for the protection of computer systems and networks (“Law 2004/5”); and


Other legal instruments that may impact the regulation of cyber-crimes and cyber security are:

- Decree 2004/1250 dated 25 May 2004 fixing the computer systems and networks of organisations subject to the periodic compulsory audit of IT security and the criteria relating to the nature of the audit and its periodicity and the procedures for follow-up on the implementation of the recommendations contained in the audit report;

- Decree 99/2768: it was under this Decree that the National Agency for Computer Security (“ANSI”) was created in 1999.

- Circular 19 dated 11 April 2007 regarding reinforcement of cybersecurity measures in public institutions;

- Circular 19 dated 18 July 2003 on safety and prevention measures for the buildings of ministries and local authorities and public enterprises;

- Decree 2008/2639 dated 7 July 2008 setting the conditions and procedures for importing and marketing encryption tools or services through telecommunications networks;

- Law 2005/51 dated 27 June 2005 relating to electronic transfer of funds (the “Electronic Transfer of Funds Law”); and

- Law 2015/26 dated 7 August 2015 regarding anti-terrorism and anti-money laundering (the “Anti-Money Laundering and Anti-Terrorism Law”).

Importantly, whilst the Tunisian Council of Ministers approved a draft ‘Cybercrime’ law that aims to “prevent and combat cyber-crimes of information and communication” (Emna Sayadi, Dima Samaro & Klara Longfellow, 2019), Tunisia does not currently have a consolidated and enforceable cybersecurity and cyber-crimes law – this draft Cybercrime law is not yet available for public comment. Apart from the patchwork of legal instruments described below, Tunisia does not have an omnibus law that adapts traditional offences or sanctions to information and communication technologies, or that provide for the protection of ‘critical infrastructure’ (despite the fact that Law 2004/5 excludes audits on computer systems and networks attached to the Tunisian defence Ministries).

Criminalisation of cyber-crimes through a patchwork of laws

The criminalisation of cyber-crime is not currently achieved by means of a dedicated cyber security and cyber-crimes law in Tunisia. Instead, the Tunisian Criminal Code, and a patchwork of other laws, make provision for criminal sanctions of various offences involving information and communication systems:

- Article 199 bis of the TCC criminalises the:
  - Unauthorised access to an automated data processing system;
  - Modification or destruction of the system’s functioning or existing data;
  - Intentional modification or destruction of an automated data processing system’s functioning; and
  - Unauthorised insertion of data in an automated data processing system.
The Draft Tunisian Digital Code

In October 2018, the Ministry of Communications Technology and the Digital Economy introduced a draft Digital Code for Tunisia. The Digital Code focuses on three main axes: (1) the digital economy; (2) infrastructure and resources; and (3) digital confidence and cyber security. The Ministry of Communications Technology and the Digital Economy launched public consultations on the draft Code in October 2018.

On 30 December 2019, the Digital Code was approved by the Tunisian Council of Ministers and returned to Parliament.

10.3.2. Cybercrime and Cybersecurity Policy Developments

The ‘National Trust in Cyberspace’ is Tunisia’s national policy coordinating cybersecurity efforts. It has been in existence since 2002. The policy provides for the creation of “more robust national information systems, legal aspects and strengthening the Tunisian cyber security workforce.” (African Union & Symantec, 91).

Tunisia has a national cybersecurity awareness campaign for children known as the Online Child Protection Initiative (COP). Tunisia also works with NGOs and civil society organizations to raise awareness about cyber risks. ANSI periodically organizes and conducts high-level training courses for Tunisian professionals (both public and private) (African Union & Symantec, 92).

A new Cybersecurity Strategy (2020-2024) has been drafted. However, it is not yet available for public consumption. In June 2019, CyberSouth - a joint project of the European Union and the Council of Europe – hosted a meeting of the working group in charge of developing a manual on cybercrime and electronic evidence for Tunisian magistrates. According to CyberSouth, The Ministry of Justice and the Institut Supérieur de la Magistrature are strong supporters of this initiative and promote the specialisation of Tunisian magistrates.

10.3.3. Cybercrime and Cybersecurity Institutional Measures

Tunisia has the following cyber security and cyber-crime related institutions:

- The Ministry of Communications Technology and the Digital Economy;
- The National Agency for Computer Security (ANSI): The ANSI was established through Law 2004/5 and is responsible for controlling Tunisia’s information systems and ensuring the implementation of a general security strategy. It also conducts periodic audits of the systems and networks of operators in Tunisia.

Law 2004/5

Law 2004/5 primarily applies to public entities and companies that are operators of public telecommunications networks and providers of telecommunications and internet services, as well as companies whose computer networks are interconnected through external telecommunications networks, and companies performing automated processing of their customers’ personal data in connection with the provision of their services through telecommunications networks. In terms of Articles 5-9 of Law 2004/5, such entities must perform mandatory audits to assess their computer systems and networks at least once every twelve (12) months.

Article 10 Law 2004/5 also requires operators of computers systems or networks (whether public or private) to report ‘disturbances’ (breaches) to the National Computer Security Agency.

The Telecommunications Code

The Telecommunications Code details the conditions and procedures pertaining to the encryption of communications. Under the Code, the unauthorized use of cryptography is punishable by up to 5 years in jail. The unauthorised use of cryptography requires prior authorisation from the authorities. The Agence Nationale de Certification (ANC) is the authority that can grant such permissions.

Article 199 ter of the TCC criminalises the:

- Harmful modification of an electronic document’s content.
- A patchwork of other laws indirectly adapt certain offences / sanctions to Information and Communication systems:
  - Electronic theft of data (which can extend to one’s identity) would be considered theft under Tunisian law (Article 261 of the TCC);
  - The electronic theft of funds is considered an offence under the Electronic Transfer of Funds Law;
  - Law 94/36 dated 24 February 1994 on literary and artistic property (the “Copyright Law”), prohibits the use of any protected work under copyright without obtaining proper authorisation is sanctioned. The misuse could be the result of an electronic theft; and
  - Causing an interruption of telecommunications by the breaking of lines or the deterioration or destruction of equipment by any means whatsoever (Denial-of-Service DDSOS attacks) is an offence under Article 82 of the Code of Telecommunications.

Law 2004/5

Law 2004/5 primarily applies to public entities and companies that are operators of public telecommunications networks and providers of telecommunications and internet services, as well as companies whose computer networks are interconnected through external telecommunications networks, and companies performing automated processing of their customers’ personal data in connection with the provision of their services through telecommunications networks. In terms of Articles 5-9 of Law 2004/5, such entities must perform mandatory audits to assess their computer systems and networks at least once every twelve (12) months.

Article 10 Law 2004/5 also requires operators of computers systems or networks (whether public or private) to report ‘disturbances’ (breaches) to the National Computer Security Agency.

The Telecommunications Code

The Telecommunications Code details the conditions and procedures pertaining to the encryption of communications. Under the Code, the unauthorized use of cryptography is punishable by up to 5 years in jail. The unauthorised use of cryptography requires prior authorisation from the authorities. The Agence Nationale de Certification (ANC) is the authority that can grant such permissions.
The Tunisian Computer Emergency Response Team (TunCERT); the ANSI also hosts "TunCERT", the emergency response team responsible for monitoring and supervising responses to cyber-attacks. TunCERT offers guidance to stakeholders in Tunisia on how to prevent attacks on vulnerable or sensitive infrastructure.

The National Agency for Electronic Certification. It also has the authority to grant permissions for the use of cryptography.

Circular 19 dated 11 April 2007 requires public enterprises to prevent incidents through the creation of a "Computer Security Cell" in order to coordinate with the NISA and a "Computer Security Committee". Also, per the guidance of the NISA, private entities shall implement a certified information security management system (“SMSI” in French) for the safe use of computer systems and networks.

10.4. ELECTRONIC TRANSACTIONS

10.4.1. Overview of Electronic Transactions Legislation

Electronic communications and transactions (in the context of electronic commerce) in Tunisia are governed by:

- Law 2005/51 dated 27 June 2005 relating to electronic transfer of funds (the “Electronic Transfer of Funds Law”);
- Decree 2001/1667 - Terms of reference relating to the exercise of the activity certification service provider;
- Decree 2000/2331 - Fixing administrative and financial organization and the operating procedures of the national electronic certification agency; and
- Decree 2639/2008 - Fixing the conditions and the procedures of importation and commercialization of means and services of encryption through the telecommunications network.

The Electronic Commerce Law

The objective of the Electronic Commerce Law is to promote e-business and facilitate its growth via the creation of a legal framework.

The validity of electronic writing is acknowledged in Article 4, whilst the validity of the use of electronic signatures is acknowledged in Article 5. On this note, the requirements for the use of electronic signatures are also provided for under Article 5, including taking minimum precautions relevant to the technical characteristics of the signature (laid down by the Minister of Telecommunications), and utilise encryption. Obligations on electronic signature holders are also provided for under Article 5 which require that holders of electronic signatures inform the electronic certification service provider of any illegitimate use of his/her signature, as well as ensuring the veracity of all data reported to the electronic certification service provider (these requirements indirectly work towards securing/guaranteeing the safety of electronic transactions). Conversely, direct requirements to guarantee the safety of electronic transactions are provided for under:

- Article 17: requiring electronic certification service providers to only issue certificates that meet the security and reliability requirements set out via a Decree by the Ministry of Telecommunications;
- Article 18: requiring electronic certification service providers to guarantee:
  - The accuracy of the certified information contained in the certificate on the date of issue;
  - The link between the certificate holder and the signature verification;
  - Exclusive possession by the holder of the certificate of a signature creation device; and
  - Verify beforehand the identity and the power of representation of the natural person who presents himself to acquire an electronic signature.
- Article 19: requiring electronic certification service providers to revoke certifications in various circumstances.

The National Electronic Certification Agency is established and regulated under Chapter III of the Electronic Commerce Law, whilst electronic certification service providers are regulated under Chapter IV.

Electronic business transactions are regulated under Chapter V. Article 28 provides that (unless otherwise agreed upon between a seller and a consumer), an electronic contract is automatically entered into at the address of the seller and on the date of acceptance of the order by the consumer. Chapter V also requires online sellers to, amongst other things:

- provide consumers with various types of clear and understandable information (Article 25);
- provide consumers with all information related to the transaction within ten (10) days of entering into the electronic transaction (Article 29); and
- accept returns of goods/services ordered by consumers in certain circumstances (Articles 30-31).
Electronic business transactions are regulated under Chapter V. Article 28 provides that (unless otherwise agreed upon between a seller and a consumer), an electronic contract is automatically entered into at the address of the seller and on the date of acceptance of the order by the consumer. Chapter V also requires online sellers to, amongst other things:

Advertising by electronic means is not regulated under the Electronic Commerce Law, instead, this is regulated under Article 30 of Law 2004/63.

**The Draft Tunisian Digital Code**

In October 2018, the Ministry of Communications Technology and the Digital Economy introduced a draft Digital Code for Tunisia. The Digital Code focusses on three main axes: (1) the digital economy; (2) infrastructure and resources; and (3) digital confidence and cyber security. The Ministry of Communications Technology and the Digital Economy launched public consultations on the draft Code in October 2018.

On 30 December 2019, the Digital Code was approved by the Tunisian Council of Ministers and returned to Parliament.

**10.4.2. Electronic Transactions Policy Developments**

The implementation of the Tunisia’s electronic payment system titled ‘E-dinar’ by the Tunisian Post in 2001, as well as the secure online banking solution “Secure Payment Server” in 2005, both fostered the development of electronic commercial transactions (Tawfik Jelassi, 2010). As early as 2005, a special unit attached to the Prime Minister’s office was created to coordinate and spearhead efforts to develop an “electronic government” program to make more services available online and boost the government’s digital readiness.

“As of November 2009, more than eighty (80%) percent of companies’ income taxes are paid online using electronic signatures, and all students in the country register online for their university classes” (Tawfik Jelassi, 2010, 156).

In 2017, Tunisia ranked 99th among 176 other nations on the United Nations International Telecommunications Union’s ICT Development Index, a benchmarking tool based on eleven (11) major information and communications technologies (ICT) indicators used to measure ICT performance in and between countries (ITU, 2017).

The government of Tunisia is making efforts to promote digital payments. In May 2019, the Ministry of Finance introduced a set of new digital services to facilitate the payment of bills, taxes, and other charges by citizens and businesses. This set of new digital services, launched by the Ministry of Finance, is part of the national strategy to reduce the use of cash and increase electronic payments (Export.gov, 2019).

The ICT Ministry has introduced the Digital Code which will replace the Electronic Commerce Law. The Ministry introduced the Digital Code in response to a large number of cybercrimes taking place in Tunisia. The Digital Code is expected to create more institutions (cited below).

**10.4.3. Electronic Transactions Institutional Measures**

The following institutions play a fundamental role in Tunisia’s e-commerce:

- The National Electronic Certification Agency (Tuntrust); and
- The Ministry of Communication Technologies;
- The Ministry of Communications Technology and the Digital Economy;
- Under the Draft Tunisian Digital Code, the following new institutions relative to electronic transactions will be created:
  - The Internet Forum;
  - The Digital Development Fund;
  - The Tunisian Digital Development Foundation; and
  - The Digital Trust Services Committee.
10.5. 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;The 'National Trust in Cyberspace' is Tunisia’s national policy coordinating its cyber security efforts&lt;br&gt;<strong>National Cybersecurity strategy to implement the Policy</strong>&lt;br&gt;A new Cybersecurity Strategy (2020/2024) has been drafted. However, it is not yet available for public consumption.&lt;br&gt;<strong>Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture</strong>&lt;br&gt;The National Agency for Computer Security (“ANSI”) periodically organizes and conducts high level training courses for Tunisian professionals (both public and private).&lt;br&gt;Tunisia also has a national cybersecurity awareness campaign for children known as COP.</td>
<td><strong>Data Protection Laws and Regulations</strong>&lt;br&gt;Law 2004/63 of 27th July 2004 relating to personal data protection.&lt;br&gt;The Draft Basic Law No. 2018/25 on the protection of personal data. And&lt;br&gt;The draft Digital Code.&lt;br&gt;<strong>Electronic Commerce Laws and Regulations</strong>&lt;br&gt;Law 2000/83 dated 9 August 2000 (the Electronic Commerce Law). Law 2005/51 dated 27 June 2005 (the Electronic Transfer of Funds Law). Decree 2001/1667; Decree 2000/2331; and Decree 2639/2008.&lt;br&gt;In draft is the Digital Code.</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;Decree No. 3003 establishes the National Authority for the Protection of Personal Data (“l’Instance Nationale de Protection des Données à Caractère Personnel” (“INPDP”)) as Tunisia’s data protection body. <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 National Electronic Certification Agency (TunTrust) is the authority. <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 Ministry of Communications Technology and the Digital Economy deals with the regulation of all electronic commerce payment methods. <strong>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</strong>&lt;br&gt;The Ministry of Communications Technology and the Digital Economy deals with the regulation of ICT related matters. <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;The Tunisian Computer Emergency Response Team (TunCERT). <strong>Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.</strong>&lt;br&gt;The Tunisian Computer Emergency Response Team (TunCERT). <strong>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</strong>&lt;br&gt;The Tunisian Computer Emergency Response Team (TunCERT).</td>
</tr>
</tbody>
</table>
REFERENCES

PART I:


PART II:

Benin


Chad


Congo


Privacy Shield Framework, Republic of Congo - 3-Legal Regime, retrieved from https://www.privacyshield.gov/article?id=Republic-of-Congo-Legal-Regime


REFERENCES
Democratic Republic of Congo

Bespoke Competition Policy for Developing Countries


Guinea


Ministry of Planning and International Cooperation, 2016-2020 Economic And Social Development Plan.


REFERENCES
Kenya


Mauritania


REFERENCES
Morocco


Senegal


Ministry Of Communication, Telecommunications, Postal Services And Digital Economy - Digital Senegal 2016 – 2025 Strategy, retrieved from https://www.itu.int/net4/wsis/archive/stocktaking/Project/Details?projectId=1488401022


REFERENCES
Tunisia


# ANNEXURE “A”

## LIST OF AFRICAN UNION MEMBER STATES FOR COUNTRY SELECTION

<table>
<thead>
<tr>
<th>NO.</th>
<th>COUNTRY</th>
<th>REC</th>
<th>AUCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Angola</td>
<td>SADC, ECCAS</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Benin</td>
<td>ECOWAS</td>
<td>Signed</td>
</tr>
<tr>
<td>4</td>
<td>Botswana</td>
<td>SADC</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Burkina Faso</td>
<td>ECOWAS</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Burundi</td>
<td>COMESA, ECCAS</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Cameroon</td>
<td>ECCAS</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Cape Verde</td>
<td>ECOWAS</td>
<td>Signed</td>
</tr>
<tr>
<td>9</td>
<td>Central African Republic</td>
<td>ECCAS</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Chad</td>
<td>ECCAS</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Comoros</td>
<td>SADC</td>
<td>Signed</td>
</tr>
<tr>
<td>12</td>
<td>Congo</td>
<td>ECCAS</td>
<td>Signed</td>
</tr>
<tr>
<td>13</td>
<td>Djibouti</td>
<td>COMESA, IGAD</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>DRC</td>
<td>ECCAS, SADC</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Egypt</td>
<td>COMESA</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Equatorial Guinea</td>
<td>ECCAS</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Eritrea</td>
<td>IGAD</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>eSwatini</td>
<td>SADC</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Ethiopia</td>
<td>COMESA, IGAD</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Gabon</td>
<td>ECCAS</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Gambia</td>
<td>ECOWAS</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Ghana</td>
<td>ECOWAS</td>
<td>Signed</td>
</tr>
<tr>
<td>23</td>
<td>Guinea</td>
<td>ECOWAS</td>
<td>Ratified</td>
</tr>
<tr>
<td>24</td>
<td>Guinea Bissau</td>
<td>ECOWAS</td>
<td>Signed</td>
</tr>
<tr>
<td>25</td>
<td>Ivory Coast</td>
<td>ECOWAS</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Kenya</td>
<td>EAC, COMESA, IGAD</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Lesotho</td>
<td>SADC</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Liberia</td>
<td>ECOWAS</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Libya</td>
<td>UMA</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Madagascar</td>
<td>SADC</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Malawi</td>
<td>SADC, COMESA</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Mali</td>
<td>ECOWAS</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Mauritania</td>
<td>ECOWAS, UMA</td>
<td>Signed</td>
</tr>
<tr>
<td>34</td>
<td>Mauritius</td>
<td>SADC</td>
<td>Ratified</td>
</tr>
<tr>
<td>35</td>
<td>Morocco</td>
<td>UMA</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Mozambique</td>
<td>SADC</td>
<td>Signed</td>
</tr>
<tr>
<td>37</td>
<td>Namibia</td>
<td>SADC</td>
<td>Ratified</td>
</tr>
<tr>
<td>38</td>
<td>Niger</td>
<td>ECOWAS</td>
<td></td>
</tr>
<tr>
<td>NO.</td>
<td>COUNTRY</td>
<td>REC</td>
<td>AUCC</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------</td>
<td>--------------------</td>
<td>--------</td>
</tr>
<tr>
<td>39</td>
<td>Nigeria</td>
<td>ECOWAS</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Rwanda</td>
<td>COMESA, EAC</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>Sahrawi Arab Democratic Republic</td>
<td>UMA</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>Sao Tome &amp; Principe</td>
<td>ECOWAS, ECCAS</td>
<td>Signed</td>
</tr>
<tr>
<td>43</td>
<td>Senegal</td>
<td>ECOWAS</td>
<td>Ratified</td>
</tr>
<tr>
<td>44</td>
<td>Seychelles</td>
<td>SADC</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>Sierra Leone</td>
<td>ECOWAS</td>
<td>Signed</td>
</tr>
<tr>
<td>46</td>
<td>Somalia</td>
<td>IGAD</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>South Africa</td>
<td>SADC</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>South Sudan</td>
<td>IGAD</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Sudan</td>
<td>IGAD</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Tanzania</td>
<td>EAC, SADC</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Togo</td>
<td>ECOWAS</td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>Tunisia</td>
<td>UMA</td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>Uganda</td>
<td>EAC, IGAD</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>Zambia</td>
<td>SADC</td>
<td>Signed</td>
</tr>
<tr>
<td>55</td>
<td>Zimbabwe</td>
<td>SADC</td>
<td></td>
</tr>
</tbody>
</table>
# Annexure “B”
## Checklist of AUCC Requirements by Chapter

### Chapter I: Electronic Commerce

<table>
<thead>
<tr>
<th>Obligation</th>
<th>Reference</th>
<th>Measure</th>
</tr>
</thead>
</table>
| Exempt activities from e-commerce regulation: Ensure that all e-commerce activities are exercised freely except:  
- Gambling  
- Legal representation and assistance activities  
- Activities exercised by notaries or equivalent authorities in application of extant texts | Article 2(1). | Legislation Regulations |
| Provide for obligations of e-commerce service providers: Ensure that any person involved in e-commerce provides easy, direct and uninterrupted access to the following information:  
- Name (corporate name where relevant), capital and registration number;  
- Full address, email address and telephone number;  
- Business registration formalities or registration in national directory of businesses or associations, the registration number, share capital and corporate headquarters;  
- Tax identification number (where a person is subject to tax);  
- Name and address of issuing authority and reference of the authorization (where the person’s activity is subject to licensing regime);  
- Professional rules, professional title, African Union state which granted authorization as well as the name of the body or order which they are registered with (where a person is a member of a regulated profession). | Article 2(2). | Legislation |

Any person (natural or legal) involved in e-commerce shall clearly and unambiguously indicate a price (provided that person has provided a price), particularly where it includes taxes, delivery and other charges. (Article 2(3))
<table>
<thead>
<tr>
<th>OBLIGATION</th>
<th>REFERENCE</th>
<th>MEASURE</th>
</tr>
</thead>
</table>
| Regulate direct marketing  
Prohibit direct marketing through any kind of indirect communication, in any form, the particulars of an individual who has not given prior consent to receiving the marketing material. | Article 4 (3).  
Instance where direct marketing shall be permissible are included in article 4(4) | Legislation Regulation       |
| Regulate “spam”  
Prohibit the transmission, for direct marketing purposes, messages of any form of indirect communication without indicating valid particulars to which the address may send a request to stop communications without incurring charges other than those arising from the transmission of that request. | Article 5.                                                                 | Legislation Regulation       |
| Approve electronic payment methods  
Ensure that the supplier of goods or services uses payment methods approved by the State. | Article 7(1)                                                               | Institutional                  |
| Accredit bodies to certify true copies of contracts signed by electronic means  
Accredited bodies (by the State) will certify copies of contracts signed electronically and where necessary issue a certificate of conformity. | Article 7(3)                                                               | Institutional                  |
| Provide for accredited (qualified) electronic signatures: An electronic signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications. | Article 1  
Article 6(5)                                                             | Institutional Regulation Legislation |
### CHAPTER II: PERSONAL DATA PROTECTION

#### Section I: Personal Data Protection

<table>
<thead>
<tr>
<th>OBLIGATION</th>
<th>REFERENCE</th>
<th>MEASURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a legal framework to strengthen fundamental rights, in particular the protection of physical data and punish any violation of privacy, without prejudice to the free flow of information.</td>
<td>Article 8 (1). The scope of application and data processing formalities can be found in articles 9 and 10.</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>The framework or mechanism established must ensure that any data processing respects fundamental freedoms and rights of natural persons, while recognising State prerogatives, the rights if local communities and the purposes for which the businesses were established. (article 8 (2)).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Section II: Institutional framework for the protection of personal data

<table>
<thead>
<tr>
<th>OBLIGATION</th>
<th>REFERENCE</th>
<th>MEASURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish Data Protection Authority.</td>
<td>Article 11(1)(a). The composition and organisation of these data processing authorities can be found in article 11(1)(b) to 11 (7). The duties and powers of the data processing authorities can be found in article 12.</td>
<td>Institutional</td>
</tr>
<tr>
<td>Provide the Data Protection Authority with the human, technical and financial resources necessary to carry out their function.</td>
<td>Article 11 (8).</td>
<td>Governance Institutional</td>
</tr>
</tbody>
</table>
### Section III: Obligations relating to conditions governing personal data processing

<table>
<thead>
<tr>
<th>OBLIGATION</th>
<th>REFERENCE</th>
<th>MEASURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take legislative measures to prohibit any data collection and processing revealing racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or health information of a data subject.</td>
<td>Article 14(1): Processing of sensitive data</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td></td>
<td>Article 14 (2) provides exceptions to prohibition.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Basic principles governing the processing of personal data are included in article 13.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The rights of a data subject are outlined in sections 16 (right to information), 17 (right to access), 18 (right to object) and 19 (right to rectification or erasure).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obligations of personal data controllers can be found in articles 20 (confidentiality), 21 (security), 22 (storage), and 22 (sustainability).</td>
<td></td>
</tr>
</tbody>
</table>

### CHAPTER III: PROMOTING CYBER SECURITY AND COMBATING CYBERCRIME

#### Section I: Cyber Security Measures to be taken at National Level

<table>
<thead>
<tr>
<th>OBLIGATION</th>
<th>REFERENCE</th>
<th>MEASURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop a national cybersecurity policy (in collaboration with stakeholders) that recognises the importance of Critical Information Infrastructure.</td>
<td>Article 24 (1).</td>
<td>Policy</td>
</tr>
<tr>
<td>Adopt strategies deemed appropriate an adequate to implement the national cyber security policy, particularly in the area of legislative reform and development, sensitization and capacity building, public-private partnership, and international cooperation, amongst others.</td>
<td>Article 24 (2).</td>
<td>Strategy</td>
</tr>
<tr>
<td>Adopt legislative and/or regulatory measures against cybercrime as deemed effective by considering substantive criminal offences acts that affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data</td>
<td>Article 25 (1)</td>
<td>Legislative Regulatory</td>
</tr>
<tr>
<td></td>
<td>In adopting the relevant legislative measures, states are expected to</td>
<td></td>
</tr>
<tr>
<td>OBLIGATION</td>
<td>REFERENCE</td>
<td>MEASURE</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-----------</td>
<td>------------------------</td>
</tr>
<tr>
<td>processed and the underlying network infrastructure and the effective procedural measures to pursue and prosecute offenders.</td>
<td>consider the choice of language that is used in international best practice.</td>
<td></td>
</tr>
<tr>
<td>Adopt legislative and/or regulatory measures as it deems necessary to confer specific responsibility on institutions, either newly established or pre-existing, as well as on the designated officials of the said institutions, with a view to conferring on them a statutory authority and legal capacity to act in all aspects of cyber security application.</td>
<td>Article 25 (2).</td>
<td>Legislative Regulatory</td>
</tr>
<tr>
<td>Ensure that the measures so adopted (in the area of cyber security and the implementation thereof) will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, amongst others.</td>
<td>Article 25 (3)</td>
<td>Governance Oversight Legislation Regulation</td>
</tr>
<tr>
<td>Adopt legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure; and, in this regard, proposing more severe sanctions for criminal activities on ICT systems in these sectors, as well as measures to improve vigilance, security and management.</td>
<td>Article 25 (4)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Undertake to promote the culture of cyber security among all stakeholders, namely, governments, enterprises and the civil society, which develop, own, manage, operationalize and use information systems and networks.</td>
<td>Article 26 (1) (a)</td>
<td>Governance Oversight</td>
</tr>
<tr>
<td>In promoting the culture of cyber security, states may adopt the following measures: establish a cyber-security plan for the systems run by their governments; elaborate and implement programmes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBLIGATION</td>
<td>REFERENCE</td>
<td>MEASURE</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-----------</td>
<td>------------------</td>
</tr>
<tr>
<td>and initiatives for sensitization on security for systems and networks users; encourage the development of a cybersecurity culture in enterprises; foster the involvement of the civil society; launch a comprehensive and detailed national sensitization programme for Internet users, small business, schools and children. (article 26(1)(b))</td>
<td>Article 26 (2)</td>
<td>Governance Oversight</td>
</tr>
<tr>
<td>Undertake to provide leadership for the development of the cybersecurity culture within its borders.</td>
<td>Article 26 (3)</td>
<td>Governance</td>
</tr>
<tr>
<td>Develop public-private partnership as a model to engage industry, the civil society, and academia in the promotion and enhancement of a culture of cybersecurity.</td>
<td>Article 26 (4)</td>
<td>Legislation Regulation Institutional</td>
</tr>
<tr>
<td>Adopt measures to develop capacity building with a view to offering training which covers all areas of cybersecurity to different stakeholders, and setting standards for the private sector.</td>
<td>Article 27(1) (a)</td>
<td>Governance Oversight Institutional</td>
</tr>
<tr>
<td>Adopt the necessary measures to establish an appropriate institutional mechanism responsible for cybersecurity Governance.</td>
<td>Article 27(2)</td>
<td>Institutional</td>
</tr>
<tr>
<td>Ensure that the legislative measures and/or regulations adopted to fight against cyber-crime will strengthen the possibility of regional harmonization of these measures and respect the principle of double criminal liability.</td>
<td>Article 28 (1)</td>
<td>Legislation Regulation</td>
</tr>
</tbody>
</table>
## Section II: Criminal Provisions

<table>
<thead>
<tr>
<th>Obligation</th>
<th>Reference</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undertake to encourage the signing of legal mutual assistance agreements</td>
<td>Article 28 (2) The Agreements must conform with the principle of double</td>
<td>International co-operation</td>
</tr>
<tr>
<td>(where states do not have such agreements).</td>
<td>criminal liability, while promoting exchange of information and efficient</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sharing of data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Institutional</td>
</tr>
<tr>
<td>Encourage the establishment of institutions that exchange information on</td>
<td>Article 28 (3) These institutions include Computer Emergency Response</td>
<td></td>
</tr>
<tr>
<td>cyber threats and vulnerability assessments.</td>
<td>Response Teams (CERTs) or the Computer Security Incident Response Teams</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(CSIRTs).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Article 28 (4) These means may be international, intergovernmental,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>regional or based on public or private partnerships.</td>
<td></td>
</tr>
</tbody>
</table>

### OBLIGATION

- Take necessary legislative and/or regulatory measures to criminalise attacks on computer systems. States must make it an offence to:
  - Gain unauthorised access to part or all of a computer system (including attempts).
  - Gain unauthorized access to part or all of a computer system or exceed authorized access with intent to commit another offence or facilitate the commission of such an offence;
  - Remain or attempt to remain fraudulently in part or all of a computer system;

<table>
<thead>
<tr>
<th>Obligation</th>
<th>Reference</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take necessary legislative and/or regulatory measures to criminalise</td>
<td>Article 29(1) (a)</td>
<td>Legislation</td>
</tr>
<tr>
<td>attacks on computer systems. States must make it an offence to:</td>
<td></td>
<td>Regulation</td>
</tr>
<tr>
<td></td>
<td>Article 29 (1) (b)</td>
<td></td>
</tr>
<tr>
<td>OBLIGATION</td>
<td>REFERENCE</td>
<td>MEASURE</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Hinder, distort or attempt to hinder or distort the functioning of a computer system;</td>
<td>Article 29 (1)(c)</td>
<td></td>
</tr>
<tr>
<td>Enter or attempt to enter data fraudulently in a computer system;</td>
<td>Article 29 (1)(d)</td>
<td></td>
</tr>
<tr>
<td>Damage or attempt to damage, delete or attempt to delete, deteriorate or attempt to deteriorate, alter or attempt to alter, change or attempt to change computer data fraudulently</td>
<td>Article 29 (1)(e)</td>
<td></td>
</tr>
<tr>
<td>Article 29 (1)(f)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adopt regulations compelling vendors of information and communication technology products to have vulnerability and safety guarantee assessments carried out on their products by independent experts and researchers, and disclose any vulnerabilities detected and the solutions recommended to correct them to consumers.</td>
<td>Article 29 (1)(g)</td>
<td>Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative and/or regulatory measures to make it a criminal offence to unlawfully produce, sell, import, possess, disseminate, offer, cede or make available computer equipment, program, or any device or data designed or specially adapted to commit offences, or unlawfully generate or produce a password, an access code or similar computerized data allowing access to part or all of a computer system.</td>
<td>Article 29 (1)(h)</td>
<td>Legislative Regulatory</td>
</tr>
<tr>
<td>Take the necessary legislative and/or regulatory measures to criminalise computerised data breaches. These offences include:</td>
<td>Article 29 (2)(a)</td>
<td>Legislation</td>
</tr>
<tr>
<td>Intercepting or attempting to intercept computerised data fraudulently by technical means during non-public transmission to, from or within a computer system;</td>
<td></td>
<td>Regulation</td>
</tr>
<tr>
<td>Intentionally inputting, altering, deleting, or suppressing computer data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible;</td>
<td>Article 29 (2) (b)</td>
<td></td>
</tr>
<tr>
<td>OBLIGATION</td>
<td>REFERENCE</td>
<td>MEASURE</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Hinder, distort or attempt to hinder or distort the functioning of a computer system;</td>
<td>Article 29 (1)(c)</td>
<td></td>
</tr>
<tr>
<td>Enter or attempt to enter data fraudulently in a computer system;</td>
<td>Article 29 (1)(d)</td>
<td></td>
</tr>
<tr>
<td>Damage or attempt to damage, delete or attempt to delete, deteriorate or attempt to deteriorate, alter or attempt to alter, change or attempt to change computer data fraudulently</td>
<td>Article 29 (1)(e)</td>
<td>Article 29 (1)(f)</td>
</tr>
<tr>
<td>Adopt regulations compelling vendors of information and communication technology products to have vulnerability and safety guarantee assessments carried out on their products by independent experts and researchers, and disclose any vulnerabilities detected and the solutions recommended to correct them to consumers.</td>
<td>Article 29 (1)(g)</td>
<td>Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative and/or regulatory measures to make it a criminal offence to unlawfully produce, sell, import, possess, disseminate, offer, cede or make available computer equipment, program, or any device or data designed or specially adapted to commit offences, or unlawfully generate or produce a password, an access code or similar computerized data allowing access to part or all of a computer system.</td>
<td>Article 29 (1)(h)</td>
<td>Legislative Regulatory</td>
</tr>
<tr>
<td>Take the necessary legislative and/or regulatory measures to criminalise computerised data breaches. These offences include:</td>
<td>Article 29 (2)(a)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Interception or attempting to intercept computerised data fraudulently by technical means during non-public transmission to, from or within a computer system;</td>
<td>Article 29 (2)(b)</td>
<td></td>
</tr>
<tr>
<td>OBLIGATION</td>
<td>REFERENCE</td>
<td>MEASURE</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>- Knowingly using data obtained fraudulently from a computer system;</td>
<td>Article 29 (2)(b)</td>
<td></td>
</tr>
<tr>
<td>- Fraudulently procuring, any benefit by inputting, altering, deleting or</td>
<td>Article 29 (2)(c)</td>
<td></td>
</tr>
<tr>
<td>suppressing computerized data or any other form of interference with the</td>
<td>Article 29 (2)(d)</td>
<td></td>
</tr>
<tr>
<td>functioning of a computer system;</td>
<td>Article 29 (2)(e)</td>
<td></td>
</tr>
<tr>
<td>- processing or having personal data processed without complying with the</td>
<td>Article 29 (2)(f)</td>
<td></td>
</tr>
<tr>
<td>preliminary formalities for the processing;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Participating in an association formed or in an agreement established with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a view to preparing or committing one or several of the offences provided</td>
<td></td>
<td></td>
</tr>
<tr>
<td>for under AUCC.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Take necessary legislative and/or regulatory measures to criminalise content related offences. These offences include:

<table>
<thead>
<tr>
<th>OBLIGATION</th>
<th>REFERENCE</th>
<th>MEASURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Producing, registering, offering, manufacturing, availing, disseminating</td>
<td>Article 29 (3)(1)(a)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>and transmitting an image or a representation of child pornography</td>
<td></td>
<td></td>
</tr>
<tr>
<td>through a computer system;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Procuring, importing or have imported, and exporting or have exported an</td>
<td>Article 29 (3)(1)(b)</td>
<td></td>
</tr>
<tr>
<td>image or representation of child pornography through a computer system;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Possessing an image or representation of child pornography in a computer</td>
<td>Article 29 (3)(1)(c)</td>
<td></td>
</tr>
<tr>
<td>system or on a computer data storage medium;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Facilitating or providing access to images, documents, sound or</td>
<td>Article 29 (3)(1)(d)</td>
<td></td>
</tr>
<tr>
<td>representation of a pornographic nature to a minor;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Creating, downloading, disseminating or availing in any form writings,</td>
<td>Article 29 (3)(1)(e)</td>
<td></td>
</tr>
<tr>
<td>messages, photographs, drawings or any other presentation of ideas or</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBLIGATION</td>
<td>REFERENCE</td>
<td>MEASURE</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>theories of racist or xenophobic nature through a computer system;</td>
<td></td>
<td>Article 29 (3)(1)(f)</td>
</tr>
<tr>
<td>→ Threatening, through a computer system, to commit a criminal offence</td>
<td></td>
<td>Note: 'no imminent</td>
</tr>
<tr>
<td>against a person for the reason that they belong to a group distinguished</td>
<td></td>
<td>violence qualifier.</td>
</tr>
<tr>
<td>by race, colour, descent, national or ethnic origin or religion where</td>
<td></td>
<td></td>
</tr>
<tr>
<td>such membership serves as a pretext for any of these factors, or</td>
<td></td>
<td></td>
</tr>
<tr>
<td>against a group of persons which is distinguished by any of these</td>
<td></td>
<td></td>
</tr>
<tr>
<td>characteristics.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>→ Insulting, through a computer system, persons for the reason that they</td>
<td></td>
<td>Article 29 (3)(1)(g)</td>
</tr>
<tr>
<td>belong to a group distinguished by race, colour, descent, national or</td>
<td></td>
<td>Note: criminalisation of</td>
</tr>
<tr>
<td>ethnic origin, or religion or political opinion, if used as a pretext</td>
<td></td>
<td>insults/criminal defamation.</td>
</tr>
<tr>
<td>for any of these factors, or against a group of persons</td>
<td></td>
<td></td>
</tr>
<tr>
<td>distinguished by any of these characteristics; and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>→ Deliberately denying, approving or justifying acts constituting</td>
<td></td>
<td>Article 29 (3)(1)(h)</td>
</tr>
<tr>
<td>genocide or crimes against humanity through a computer system.</td>
<td></td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Take the necessary legislative and/or regulatory measures to make the</td>
<td>Article 29 (3)(2)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>offences provided for under this Convention criminal offences.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Where the offences are committed by a criminal organization, the maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>punishment should be prescribed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Take the necessary legislative and/or regulatory measures to ensure that,</td>
<td>Article 29 (3)(3)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>in the case of conviction, national courts will give a ruling for</td>
<td></td>
<td></td>
</tr>
<tr>
<td>confiscation of the materials, equipment, instruments, computer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>program, and all other devices or data belonging to the convicted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>person and used to commit any of the offences mentioned in AUCC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Take the necessary legislative and/or regulatory measures to ensure that</td>
<td>Article 29 (4)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>digital evidence in</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBLIGATION</td>
<td>REFERENCE</td>
<td>MEASURE</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>criminal cases is admissible to establish offenses under national criminal law</td>
<td>Provided that such evidence has been presented during proceedings and discussed before the judge, that the person from whom it originates can be duly identified, and that it has been made out and retained in a manner capable of assuring its integrity</td>
<td></td>
</tr>
<tr>
<td>Take the necessary legislative and/or regulatory measures to criminalize the violation of property such as theft, fraud, handling of stolen property; abuse of trust, extortion of funds; and blackmail involving computer data.</td>
<td>Article 30 (1)(a)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative and/or regulatory measures to consider as aggravating circumstances the use of information and communication technologies to commit offences such as theft, fraud, handling of stolen property, abuse of trust, extortion of funds, terrorism and money laundering.</td>
<td>Article 30 (1)(b)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative and/or regulatory measures to specifically include “by means of digital electronic communication” such as the Internet in listing the means of public dissemination provided for under domestic criminal law.</td>
<td>Article 30 (1)(c)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary criminal legislative measures to restrict access to protected systems which have been classified as critical national defence infrastructure due to the critical national security data they contain.</td>
<td>Article 30 (1)(d)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure that legal persons other than the State, local communities and public institutions can be held responsible for the offences provided for by this Convention, committed on their behalf by their organs or representatives.</td>
<td>Article 30 (2)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure offences under AUCC are punishable by effective, proportionate and dissuasive criminal penalties.</td>
<td>Article 31(1)(a).</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>OBLIGATION</td>
<td>REFERENCE</td>
<td>MEASURE</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure offences under AUCC are punishable by appropriate penalties in the respective legislations.</td>
<td>Article 31(1)(b).</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure that a legal person held liable in accordance with AUCC (article 13 (2)), is punishable by effective, proportionate and dissuasive sanctions (including criminal sanctions).</td>
<td>Article 31 (1) (c)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure that in the case of conviction for an offense committed through a digital communication medium, the competent court may hand down additional sanctions.</td>
<td>Article 31 (2)(a)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure that in the case of conviction for an offence committed through a digital communication medium, the judge may in addition order the mandatory dissemination, at the expense of the convicted person, of an extract of the decision, through the same medium, and according to modalities in the domestic law.</td>
<td>Article 31 (2)(b)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure that a breach of the confidentiality of data stored in a computer system is punishable by the same penalties as those applicable for breaches of professional secrecy.</td>
<td>Article 31 (2)(c)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure that where the data stored in a computer system or in medium where computerized data can be stored in the territory of a State Party, are useful in establishing the truth, the court applied to may carry out a search to access all or part of a computer system through another computer system, where the said data are accessible from or available to the initial system.</td>
<td>Article 31 (3) (a)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure that where the judicial authority in charge of investigation discovers data stored in a computer system that are useful for establishing the truth, but the seizure of the support does not seem to be appropriate, the data as well as all such data as are required to understand them.</td>
<td>Article 31 (3) (b)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>OBLIGATION</td>
<td>REFERENCE</td>
<td>MEASURE</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>shall be copied into a computer storage medium that can be seized and sealed, in accordance with the modalities provided for under the legislations of State Parties.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure that judicial authorities can, for the purposes of investigation or execution of a judicial delegation, carry out the operations provided for under AUCC.</td>
<td>Article 31 (3) (c)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure that if information needs so require, particularly where there are reasons to believe that the information stored in a computer system are particularly likely to be lost or modified, the investigating judge may impose an injunction on any person to preserve and protect the integrity of the data in his/her possession or under his/her control, for a maximum period of two years, in order to ensure the smooth conduct of the investigation. The custodian of the data or any other person responsible for preserving the data shall be expected to maintain secrecy with regard to the data.</td>
<td>Article 31 (3)(d)</td>
<td>Legislation Regulation</td>
</tr>
<tr>
<td>Take the necessary legislative measures to ensure that where information needs so require, the investigating judge can use appropriate technical means to collect or record in real time, data in respect of the contents of specific communications in its territory, transmitted by means of a computer system or compel a service provider, within the framework of his/her technical capacities, to collect and record, using the existing technical facilities in its territory or that of State Parties, or provide support and assistance to the competent authorities towards the collection and recording of the said computerized data.</td>
<td>Article 31 (3) (e)</td>
<td>Legislation Regulation</td>
</tr>
</tbody>
</table>
# Policy and Governance Measures

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>AUCC Article/s</th>
<th>Relevant Stakeholder/s</th>
</tr>
</thead>
</table>
| - Does the Country have a Cybersecurity Policy which recognises the     | Art 24(1)      | • Presidency  
| Critical Information Infrastructure and identifies the risks to the    |                | • Ministry of ICT  
| nation and mitigation measures?                                         |                | • Ministry of Justice  
|                                                                          |                | • Cybersecurity  
|                                                                          |                |   Academia/Expert  
|                                                                          |                | • Senior ICT legal expert  
|                                                                          |                | • Telecommunications  
|                                                                          |                |   Regulator  |
| - Does the Country have a National Cybersecurity strategy to implement  | Art 24(2)      | • Presidency  
| the Policy?                                                             |                | • Ministry of ICT  
|                                                                          |                | • Ministry of Justice  
|                                                                          |                | • Cybersecurity  
|                                                                          |                |   Academia/Expert  
|                                                                          |                | • Senior ICT legal expert  
|                                                                          |                | • Telecommunications  
|                                                                          |                |   Regulator  |
| - Is the Country engaging in public-private partnerships to engage      | Art 26         | • Presidency  
| industry, civil society, and academia in the promotion and             |                | • Ministry of ICT  
| enhancement of a cybersecurity culture?                                 |                | • Ministry of Justice  
|                                                                          |                | • Law enforcement  
|                                                                          |                | • National CSIRT/ CERT  
|                                                                          |                | • Cybersecurity  
|                                                                          |                |   Academia/Expert  
|                                                                          |                | • Senior ICT legal expert  
|                                                                          |                | • Telecommunications  
|                                                                          |                |   Regulator  |
| - Does the Country have National Cyber Security Monitoring Structures   | Art 27         | • Presidency  
| in place?                                                               |                | • Ministry of ICT  
|                                                                          |                | • Ministry of Justice  
|                                                                          |                | • Law enforcement  
<p>|                                                                          |                | • National CSIRT/ CERT  |</p>
<table>
<thead>
<tr>
<th>QUESTION</th>
<th>AUCC Article/s</th>
<th>Relevant Stakeholder/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the Country have Data Protection Laws and Regulations that cater for the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>→ Exemptions/authorisations for the processing of Personal Data?</td>
<td>Art 10</td>
<td>• Ministry of ICT</td>
</tr>
<tr>
<td>→ The composition and organisation of a National Personal Data Protection Authority?</td>
<td>Art 11</td>
<td>• Ministry of Justice</td>
</tr>
<tr>
<td>→ Duties and powers of National Personal Data Protection Authorities?</td>
<td>Art 12</td>
<td>• Human rights Councils/agencies</td>
</tr>
<tr>
<td>→ Basic principles governing the processing of Personal Data?</td>
<td>Art 13</td>
<td>• Information Regulator</td>
</tr>
<tr>
<td>→ Specific principles governing the processing of Special/Sensitive Personal Data?</td>
<td>Art 14</td>
<td>• Ministry of Trade and Industry</td>
</tr>
<tr>
<td>→ Open access / interconnection of Personal Data files?</td>
<td>Art 15</td>
<td>• International Trade stakeholder</td>
</tr>
<tr>
<td>→ Data subject’s right to information?</td>
<td>Art 16</td>
<td>• Data Protection Academia/Expert</td>
</tr>
<tr>
<td>→ Data subject’s right of access?</td>
<td>Art 17</td>
<td>• Senior ICT legal expert</td>
</tr>
<tr>
<td>→ Data subject’s right to object?</td>
<td>Art 18</td>
<td>• National consumer protection agency</td>
</tr>
<tr>
<td>→ Data subject’s right of rectification or erasure?</td>
<td>Art 19</td>
<td></td>
</tr>
<tr>
<td>→ Confidentiality obligations on Personal Data Controllers?</td>
<td>Art 20</td>
<td></td>
</tr>
<tr>
<td>→ Security obligations on Data Controllers?</td>
<td>Art 21</td>
<td></td>
</tr>
<tr>
<td>→ Storage obligations on Data Controllers?</td>
<td>Art 22</td>
<td></td>
</tr>
<tr>
<td>→ Sustainability obligations on Data Controllers?</td>
<td>Art 23</td>
<td></td>
</tr>
<tr>
<td>QUESTION</td>
<td>AUCC Article/s</td>
<td>Relevant Stakeholder/s</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>How does the Country have Electronic Commerce Laws and Regulations that cater for the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>→ Contractual liability for providers who provide goods/services by electronic means?</td>
<td>Art 3</td>
<td>Ministry of ICT, Information Regulator, Ministry of Trade and Industry</td>
</tr>
<tr>
<td>→ Advertising by electronic means?</td>
<td>Art 4</td>
<td>International Trade stakeholder, Data Protection Academia/Expert</td>
</tr>
<tr>
<td>→ Electronic contracts?</td>
<td>Art 5</td>
<td>Senior ICT legal expert</td>
</tr>
<tr>
<td>→ Electronic writing/signatures?</td>
<td>Art 6</td>
<td></td>
</tr>
<tr>
<td>→ Guaranteeing the security of electronic transactions?</td>
<td>Art 7</td>
<td></td>
</tr>
<tr>
<td>→ Does the Country have Cyber-crime Laws and Regulations that cater for the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>→ The criminalisation of cyber-crime;</td>
<td>Art 25(1) / Art 29</td>
<td>Ministry of ICT, Ministry of Justice, Cybersecurity Academia/Expert</td>
</tr>
<tr>
<td>→ Adapting certain offences to Information and Communication Technologies?</td>
<td>Art 30</td>
<td>Senior ICT legal expert</td>
</tr>
<tr>
<td>→ Adapting certain sanctions to Information and Communications Technologies?</td>
<td>Art 30</td>
<td>International Trade stakeholder</td>
</tr>
<tr>
<td>→ The conferring of statutory authority and legal capacity on a national regulatory authority responsible for all aspects of national cyber security?</td>
<td>Art 25(2)</td>
<td></td>
</tr>
<tr>
<td>→ The protection of critical infrastructure?</td>
<td>Art 25(4)</td>
<td></td>
</tr>
<tr>
<td>→ The enhancement of regional harmonisation and international cooperation?</td>
<td>Art 28</td>
<td></td>
</tr>
<tr>
<td>→ Does the Country have any 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></td>
<td>Presidency, Ministry of ICT, Ministry of Justice, Cybersecurity Academia/Expert, Senior ICT legal expert</td>
</tr>
</tbody>
</table>
### INSTITUTIONAL MEASURES

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>AUCC Article/s</th>
<th>Relevant Stakeholder/s</th>
</tr>
</thead>
</table>
| Does the Country have a Data Protection Authority whose responsibilities | Art 12         | Ministry of Trade and Industry  
| in regulating data protection include: authorisation of data processing,  |                | Ministry of ICT  
| authorisation of cross border transfers of personal data?               |                | Senior ICT legal expert |
| Does the Country have an Electronic Signature Accreditation Authority    | Art 7          | Ministry of ICT  
| that will regulate what constitutes a qualified electronic signature for  |                | Telecommunications Regulator  
| the purposes of authenticating electronic records and other applications?|                | Senior ICT legal expert |
| Does the Country have a State department to regulate and approve        | Art 2.2        | Ministry of ICT  
| electronic commerce payment methods (whereby only approved payment      |                | Telecommunications Regulator  
| methods may be validly used in the Member State territory)?             |                | Senior ICT legal expert |
| Does the Country have a State Department to assessments of ICT product   | Art 25(2)      | Presidency  
| vendors including ensuring mandatory disclosures of vulnerabilities and  |                | Ministry of ICT  
| the solutions to such vendors consumers?                                |                | Ministry of Justice  
|                                                                          |                | Cybersecurity Academia/Expert  
|                                                                          |                | Senior ICT legal expert  
|                                                                          |                | National CSIRT/CERT  
<p>|                                                                          |                | Telecommunications Regulator |</p>
<table>
<thead>
<tr>
<th>QUESTION</th>
<th>AUCC Article/s</th>
<th>Relevant Stakeholder/s</th>
</tr>
</thead>
</table>
| Does the Country have any institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation? | Art 28 | • National CSIRT/CERT  
• International trade stakeholder  
• Ministry of ICT  
• Ministry of Trade and Industry  
• Senior ICT legal expert |
| Does the Country have any institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)? | Art 28 | • National CSIRT/CERT  
• International trade stakeholder  
• Ministry of ICT  
• Ministry of Trade and Industry  
• Senior ICT legal expert  
• Cybersecurity academia/expert |
About Knowledge Partner

This report was prepared independently by 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.

Disclaimer

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.