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.

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. 2008/11 on Cybercrime for the substantive and procedural aspects of cybercrime (Law “2008/11”);  
- 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 adoption 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 (CIs) 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 Ecolin, 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. Therefore:

- 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.
9.5. COMPARISON WITH THE AUCC PROVISIONS ON LAWS, POLICIES AND INSTITUTIONS FOR DATA PROTECTION, CYBERCRIME AND ELECTRONIC TRANSACTIONS.

Table 16: Senegal 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 national 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).  
Electronic Signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications  
State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;  
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)  
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)  |
| National Cybersecurity strategy to implement the Policy  
The Senegalese National Cybersecurity Strategy (SNC2022).  | Electronic Commerce Laws and Regulations  
Law No. 2008/08 on Electronic Transactions.  |
| Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture  | 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.  |  |
Disclaimer

This report was prepared independently by EndCode.

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

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

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

About EndCode

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