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 Mauritania 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 fails 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 & Cotter, 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 offenses including offenses 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 of Employment, Vocational Training and New Technologies (MEFPNT) and the Ministry of Interior and Decentralization (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 II considers electronic writing:

- Article 5 of Section I gives electronic writing legal validity, whilst Articles 6 - 15 stipulate formalities in relation thereto;

- Article 9 Section I provides that the creation and use of electronic certificates, must be in accordance with Article 83;

- Article 11 of Section II provides for formalities for the use of electronic certificates.

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 14: Mauritania 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 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 (“NSMAI”) 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 (“DPA”) 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><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><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><strong>Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.</strong></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><strong>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</strong></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>
Disclaimer

This report was prepared independently by EndCode.

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

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

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

About EndCode

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