# DRAFT NATIONAL DATA GOVERNANCE POLICY

**LIBERIA**

**2026**

# Table of Contents

# Foreword

Data has become a central driver of modern governance, economic transformation, and social development. As Liberia advances its digital transformation agenda, the ability to collect, manage, share, and protect data in a coherent and rights-respecting manner is no longer optional; it is essential to national development, public trust, and regional integration.

This National Data Governance Policy sets out the Government of Liberia's commitment to treating data as a strategic national asset while safeguarding the rights, dignity, and privacy of all Liberians. It provides a coordinated framework to address long-standing fragmentation in data management, strengthen cybersecurity and institutional capacity, and unlock the value of data for inclusive growth, innovation, and effective public service delivery.

The Policy is firmly anchored on Liberia's national priorities and development aspirations. Moreover, the Policy aligns our country's data governance regime with regional and continental frameworks, such as the African Union Data Policy Framework (AUDPF), the African Continental Free Trade Area (AfCFTA), and the Single African Digital Market, as well as relevant African Union instruments on cybersecurity, personal data protection, and emerging technologies. Through this alignment, Liberia reaffirms its commitment to cooperation, integration, and data sovereignty within a rapidly evolving digital economy.

Developed under the leadership of the Ministry of Posts and Telecommunications through an inclusive, multi-stakeholder process, this Policy reflects the contributions of government institutions, the private sector, civil society, the media, academia, and development partners. It responds to practical realities, including the need to improve data sharing and interoperability across government systems, strengthen oversight and accountability over data management, expand digital infrastructure, and build the skills required to participate meaningfully in a data-driven economy.

This National Data Governance Policy is a living framework. Its success will depend on sustained political will, adequate resourcing, strong institutional coordination, and continuous stakeholder engagement. The Government of Liberia remains committed to reviewing and updating the Policy as technologies, risks, and opportunities evolve, ensuring a resilient and future-ready data governance ecosystem.

We call upon all stakeholders to work collectively in operationalising this Policy so that data is harnessed responsibly to strengthen governance, drive inclusive economic growth, and position Liberia as a trusted participant in the African and global digital economy.

Hon. Sekou M. Kromah
Minister of Posts and Telecommunications
Republic of Liberia

# Acknowledgements

This National Data Governance Policy has been developed by the Ministry of Posts and Telecommunications, guided by a set of national data priorities, which include strengthening cybersecurity, improving fragmented data systems, building institutional capacity, and leveraging data for inclusive economic growth.

This policy was developed with the support of the German Agency for International Cooperation (GIZ) to the African Union and the AU Development Agency-NEPAD (AUDA-NEPAD). Technical assistance was provided by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA).

# List of Abbreviations

| | |
|---|---|
| ACE: | Africa Coast to Europe |
| AfCFTA: | African Continental Free Trade Agreement |
| AMP: | Aid Management Platform |
| API: | Application Programming Interface |
| ATI: | Access to Information Act |
| AU: | African Union |
| AUDPF : | African Union Data Policy Framework |
| CBL: | Central Bank of Liberia |
| CEMESP: | Center for Media Studies and Peacebuilding |
| CERT: | Computer Emergency Response Team |
| D4WEE: | Digital Inclusion for Women's Economic Empowerment |
| DPI: | Digital Public Infrastructure |
| DPPA: | Personal Data Protection and Privacy Act |
| DTWG: | National Digital Transformation Working Group |
| ECOWAS: | Economic Community of West African States |
| EMIS: | Education Management Information System |
| EU: | European Union |
| FOI: | Freedom of Information |
| FSDIP: | Financial Sector Development Implementation Plan |
| G2B: | Government-to-Business |
| GDP: | Gross Domestic Product |
| GDPR: | General Data Protection Regulation |
| GREAT: | Governance Reform and Accountability Transformation |
| HMIS: | Health Management Information System |
| ICT: | Information and Communication Technology |
| IFMIS: | Integrated Financial Management Information System |
| IGMS: | International Gateway Monitoring System |
| IIC: | Independent Information Commission |
| IIPS: | Liberian Inclusive Instant Payments System |

| | |
|---|---|
| LiSA: | Liberia Standards Authority |
| LISGIS: | Liberia Institute of Statistics and Geo-Information Services |
| LLA: | Liberia Land Authority |
| LTA: | Liberia Telecommunications Authority |
| LYDTI: | Liberia Youth Digital Transformation Initiative |
| M&E: | Monitoring and Evaluation |
| MACs: | Ministries, Agencies, and Commissions |
| MGCSP: | Ministry of Gender, Children and Social Protection |
| MoJ: | Ministry of Justice |
| MoPC: | Ministry of Posts & Telecommunications |
| MSMEs: | Micro, Small, and Medium Enterprises |
| NIR: | National Identification Registry |
| NSDI: | National Spatial Data Infrastructure |
| ODA: | Official Development Assistance |
| PUL: | Press Union of Liberia |
| SADM: | Single African Digital Market |
| STEM: | Science, Technology, Engineering, and Mathematics |
| UNCTAD: | United Nations Conference on Trade and Development |
| WACREN: | West African Research and Education Network |

# Executive Summary

The National Data Governance Policy 2026 is set to leverage efforts built on galvanising data as a national asset that promotes socio-economic development and digital transformation. This policy is part of the commitments and processes by the Liberian government to align Liberia's data governance frameworks with the regional, continental and international data governance frameworks. These frameworks include among others, the African Union Data Policy Framework, African Continental Free Trade Agreement (AfCFTA) and the Single African Digital Market (SADM), Continental Artificial Intelligence Strategy, 2024, and the Africa Union Convention on Cybersecurity and Personal Data Protection.

The policy was developed under the leadership of the Ministry of Post and Telecommunications through a consultative process. It is built on a multi-step and multi-stakeholder consultative process involving legal and policy analysis of Liberia's data governance legal and policy framework to identify gaps and draw up recommendations to bridge them. In addition, there were stakeholder consultations with government officials from several government ministries, agencies and commissions, the private sector, civil society organisations, media, academia and development partners.

Built on the need to build a robust data governance regime that is not only inclusive but fosters coordination and cooperation to promote data integration, data sovereignty and cross border data flows, the policy focuses on:

- Promoting data-driven decision-making;
- Improving data quality and availability;
- Fostering innovation and economic growth;
- Enhancing security, transparency, accountability, and
- Protecting personal data and individuals' privacy rights

The Policy identifies the gaps in data governance in Liberia and proposes several actions and reforms that will lead to maximisation of benefits from datafication and digitalisation. Amongst the key actions include enactment of laws and adoption of policies that address data protection, signing and ratification of key regional and international data protection instruments, building stronger and independent institutions to oversee data protection, digital education, literacy and awareness raising, expansion of digital connectivity throughout the country, gender mainstreaming and wide civil society engagement.

Liberia is committed to unlocking the potential of data to foster, promote and enhance digitalisation, digital transformation and socio-economic development. Every effort will be undertaken to ensure harmonisation of national laws and policies with the regional and international data governance standards.

# 1.0 INTRODUCTION

## 1.1 Background and Overview

Since 2018, the Government of Liberia has undertaken efforts to transform public service delivery and administration as a holistic approach to expanding the public sector capacity. In 2019, the government adopted the Information and Communications Technology (ICT) Policy (2019-2024), which focused on three pillars: Structure, Empower, and Transform (SET). These pillars position ICT as an integrated driver of economic growth, transformation, and social inclusion. Despite these efforts, there are still notable challenges to service delivery in the country, and digitalisation is yet to be definitively leveraged for socio-economic transformation.

As elsewhere across the world, data is increasingly recognised as a valuable asset and public good crucial for improved public service delivery, innovation, and socio-economic transformation of Liberia. However, in order for Liberia to realise this potential, it is crucial that the country has clear and deliberate regulations governing how data is collected, stored, shared, and re-used. Such regulations should also address critical concerns related to privacy, security, ethics, equity, and national sovereignty that are posed by the rapid growth of digital technologies and data-driven systems. Equally important is the need for Liberia's policy to reflect regional and international human rights standards and best practices, such as the African Union Data Policy Framework.

Accordingly, the Ministry of Posts and Telecommunications (MoPT), in partnership with the African Union Commission (AUC), has developed this National Data Governance Policy which aligns with the African Union Data Policy Framework. Developed in collaboration with the private sector and civil society organisations, this Policy establishes a policy framework for the protection, promotion and enhancement of responsible use of data for digital transformation and socio-economic development.

This Data Governance Policy complements various national laws and strategies that aim to leverage trusted, inclusive technology for socio-economic transformation. These include the National Cybersecurity Strategy (2024–2029), which aims to build, protect and sustain cybersecurity standards in the country. The strategy prioritises the development and adoption of robust legal and regulatory frameworks, ensuring sustainable funding, and strengthening cybersecurity skills. However, Liberia still faces challenges, notably with data sharing and data interoperability across government agencies.

Nationwide digital infrastructure is necessary to support connectivity and digital services. Liberia is connected to global fiber-optic connectivity through the Africa Coast to Europe (ACE) cable. This infrastructure is the key supplier of backbone connectivity for the country's telecommunication companies, notably Orange Liberia, Lonestar Cell MTN, and CSquared.

The Government of Liberia's Network (GovNet) is the main channel for connecting the more than 107 Ministries, Agencies, and Commissions (MACs).[1] However, GovNet faces several challenges, including cybersecurity vulnerabilities, limited infrastructure, such as the absence of a centralised data centre, inadequate technical capacity, weak infrastructure governance structures, and inadequate backup systems, and vulnerability to common digital security threats.

[1] N.E. Wreh, 'Investigating the Cybersecurity Aspects of the Liberian Government's Network (GovNet) as a Critical National Infrastructure' (2023) 13 Advances in Data Science and Adaptive Analysis 1, https://www.worldscientific.com/doi/10.1142/S2424922X21500078

In terms of e-commerce, Liberia is still in its early stages of development. Strengthening e-commerce readiness is essential for economic growth and development, especially for Micro, Small, and Medium Enterprises (MSMEs), as well as marginalised groups such as the youth and women. The growth of e-commerce requires the implementation of various digital transformation strategies and policies, and a unified national e-commerce platform. Initiatives such as the Digital Inclusion for Women's Economic Empowerment (D4WEE) project demonstrate how technology can bridge financial inclusion gaps among rural women by connecting them to broader markets through mobile money.[2]

Mobile money is indeed an essential component for promoting the growth of Liberia's digital infrastructure[3] However, progressive reforms are required to transform the financial sector. In this regard, the Central Bank of Liberia (CBL), with support from the World Bank, developed a Financial Sector Development Implementation Plan (FSDIP) as the roadmap for developing the sector. Related to this is the need to develop an intelligent, scalable, and interoperable Digital Public Infrastructure (DPI) to improve the livelihoods of the citizens by enhancing digital financial inclusion.[4] These efforts would require a robust data governance system to ensure the protection of Liberians' financial data.

E-governance is essential to enhance accountability, transparency, and efficiency in public service delivery. The e-Government Strategy (2014–2018) set out to deliver customer-centred services through four defined channels, including a Portal, Call Centre, Mobile devices, and Citizen Computer Centres. The core of the strategy was an Integrated Financial Management Information System (IFMIS), which would provide a centralised e-government portal for e-procurement and electronic payments, including mobile money, and help to weed out corruption in government service delivery.

Lastly, skills and capacities of citizens to utilise technology and tech-enabled services are a requirement for progression in development. Digital empowerment of citizens and businesses through addressing the skills gap is amongst the central pillars of the National Digital Strategy.[5] The 10k Youth Digital Transformation Project was launched to cover 10,000 young people by skilling them in digital technology marketing and eminently bridge the digital divide.[6] This has been coupled with nationwide digital literacy and awareness-raising campaigns in dealing with common cybersecurity threats. The Liberia Youth Digital Transformation Initiative (LYDTI) also aims to contribute to digital literacy amongst the young people and enhance their civic engagement.

## 1.2 The Data Governance Landscape in Liberia

Liberia's legal and regulatory framework for data protection remains fragmented. The Constitution of Liberia of 1986 provides for the right to privacy under article 16. The Telecommunications Act of 2007 provides for safeguarding of customer information under section 51, while the National ICT Policy of

[2] UN Women, 'Empowering Rural Women in Liberia Through Digital Inclusion' (Factsheet, 2024) p 2, https://africa.unwomen.org/sites/default/files/2025-01/20240703_un_women_liberia_eng_webpages.pdf

[3] UNCTAD, 'Case Study on Liberia's Digital Infrastructure' (UNCTAD, 7 October 2025), https://www.uneca.org/case-study-on-liberia%E2%80%99s-digital-infrastructure

[4] International Journal of Economics, Business and Management Research, 'Digital Public Infrastructure, the Building Blocks for Digital Financial Inclusion and Taxation of the Digital Economy in Liberia' (IJEMBR, 12 November 2025) p 4, https://ijebmr.com/uploads/pdf/archivepdf/2025/IJEBMR_1748.pdf

[5] Ministry of Posts and Telecommunications, 'Government of Liberia - National Digital Strategy' (MoPT, 2025) p 16, https://mot.gov.gm/wp-content/uploads/2025/11/Liberia-National-Digital-Strategy.pdf

[6] Ministry of Posts and Telecommunications, 'Official Launch of the 10k Youth Digital Transformation Project' (MoPT, 1 May 2024), https://mopt.gov.lr/official-launch-of-the-10k-youth-digital-transformation-project/

2009 provides various principles for lawful processing of personal data, including fair use. Meanwhile, the Central Bank of Liberia (CBL) Payment System Act of 2014 provides the legal framework for regulation, supervision and development of a safe and efficient national electronic payment infrastructure.[7] However, these provisions are scattered across multiple legal instruments and are insufficient to offer comprehensive guidance on the collection, safeguarding and utilisation of data. They also fall short of positioning data as a key tool for economic growth and social transformation.

In recognition of these gaps, the Government of Liberia has taken steps to strengthen its digital policy and legislative landscape. Key among these efforts are the Cybercrime Act, 2025, which was passed by the Senate, and the Personal Data Protection and Privacy Act of 2024, which is yet to be passed. These legislative initiatives reflect the government's commitment to strengthening data governance and digital trust.

## 1.3 Data Governance Related Initiatives

Besides the ongoing efforts to strengthen the legislative framework, the government has also undertaken complementary initiatives towards enhancing digital and data governance. These include the establishment of the National Data Center and the development of the National Digital Strategy in 2025.

### 1.3.1 The National Data Center

The National Data Center, located at the state-owned national operator LTC-Mobile, is spearheaded by the Ministry of Posts and Telecommunications to establish robust, secure data centres for government and private sector use. It is being upgraded under the World Bank Project known as the Governance Reform and Accountability Transformation (GREAT) Project. The initiative is intended to improve public services, strengthen tax collection, and enhance government transparency. It targets institutions such as the Liberia Revenue Authority and the Civil Service Agency. The Data Center, when upgraded, will enhance national data storage capacity.

### 1.3.2 The Digital Forensic Lab

The Digital Forensic Lab (DFL), led by the Ministry of Posts and Telecommunications (MoPT), with support from the ECOWAS Commission on Infrastructure and Digitalization, is expected to become operational soon. Hosted by the Liberia National Police Training Academy, the lab will enhance digital security and legal infrastructure and investigate crimes that are committed using digital devices. Its core objectives include to foster evidence collection and analysis, support criminal prosecutions, promote regional cooperation, and enhance national security protection.

### 1.3.3 Data Management Oversight Institutions

Data management and oversight in Liberia are characterised by institutional fragmentation, which underscores the need for a coordinated, multi-sectoral approach to data governance oversight. The

[7] Central Bank of Liberia (CBL) Payment System Act of 2014, https://www.cbl.org.lr/sites/default/files/documents/payment%20systems%20act.pdf

Personal Data Protection and Privacy Act of 2024 is expected to introduce a unified data governance system in the country.

Today, the responsibility for data protection and governance is spread across multiple administrative and regulatory bodies, each overseeing specific data sets and sectors. At the top, the MoPT is the oversight ministry that holds overall responsibility for data governance, and it has spearheaded efforts to enact a specific data protection law. The Ministry has also developed the National Digital Strategy (2025–2029), which complements national data governance and digitalisation efforts.

The Liberia Telecommunications Authority regulates the communications sector and is responsible for enforcing the quality of services and managing the International Gateway Monitoring System (IGMS), which is used for tracking revenue flows and checking fraud. Its role in data governance includes enforcing cybersecurity standards and managing national digital infrastructure. On the other hand, the National Digital Transformation Working Group (DTWG) is charged with driving digital reforms and coordinating the transformation of government Ministries, Agencies, and Commissions (MACs).

The different sectoral data managers in Liberia include the Central Bank of Liberia (CBL), which governs digital financial data. It has taken steps to promote interoperability of financial data through the Liberian Inclusive Instant Payments System (IIPS). The Liberia Institute of Statistics and Geo-Information Services (LISGIS), established by the National Statistics and Geo-Information Act of 2004, is responsible for managing national statistical data and geospatial information, including through coordination, standard setting and safe custody of data.

Additional sectoral data managers include the Ministry of Labour, which oversees labour market data such as employment and unemployment statistics; the Ministry of Health, which manages health data primarily through the Health Management Information System (HMIS); and the Ministry of Education, which oversees education data through the Education Management Information System (EMIS).

# 2.0 DEFINITIONS

To create a data governance framework that is inclusive, trustworthy, and cohesive, there must be a common understanding of the fundamental concepts covered by the Policy . This section therefore outlines the definitions that guide the interpretation and application of this Policy. Establishing a shared meaning across MACs, sectors, and stakeholders facilitates data governance by reducing ambiguity, enhancing coordination, and encouraging accountability in the management and use of data.

The terms and concepts in this policy should be interpreted in light of the Republic of Liberia's Constitution, existing national laws, and relevant regional and international agreements, including the African Union Data Policy Framework. The definition of a term from the relevant law will be used unless this Policy specifies otherwise.

**Anonymisation** is the removal of direct and indirect personal identifiers from data**.**

**Biometric data** means personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition.

**Cloud services** are used on-demand at any time, through any access network, using any connected devices that use cloud computing technologies. They utilise software and applications located on the cloud and not on users' own devices.

**Cloud-based services** include mass-market applications (e.g., social media and webmail, such as Facebook and GMail) offered over the internet. The data does not sit on individuals' devices but is stored remotely in a data centre.

**Competition** means actual or potential competitor.

**Cross-border data flows** refers to the movement or transfer of information between servers located in different countries.

**Cybercrime** refers to unlawful acts that affect the confidentiality, integrity, availability, and survival of information and communication technology systems, the data they process, and the underlying network infrastructure.

**Cybersecurity** refers to the body of technologies, processes, and practices designed to protect networks, devices, programmes, and data from attack, damage, or unauthorised access to protect and preserve the fundamental principles of confidentiality, integrity, and availability.

**Data** refers to a collection of facts, statistics, information, or any pieces of knowledge that are recorded, stored and can be processed, or analysed. There are various forms of data, such as numbers, text, images, audio, video, and more. Data can be raw and unprocessed (for example, a list of numbers), or it can be processed and organised into meaningful information. In computing and technology, data is often defined as digital information stored in electronic devices or systems.

**Datafication** refers to the process by which daily interactions of living things can be rendered into a data format and put to social and economic use or value.

**Data classification** is the categorising and labelling process used to differentiate data based on its level of sensitivity, importance, access permissions and security requirements.

**Data collection** is the process of gathering and capturing information or data from various sources for the purpose of analysis, research, decision-making, or record-keeping. It involves systematically collecting data or information about specific variables, individuals, events, or phenomena to create a dataset that can be used for various purposes

**Data controller** means any natural or legal person, public or private, any other organisation or association that alone or jointly with others, decides to collect and process personal data and determines the purposes.

**Data ecosystem** as used here refers to the programming languages, packages, algorithms, cloud-computing services, and general infrastructure an organisation uses to collect, store, analyse, and leverage data as well as to the underlying value chain associated with data as a factor of production, the governance of data systems and the protection of data subjects.

**Data Governance** is a comprehensive framework and set of practices that aim to ensure the effective management of data in a country. The primary objectives of data governance are to maintain the quality, availability, security, and integrity of data assets. It entails the establishing and maintaining control over the collection, storage and processing, utilising, dissemination, and disposal of data.

In national contexts, data governance is designed to enable countries to leverage data effectively for informed decision-making, by cultivating a culture where data is valued as a strategic asset, encouraging transparency and accountability in data-related activities. This approach enhances the efficiency of data management, fosters a data-driven culture, and contributes to better decision-making across various sectors and industries. The technological aspect of data governance emphasises interoperability, standardisation, and responsible development of data-related technologies. This ensures seamless communication between systems and actors, promotes efficiency, and supports ethical innovation.

**Data protection** regulates how data is used or processed and by whom, and ensures citizens have rights over their data. It is particularly important in ensuring digital dignity, as it can directly address the inherent power imbalance between “data subjects” and the institutions or people who collected data.

**Data protection authorities** are independent public authorities that monitor and supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints that may have breached the law.

**Data Sharing** is the process of making the same data resources available to multiple applications, users, or organisations.

**Data sovereignty** draws on the concept of the sovereign nation state. As articulated in the African Union Data Protection Framework, it refers to the view that data that is generated in or passing through national internet infrastructure should be protected and controlled by that state.

**Data subject** means an identified or identifiable living individual to whom personal data relates. An "identified" or "identifiable" individual means:

(a) A person who can be identified directly or indirectly, in particular by reference to an identification number or one more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity;

(b) To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the said person;

(c) An individual is "identifiable" if the processing allows the individual to be "singled" out from other individuals;

**Digital identity** is a set of electronically captured and stored attributes and/or credentials that uniquely identify a person, enabling the distinction of one individual from another. It may be government issues (e.g., national eID) or platform-based (e.g., login credentials).

**E-commerce** refers to commercial transactions that occur through electronic channels, including buying and selling of goods or services via the internet and the transfer of money and data to complete the sales, by methods specifically designed for the purpose of receiving or placing orders.

**Foundational data infrastructure** refers to advanced technologies which facilitate the intensive use of quality data. This may include broadband networks, internet exchange points, data centres and cloud services, electronic hardware and software, and digital applications available on the internet.

**Harmonisation** is ensuring uniformity in data systems through the use of minimum standards to facilitate interoperability and creating legal and trust frameworks (e.g. for levels of assurance) that set rules and build confidence in the respective systems.

**Interoperability** is the ability of different function units, such as systems, databases, devices, or applications, to communicate, execute programmes, or transfer data in a manner that requires the user to have little or no knowledge of those functional units.

**Metadata** is structured reference data that describes other data. It helps to sort and identify the attributes of the information it describes.

**Ontologies** are a way of systematically organising structured and unstructured data using entities, properties, and relationships.

**Open data** refers to data that anyone can freely access, use, modify, and share for any purpose.

**Personal data** refers to any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly, particularly by reference to an identification number or factors specific to their physical, physiological, mental, economic, cultural, or social identity. It includes direct identifiers such as names, addresses, email addresses, phone numbers, and national ID or passport numbers, as well as special or sensitive data such as biometric data, health records, and information about race, ethnicity, or political opinions.

**Processing or Data Processing** means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as

(a) collection, recording, organisation, structuring;

(b) storage, adaptation or alteration;

(c) retrieval, consultation or use;

(d) disclosure by transmission, dissemination, or otherwise making available; or

(e) alignment or combination, restriction, erasure or destruction.

**Public data** means all information and data held by the government and its entities that can be freely used, reused and redistributed by anyone with no existing local, national or international legal restrictions on access or usage.

**Sensitive data** means all personal information relating to religious, philosophical, political opinion as well as to sex life, race, and health, social conditions of the data subject.

**Taxonomies** are a way of organising data in a Hierarchical Structure with a tree-like structure with parent-child relationships. Each level is more specific than the one above it.

# THE POLICY

# 2.0 POLICY VISION, OBJECTIVES AND PRIORITIES

## 2.1 Vision

To establish Liberia as a digital economy in which data serves as a protected strategic national asset that bridges the digital divide, enhances government transparency, and accelerates socio-economic development for all citizens.

## 2.2 Mission

To establish and implement a coordinated, transparent and accountable national data governance framework that safeguards the sovereignty, security and integrity of data; protects the rights and privacy of Liberians through effective oversight; and enables responsible data use to support sustainable national development.

This Policy is built on the principle of data as a national asset and a catalyst for socio-economic development and digital transformation. It complements the National ICT Policy (2009), the National Cybersecurity Strategy (2024–2029), and the National Digital Strategy (2025–2029). Its development forms part of Liberia's effort to align its data governance framework with the African Union Data Policy Framework.

## 2.3 Policy Priorities

Liberia envisions a centric-national national data ecosystem in which data serves as a strategic asset for advancing good governance, empowering citizens, and catalysing economic development and digital transformation. With the adoption of the Data Governance Policy, Liberia seeks to establish a secure, interoperable and well-regulated data framework that supports digital evolution and inclusive economic transformation.

The specific priorities are:

**i) Strong Institutions and Governance:** Liberia will build clear institutional structures and accountability frameworks for data governance, ensuring coordinated action across government, private sector, and civil society. Defined roles, responsibilities, and inter-agency collaboration will foster transparency, efficiency, and public trust in how data is managed.

ii) **Privacy, Security, and Trust:** Protecting personal and sensitive data is central to this Policy. Liberia will strengthen legal frameworks, cybersecurity measures, and ethical practices to safeguard citizens' rights, enhance compliance, and build public confidence in digital services.

iii) **Interoperability and Standards:** Seamless, secure data exchange is critical for an effective national data ecosystem. Liberia will adopt shared technical standards, metadata frameworks, and open APIs to ensure data is accurate, consistent, and usable, supporting evidence-based decisions and enabling innovation across sectors.

iv) **Digital Infrastructure and Access:** Reliable and inclusive digital infrastructure underpins Liberia's socio-economic transformation. Expanding data centres, cloud services, broadband networks, and other foundational systems will ensure equitable access to digital services,

strengthen e-governance, and enable citizens and businesses to fully participate in the digital economy.

v) **Capacity Development and Digital Literacy:** Human and institutional capacity is key to unlocking the value of data. The Policy prioritises training, awareness, and digital literacy initiatives that equip public servants, private actors, and citizens to manage, interpret, and use data responsibly, empowering informed participation across the national ecosystem.

vi) **Innovation and Entrepreneurship:** Data will drive innovation, entrepreneurship, and socio-economic development. Liberia will facilitate access to non-sensitive data, support emerging technologies like AI, the Internet of Things (IoT), and blockchain, and create a conducive policy environment for research and data-driven enterprises that support inclusive growth.

vii) **Regional and International Alignment:** Liberia's data governance framework will align with continental standards, including the African Union Data Policy Framework, AU Cybersecurity and Data Protection Convention, AfCFTA, and the Single African Digital Market. This will enable responsible cross-border data flows, protect national sovereignty, and strengthen Liberia's participation in regional digital integration.

This Policy framework adopts a principle-based approach that is informed by regional and international best practices, particularly neighbouring states and the AU Member States, that promote coordinated data governance, support data sovereignty, and enable cross-border data flows as a foundation for Liberia's holistic socio-economic transformation.

## 2.4 Policy Objectives

The National Data Governance Policy recognises data as a strategic national asset that can foster inclusive digital transformation, socio-economic progress, and responsible governance in Liberia. It envisages a robust and secure data governance regime that supports innovation, is inclusive, and promotes safety in data collection, processing, and sharing. To realise the Priorities outlined above, the Policy sets the following objectives:

| **No**. | **Objective** | **Description** |
|---|---|---|
| 1 | **Create a clear and coordinated framework for data governance** | Ensure all data, both public and private, is managed under clear, consistent rules and institutional arrangements |
| 2 | **Protect privacy, security, and citizens' rights** | Keep personal and sensitive data safe, and build confidence among citizens that their information is handled responsibly |
| 3 | **Make data reliable, connected, and useful** | Support seamless sharing of high-quality data across government, the private sector, and civil society to inform better decisions |
| 4 | **Strengthen infrastructure and expand access** | Build and maintain the digital backbone, including data centres, cloud systems, and broadband, so all Liberians can benefit |

| | | |
|---|---|---|
| 5 | **Develop skills and digital understanding** | Equip individuals and organisations with the know-how to collect, manage, and use data responsibly and effectively |
| 6 | **Encourage innovation, research, and economic opportunity** | Use data to drive new ideas, technology solutions, and entrepreneurship while ensuring fairness and inclusivity |
| 7 | **Align with regional and continental standards** | Follow African Union frameworks, enabling cross-border collaboration while protecting Liberia's data sovereignty |

## 2.5 Policy Guiding Principles

These guiding principles outline the standards and values that will guide how this National Data Governance Policy will be implemented and applied. They demonstrate Liberia's commitment to protecting rights, upholding national sovereignty, and using data responsibly to promote inclusive development, and are in line with the African Union Data Policy Framework.

| | |
|---|---|
| **Cooperation** | Liberia shall, subject to national sovereignty, cooperate with African countries and other jurisdictions in the exchange and use of data. The Policy acknowledges data as a driver of the African and global economy, and supports the harmonisation of data regulation and the interoperability of data systems to support regional integration, including the development of a single African Digital Market. |
| **Integration** | Promote intra-Africa data flows, including by removing legal barriers to data flow, subject to the relevant security, human rights and data protection standards and requirements. |
| **Fairness and Inclusiveness** | Ensure inclusive and equitable implementation of the national data governance ecosystem to address social and structural inequalities, and protect vulnerable and marginalised groups from algorithmic bias and from exclusion in technological development and emerging digital technologies. |
| **Trust, Safety and Accountability** | Promote a trustworthy and secure data environment and ecosystem that is ethical by design, transparent, and accountable to data subjects. |
| **Sovereignty** | Establish policy, legal and regulatory data governance measures to effectively govern data, and to take advantage of the digital economy and digital transformation opportunities, including data flows. |

| | |
|---|---|
| **Comprehensive and Forward-Looking** | Create a harmonised data governance framework that promotes data-enabled innovation and investment in the development of infrastructure and human capacity. |
| **Integrity and Justice** | Ensure data is collected, processed, and used lawfully, fairly, and without discrimination, upholding human rights and dignity. |
| **Interoperability** | Ensure all new government digital standards adhere to open API standards and harmonisation, and are built to exchange data without proprietary limitations and significant integration costs. |
| **Privacy and Security by Design and Default** | Technical systems must be configured to minimise data collection to what is strictly necessary. Security measures such as encryption at rest and in transit must be enabled automatically, and not treated as optional. Likewise, critical national information infrastructure must be protected from cyber threats to ensure business continuity and digital resilience. |

## 2.6 Scope and Application of the Policy

This Policy applies to:

i) All public sector institutions, including ministries, agencies, commissions, and local governments.

ii) All private sector entities, civil society organisations, and other entities based in Liberia that collect or process personal data in the country.

iii) Foreign entities that process data relating to individuals or activities within Liberia.

iv) The general public

### 2.6.1 Data Covered

This Policy covers the following types of data[8]:

i) Personal data
ii) Sensitive personal data

iii) Non-personal data
iv) Public sector data

[8] For definitions of the different types of data, refer to the Definitions on pages 13-16.

# 3.0 CURRENT LEGAL AND POLICY FRAMEWORK FOR DATA GOVERNANCE

Liberia's data governance system is currently in its early stages of development. Existing provisions related to data governance, privacy, and data protection are scattered across multiple legislative and policy instruments. For consistency, accountability, and public trust to be maintained, a robust and enforceable data governance regime needs a well-defined legal basis that is in line with regional and global standards. This Policy builds upon existing and emerging legislation to provide such guidance.

## 3.1 Existing Policy Instruments

Liberia has adopted several policy instruments that contribute to the data governance landscape. These include:

- The National Digital Strategy (2025–2029), whose main focus is digital governance and cybersecurity. It also focuses on establishing a Data Marketplace to promote the safe use of data for economic growth and development.
- The National ICT Policy (2019–2024), which was extended to 2025, focuses on the structure, empowerment and transformation of the ICT sector. It promotes the expansion of e-government services and recognises data protection as a central pillar of cybersecurity.
- The National Cybersecurity Strategy (2024–2029) seeks to build, protect, and sustain the country's critical information infrastructure and cybersecurity standards.

Collectively, these regulations demonstrate Liberia's dedication to digital transformation. Yet, these laws are not comprehensive enough to ensure a robust data governance landscape. For consistency, enforceability, and alignment with the African Union Data Policy Framework, a comprehensive data governance framework is required. This Policy closes that gap by linking strategic priorities with current and planned legal frameworks.

## 3.2 Existing Legislation

Several existing laws contain provisions that are relevant to data protection and governance.

**The Constitution of Liberia of 1986** provides for the right to privacy under **Article** 16. It provides that "No person shall be subjected to interference with his privacy of person, family, home or correspondence except by order of a court of competent jurisdiction." Under Article 2, the Constitution is the supreme law of Liberia, and its provisions have binding force on all authorities and persons throughout the Republic.

**The Freedom of Information (FOI) Act, 2010,** provides for the right of everyone to access information held by public bodies, subject to narrowly defined limitations s. Nevertheless, section 4.5 exempts access to documents or records that potentially constitute an unreasonable disclosure of personal information. This section specifically provides that, "Personal Information: A document or record is exempted from the general right of access if its disclosure would constitute an unreasonable disclosure of the personal information." However, it is important that the protection of personal data is not used as a reason to restrict access to non-personal public information.

**The Liberia Telecommunications Act, 2007** regulates the telecommunications sector and provides for an effective and efficient sector that promotes social and economic development throughout Liberia.

Under section 2(5), the Act addresses the proper handling of customers' data, which is expressly subject to laws, regulations, standards or guidelines.

**The Electronic Transactions Law, 2002,** facilitates the use of electronic transactions for commercial purposes. It provides a framework for a data-driven sector where electronic contracts have similar legal effects as paper-based contracts.

**The Central Bank of Liberia e-Payment Regulations** issued by the Central Bank of Liberia provide a framework for mobile money operations and require banks to respect customers' privacy by strictly adhering to confidentiality statements when dealing with the customers' account information.

Although the above laws and regulations address certain aspects of data governance, they fall short of constituting a comprehensive data protection and governance regime. They are fragmented, mostly have a sector-specific reach, and do not offer clear accountability mechanisms or unified oversight for national data lifecycle governance.

## 3.3 Emerging Legislation

In order to buttress the legal framework on data governance, the Government of Liberia has drafted two key laws, although they are yet to be enacted. These are the Personal Data Protection and Privacy Act of 2024 and the Cybercrime Act 2025.

### 3.3.1 Personal Data Protection and Privacy Act of 2024

Liberia is in the process of enacting the Personal Data Protection and Privacy (PDPP) Act of 2024. The law seeks to provide a unified framework for the collection, processing, and protection of personal data. Once enacted, the law will apply to the processing of all types of personal information and to any natural and juridical person involved in processing the personal information of residents of Liberia, including processing activities conducted within or outside the country.

The enactment of this law will be a major step in bringing Liberia closer to regional frameworks, such as the African Union Data Policy Framework and the ECOWAS Supplementary Act, 2010 on Personal Data Protection.

***Policy Prescriptions***

It is recommended that the Government should undertake the following actions:

1. Prioritise and expedite the adoption of the PDPP 2024, to address data protection challenges in the country. This will bring Liberia into compliance with the ECOWAS Supplementary Act, 2010 on Personal Data Protection.
2. Amend the proposed law to ensure it is aligned with the African Union Data Policy Framework, the ECOWAS Supplementary Act on Personal Data Protection and the Malabo Convention on Cyber Security and Personal Data Protection. Aligning its laws with these regional instruments will help Liberia to promote digital trade and regional integration since Liberia's laws will be harmonised with those of other countries.
3. Sign and ratify the Malabo Convention on Cyber Security and Personal Data Protection to demonstrate commitment to the continental treaty and take necessary measures to establish legal frameworks for data protection and cybersecurity.

4. Integrate provisions for data literacy and raising awareness to educate and empower citizens and businesses on data rights and principles in order for them to meaningfully participate in data-driven decision-making.
5. Develop sector-specific guidelines and conduct awareness campaigns to operationalise the PDPPA and promote compliance across all sectors.

### 3.3.2 Cybercrime Act 2025

The Cybercrime Act 2025 aims to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Liberia. It further aims to ensure protection of the critical national information infrastructure and promote cybersecurity and protection of computer systems and networks, electronic communications and intellectual property and privacy rights.

This Bill is in its final stages of becoming fully operational following its adoption by the Senate in November 2025. Among its key provisions, the proposed law requires that data breaches are reported to the authorities within **72 hours** of discovery. It also criminalises unauthorised data interference and identity theft.

Once it comes into force, the Cybercrime Act 2025 will mark a significant step toward strengthening Liberia's cybersecurity, building digital trust, and complementing the data governance framework.

***Policy Prescriptions***

The Government shall:

1. Expedite the operationalisation of the Cybercrime Act, including the establishment of the Liberia National CERT, the development of technical standards, and international cooperation mechanisms.
2. Develop a framework for protecting critical information infrastructure in line with the Act and international standards e.g. ISO 27001.
3. Develop cyber hygiene awareness programmes for government officials and the general public to strengthen national digital resilience.

## 3.4 Fair Competition

Fair competition is increasingly central to digital growth and transformation in Liberia. It is necessary for the shift from a heavily monopolised data marketplace to an inclusive one. According to the National Digital Strategy (2025–2029), non-personal public data in sectors such as agriculture, transport, and trade should be accessible to all sector players, including SMEs, to promote fair competition.

***Policy Prescription***

The Government shall:

- Establish a competitive environment where data as a national asset is equally accessed and utilised to bring precision in socio-economic development and digital transformation.

# 4.0 GOVERNANCE AND INSTITUTIONAL MEASURES

Clear institutional mechanisms that create clear distinctions between the roles of policy makers, regulators, and other stakeholders are key to effective data governance. They guide the practical implementation of data regulations and standards and promote consumer protection and accountability in the data ecosystem.

Because of the importance of data protection, there should be a dedicated institution mandated with oversight of personal data and non-personal data. However, there is no institution in Liberia that is currently charged with the responsibility of overseeing data management and governance. Creating a standalone Data Protection Agency, as some countries have done, requires significant investment, legislative time, and administrative overhead. Recognising Liberia's fiscal constraints and the scarcity of specialised technical talent, it is important to leverage existing institutions to operationalise this policy.

The institutional arrangements outlined below are designed to facilitate data coordination, accountability and transparency, while supporting social and economic development through a trusted data governance system.

## 4.1 Ministry of Posts and Telecommunications (MoPT)

The MoPT retains the role of the primary policy architect and convener of Liberia's digital ecosystem. Its responsibilities include implementation of the National Digital Strategy (2025–2029), ensuring Liberia aligns with AU and ECOWAS protocols on digital governance and data protection; and convening the inter-ministerial committees and facilitating alignment of strategic priorities across government agencies.

## 4.2 Extending the Mandate of the Independent Information Commission (IIC)

The Independent Information Commission (IIC) is mandated by section 5.1 of the Freedom of Information Act, 2010, to oversee the implementation of the Act, including the receipt and handling of any complaints related to access to information. According to the proposed Personal Data Protection and Privacy Act of 2024, the IIC mandate is extended to oversee the processing of personal data.

Under section 8 of the proposed Personal Data Protection and Privacy Act of 2024, the IIC will implement the provisions of the law, monitor and ensure the country's compliance with international standards and best practices for data protection and privacy.

The IIC's mandate shall include receiving complaints, instituting investigations, facilitating dispute resolution and award of remedies on matters affecting any personal information.

Data Protection authorities should operate independently of any external interference to ensure that they deliver their mandate objectively within the established legal and human rights standards. Under section 5.1 of the FOI Act, the independent Information Commissioner is appointed by the President with the advice and consent of the Liberian Senate and shall serve on a full-time basis.

The IIC is protected against political interference, and the president, despite appointment, may not unceremoniously remove the ICC from office. According to the FOI Act, the IIC may only be removed from office for gross misconduct, incapacity to perform, incompetence or in case of a criminal conviction against him. There would have to be thorough investigations and legislative oversight for the IIC to be removed from the office.

Under section 5.1, the work of the IIC and the technical secretariat is funded by the Government through the National budget. This potentially ensures the independence of the IIC and the availability of resources to ensure that it continues to operate effectively and enforce data protection laws and policies without any major hindrances.

The above provisions provide a firm foundation for an independent data regulator in Liberia.

***Policy Prescriptions***

a) Based on the PDPPA 2024, expedite institutional reforms to enable the IIC to discharge its additional mandate on privacy and data protection;
b) Allocate a sufficient budget to the IIC to enable it to effectively discharge its new functions, including recruitment and capacitation of new staff, development of strategies, tools and standard operating procedures, conduct of public awareness and undertaking of enforcement actions.

Implementing the above actions will enable Liberia to establish a data governance framework that is well-coordinated, transparent, and trusted, fully compliant with AU and ECOWAS standards, and supportive of inclusive social and economic transformation.

## 4.3 Sectoral Regulators

a) **Central Bank of Liberia (CBL):** Retains regulatory authority over financial data, credit information, and the interoperability of the Liberian Inclusive Instant Payments System (IIPS).

b) **Liberia Telecommunications Authority (LTA):** Regulates Internet Service Providers and Mobile Network Operators, and manages the International Gateway Monitoring System (IGMS) to secure the infrastructure through which data flows.

c) **Liberia Institute of Statistics and Geo-Information Services (LISGIS):** The LISGIS remains the custodian of national statistical and geospatial data. Within the data governance framework, LISGIS acts as the quality assurance body for non-personal data. It is responsible for setting standards for data anonymisation, ensuring that datasets released for public consumption (Open Data) cannot be reverse-engineered to re-identify individuals, thus protecting privacy while enabling research.

**d) The National Identification Registry (NIR):** Its mandate includes the management of foundational identity data such as the National Biometric Identification System (NBIS), issuing biometric ID cards to citizens and legal residents and streamline public services like birth registration, passports, and social benefits. Its ongoing efforts include linking identity cards to all government services and potentially cross-border travel within the ECOWAS region.

e) **The Ministry of Gender and Children Protection:** The MGCSP is responsible for the promotion of gender equality and social welfare. Its mandate extends to gender mainstreaming, social protection, child protection, countering Sexual and Gender-Based Violence and ensuring compliance with international treaties with a common goal or vision. Its scope of work entails protection of vulnerable populace, promotion of gender equality, protection of the rights and welfare of children. It therefore collects and manages significant data sets.

## 4.4 Intra-Government Committees on Data Governance

As a national asset, data cuts across multiple government ministries and agencies. Whereas different MACs deal with data for different purposes, it is essential that all data be protected, managed responsibly, and harnessed for national development. This makes it imperative for various MACs to be involved in data governance, and for their efforts in this regard to be harmonised. There are several initiatives underway to harmonise data governance in the country.

**The National Steering Committee**, which is chaired by the President, coordinates the National Development Plan (2025-2029), which underscores data as a national strategic asset and resource.

**The Independent Information Commission** oversees the implementation of the Freedom of Information Act, 2010 and it has been proposed that its mandate should be extended to cover the protection and processing of personal data.

**The Inter-Ministerial Committee**, which comprises MoPT, the Ministry of Justice, and the Financial Intelligence Agency (FIA), leads efforts to develop a National Data Governance Policy. This committee is working towards ensuring that Liberia's data governance framework aligns with the African Union Data Policy Framework and other regional, continental, and international standards.

The Liberia Institute of Statistics and Geo-Information Services (LISGIS) which was established by the National Statistics and Geo-Information Act of 2004 and is mandated to coordinate the collection and dissemination of all official national socio-economic and spatial data.

These committees require sufficient funding to enable them to undertake their regular activities, such as meetings, establishing the shared relevant infrastructure, capacity building and training and technical audits and reporting that will enhance effective data governance. Moreover, their roles, particularly that of the IIC and the Inter-Ministerial Committee, will be crucial in implementation of the Data Governance Policy, as regulators and policy overseers respectively.

## 4.5 Digitisation, Data Sharing, and Data Value Creation Mandates

Data is a critical economic asset that can transform public services delivery and promote national socio-economic development in Liberia. Advances in technology are shaping ways in which public institutions operate and how citizens interact with public institutions. For instance, Digital Public Infrastructure (DPI) have become central pillars in the digital transformation journey of countries, with the establishment of the National Identification Registry (NIR), digital payment systems and data exchanges. In turn, this DPI has made it crucial to have interoperable data and digital systems across various government ministries and agencies.

Open Government Data (OGD) initiatives are also creating economic value by making non-sensitive datasets such as those in agriculture, education and finance accessible to innovators and entrepreneurs.

Intra-agency agreements have been established in various sectors, such as agriculture, energy, and transport, to foster and enhance seamless data sharing across government MACs. Some of the existing agreements are between the Civil Service Agency and National Identification Registry in 2024; Liberia National Police and the Ministry of Justice; LISGIS and Sector Ministries of Health, Agriculture, and Labour; and the MoPT and the ECOWAS. These agreements aim to enhance service delivery and improve tax compliance.

***Policy Prescriptions***

To maximise the benefits of digitisation, data sharing, and data value creation, the government shall:

a) Identify priority data-driven transformation initiatives to improve public service delivery and boost socio-economic transformation.
b) Develop and implement API gateways and integration middleware to enable secure and interoperable communication between different government registries and databases (e.g., civil registry, health, education, transport, taxation, and finance).
c) Pilot data exchanges among government MACs to facilitate public service delivery.
d) Develop and implement clear data-sharing regulations for Ministries, Agencies, and Commissions (MACs) to guide how data is shared and used across government. Such a clear framework is needed to ensure that data is used responsibly, shared when necessary, and always protected. Also, by putting these regulations in place, Liberia will strengthen coordination across public institutions, make services more efficient and evidence-based, protect individual rights, and build public trust in data as a national resource that benefits everyone.

   These regulations should set out when and why data can be shared, and provide safeguards for personal and sensitive information. They should embed key principles such as purpose limitation, data minimisation, security, accountability, and transparency, so that all data-sharing activities respect citizens' rights while supporting government operations.

   The Government should ensure that all inter-agency data-sharing arrangements are documented, with clear roles, responsibilities, and oversight measures. When there is potential for high-risk processing, agencies should carry out appropriate risk or impact assessments.

# 5.0 DATA INFRASTRUCTURE AND TECHNOLOGY

## 5.1 National Digital Infrastructure

Proper infrastructure is critical for data management and provides security, scalability and inclusion within technological advancements, data sovereignty and effective use of data for national development.

Digital Infrastructure is the backbone of data governance as well as reliable and affordable digital systems. It acts as a backbone by providing the foundational systems needed for economic and social development, connecting citizens, businesses, and the government digitally. Digital infrastructure includes mobile and broadband networks, digital payment systems, and e-governance platforms, all of which are crucial for expanding access to education, health, and financial services, fostering inclusive growth, and improving government efficiency and accountability.

The e-Liberia portal is a citizen navigation portal that provides access to government services such as paying taxes, passport applications and birth registrations. The Liberia Data Portal (LISGIS), managed by the Liberia Institute of Statistics and Geo-Information Services, is the official repository for socio-economic, demographic, and agricultural data. The Aid Management Platform (AMP) is a repository used by the Ministry of Finance and Development Planning to track Official Development Assistance (ODA).

Other repositories include the Online Mining Cadastre under the Ministry of Mines and Energy that handles data related to minerals and mining. The Liberia Land Authority (LLA) database is a repository for land titles and customary land shapefiles. The National Identification Registry handles biometric verification and the payroll for civil servants. The GFF Data Portal for the Ministry of Health handles all health-related data.

These developments show the need to establish a national data centre for a robust data management framework, with key components including digital identity, secure payment systems, and improved internet connectivity. A centralised database will provide a secure and inclusive digital environment that promotes transparency, accountability, and citizen empowerment through better data handling and use.

The database should be designed with interoperability measures to facilitate the seamless yet secure flow of data among MACs. This will require developing appropriate standards and security protocols that foster data sharing while respecting individuals' privacy.

***Policy Prescriptions on the National Digital Infrastructure***

**The Law and Policy:** Clearly establish and define rules for ownership and transfer or sharing of data through formal MoUs and classification policies. This should define specific duties for managers, custodians, and users of data.

**Institutional Governance:** Establish relevant digital governance and transformation structures to oversee implementation, enforce data protection standards, ensure compliance and serve as arbitrators for any disputes.

**Semantic Alignment:** Establish unified data models and shared vocabularies to ensure retention of data meaning across different systems. Taxonomies, Ontologies and metadata should be aligned to eliminate any ambiguities and make national datasets universally interpretable.

**Technical:** Clearly define the interoperability framework to establish common standards for data formats secure integration and communication protocols (APIs), as well as robust identity management to foster standardised seamless and secure connectivity across platforms.

## 5.2 Digital Identity and Authentication Systems

The National Identification Registry (NIR) is central to digital transformation in Liberia. It can be a benchmark for the inclusion of the populace in access to essential services. An effective NIR entails enhancement of biometric security to check on data breaches and fraud, universal coverage including of marginalised populations, seamless data integration that serves authenticity in service delivery and ensuring data sovereignty and privacy within robust data protection protocols.

***Policy Prescriptions***

a) Upgrade the NIR to ensure an efficient digital identity ecosystem that acts as a backbone for e-governance.
b) Develop secure gateways, especially the Application Programming Interfaces (APIs) that facilitate real-time verification of identities while maintaining data integrity by third parties such as commercial banks and mobile money service operators.
c) Update the legal frameworks on data governance to align with modern advancements in technology and with new and emerging regional and international data governance standards, such as those of the African Union and ECOWAS.
d) Define the scope of digital identity in light of interoperability requirements in intra-governmental undertakings and commitments by MACs to ensure independent oversight, accountability and transparency.

## 5.3 Connectivity

Liberia's connectivity levels vary between the urban and rural areas, with the capital Monrovia and other urban centres having a high penetration of high-speed broadband and mobile internet, while rural areas remain underserved, limiting digital inclusion. The inclusion gap is further worsened by the high internet costs relative to individual incomes. Furthermore, the dependence on a single backbone (the ACE submarine cable) makes Liberia vulnerable to outages and bandwidth bottlenecks.

There is a need to bridge the urban-rural connectivity divide to ensure equitable access, build skills and capacities to match technological advancements and secure sustainable funding to support inclusive data governance initiatives.

***Policy Prescriptions***

**The government shall:**

a) Expand Rural Broadband including by partnering with telecoms and ISPs to deploy new rural towers and expand rural broadband coverage.
b) Develop an Affordable Internet Policy by 2029 and introduce subsidies or tax incentives on technology tools and the internet to reduce average household tech costs by 30%, with a view to attaining universal, affordable access by 2030.
c) Leverage the Universal Access Fund to undertake Public–Private Partnerships with telecom operators such as Orange Liberia, Lonestar Cell MTN, and CSquared in data-driven innovations, infrastructure sharing and continuous monitoring to expand connectivity and ensure universal access across the country.

# 6.0 DATA STORAGE, SOVEREIGNTY, AND CROSS-BORDER FLOWS

## 6.1 Data Storage

Secure, resilient, and sovereign data storage is a fundamental pillar of Liberia's ARREST (Agriculture, Roads, Rule of Law, Education, Sanitation, and Tourism) Agenda and its national digital sovereignty. As Liberia accelerates its digital transformation and transitions from fragmented paper-based systems to integrated digital platforms—there is an urgent need for a unified, standards-based data infrastructure that guarantees the availability, integrity, and confidentiality of the country's data assets.

Central to sovereign data storage is the establishment of a National Data Center, complemented by secure, localised cloud solutions like the Tier III+ facility currently under development in Buchanan city. This infrastructure will serve as the backbone for Liberia's e-government services, ensuring sovereign hosting of data by key institutions such as the NIR and the Liberia Revenue Authority.

The Government therefore seeks to reduce its over-dependence on international providers, enhance its disaster recovery and business continuity capabilities, and provide a scalable foundation for the National Spatial Data Infrastructure (NSDI). It shall therefore:

a) Establish or designate a national data centre to host critical government datasets and digital public services, with appropriate disaster recovery and business continuity mechanisms.
b) Ensure alignment of the national standards for data storage, backup, retention, and archival in the PDPPA 2024, and ensure their applicability across Ministries, Agencies, and Commissions (MACs).
c) Promote and foster the use of secure hybrid and cloud-based solutions where appropriate, subject to national data protection, security, and sovereignty requirements.
d) Ensure that all public sector data storage systems comply with recognised cybersecurity and information security standards, including access controls, encryption, and audit mechanisms.
e) Allocate sustainable funding within the national budget and technical capacity to maintain, upgrade, and secure national data storage infrastructure.

## 6.2 Cross-Border Data Flows

Liberia's cross border data flows stand to be shaped by the Cybercrime Act of 2025 and the African Union Data Policy Framework. The seamless flow of data could drive regional digital trade. With the launch of the SIGMAT corridor (Customs Data Exchange) between Liberia, Côte d'Ivoire, and Guinea, mobile money interoperability, public health research through LISGIS could be enhanced. Additionally, the delivery of cloud-based government services under the ARREST Agenda for Inclusive Development (2025–2029) is further enhanced.

At the same time, unregulated or opaque data transfers imply lack of clear oversight on international data transfers which exposes individuals and presents data security risks that put Liberia's data sovereignty at stake with potential data privacy breaches, loss of judicial control over data justice and national security breaches.

Liberia shall therefore adopt a balanced approach that enables lawful and beneficial cross-border data flows while safeguarding national interests, individual rights, and public trust.

***Policy Prescriptions***

a) Fast track the adoption of the legal and regulatory frameworks governing cross-border data transfers, consistent with national law, data protection principles, and international best practices. The PDPPA 2024 shall be expedited to ensure that issues of cross border data flows are addressed.
b) Personal data may only be transferred outside Liberia if the destination country provides an adequate level of protection to the data or where explicit consent is obtained. All transfers must abide by national laws such as the PDPPA 2024, regional frameworks such as the ECOWAS Supplementary Act, and relevant continental agreements. This measure will safeguard personal information from being transferred to jurisdictions with insufficient data protection standards.
c) Subject all cross-border data transfers involving public sector data, sensitive personal data, or strategic national datasets to safeguards, including encryption, adequacy assessments, contractual protections, or other approved transfer mechanisms within the established legal and regulatory mechanisms.
d) Establish relevant mechanisms and, require strict compliance with transparency and accountability in data-sharing arrangements with foreign governments, international organisations, development partners, and private entities.
e) Promote data-sharing arrangements that support development objectives, research, innovation, and regional integration, while respecting privacy, security, and national sovereignty.

## 6.3 Data Sovereignty

Data sovereignty entails the State's authority and responsibility to regulate the collection, storage, processing, and use of data generated within its jurisdiction, in accordance with national laws like the Personal Data Protection and Privacy Act and the Cybercrime Act and public interest objectives. As Liberia expands its digital ecosystem, safeguarding data sovereignty is essential to protect citizens' rights, national security, and economic interests.

Data sovereignty does not preclude international cooperation or data exchange but rather ensures that such engagements occur within a clear legal, institutional, and accountability framework.

***Policy Prescription***

The Government shall:

a) Define categories of data deemed strategic, sensitive, or of national importance, and establish specific rules for their storage, processing, and transfer.
b) Ensure that public sector data remains subject to Liberian law, regardless of where it is stored or processed.
c) Strengthen oversight mechanisms to prevent unauthorised access, misuse, or commercial exploitation of national data assets.
d) Promote local capacity development in data infrastructure, analytics, and management to reduce over-reliance on external service providers.

## 6.4 Regional Cooperation and Harmonisation

Liberia's data governance framework shall be viewed as a bridge to the ECOWAS Single Digital Market and the African Continental Free Trade Area (AfCFTA). It is designed with interoperability in consideration to align with regional and continental initiatives including the ECOWAS Supplementary Act on Personal Data Protection and the African Union Data Policy Framework. These initiatives foster and enhance cooperation, interoperability, and integration within the African digital economy. Alignment with regional standards enhances trust, regulatory convergence with the regional instruments, collective cyber security through Digital Forensic Lab's integration with the ECOWAS regional CERT (Computer Emergency Response Team) network supports cross-border services, and strengthens Liberia's participation in regional trade, research and development initiatives in collaboration with the West African Research and Education Network (WACREN).

***Policy Prescriptions***

The Government of Liberia undertakes to:

a) Align national data infrastructure and governance frameworks with applicable regional and continental instruments, including those of ECOWAS and the African Union.
b) Promote active stakeholder and government participation in regional data governance initiatives aimed at standardisation, interoperability, cybersecurity cooperation, and capacity building.
c) Promote cross-border collaboration on data infrastructure, research, innovation, and digital public goods that support shared development objectives.
d) Cooperate with and engage regional partners to address common challenges related to connectivity, cybersecurity threats, data protection enforcement, and digital inclusion.

# 7.0 DATA MANAGEMENT FRAMEWORK AND STANDARDS

## 7.1 Data Classification

To manage data effectively, it is crucial to categorise it based on sensitivity and strategic value. Liberia shall adopt a tiered national data classification matrix which delineates where data can be stored and the security protocols required. Recognising the global nature of the digital economy, the IIC shall publish a framework for data classification and maintain a registry of jurisdictions that provide an "adequate level of protection" as set out in the PDPPA 2024. For transfers to non-listed jurisdictions or intra-corporate transfers (e.g., multinational banks), Standard Contractual Clauses (SCCs) must be adopted to ensure the data processor accepts liability for breaches.

| **Classification Level** | **Definition** | **Examples** | **Residency Requirement** | **Security Requirement** |
|---|---|---|---|---|
| Level 1: Public Data | Information explicitly created for public release or non-sensitive administrative data. Disclosure causes no harm. | Budget reports, weather data, census aggregates, government press releases, tourism data. | Public Cloud: Can be stored in secure public clouds by the private sector to maximise accessibility, redundancy and cost-efficiency. | Standard encryption (HTTPS/TLS) in transit. Access controls for publishing. |
| Level 2: Confidential Data | Sensitive information specific to individuals (PII) or internal government operations. Unauthorized disclosure could cause harm, privacy violation, or financial loss. | Tax records (LRA), educational records (EMIS), health records (HMIS), basic NIR demographic data, civil service payroll. | Sovereign Cloud / Hybrid: Must be stored within Liberia OR in a "Data Embassy" (a trusted jurisdiction with a binding adequacy agreement). | Strong encryption at rest and in transit (AES-256). Multi-Factor Authentication (MFA) for access. Strict audit logging. |
| Level 3: Sovereign/ Restricted Data | Critical data where compromise impacts national security, economic | Biometric databases (NIR), Classified National Security info, Critical Infrastructure | Strict Localization: Must be stored physically within Liberia on Government Data | Air-gapped backups. Hardware Security Modules (HSM) for key management. |

| | | | | |
|---|---|---|---|---|
| | stability, or constitutional rights. | schematics (Mt. Coffee, GovNet), Intelligence data. | Centers. No cross-border mirroring without Cabinet approval. | Vetted personnel access only. |

## 7. 2 Artificial Intelligence (AI) and Emerging Technologies

As technology advances, cloud computing and emerging technologies (AI, blockchain, cloud computing, 5G, and IoTs) present the need for adoption of secure systems to ensure that the cloud-based infrastructure is robust. These efforts will foster a resilient and efficient digital economy since they offer timely data analytics and automation of initiatives.

Liberia suffers from insufficient financial resources, poor data quality, and inconsistent compliance with existing regulations, all of which are compounded by weak institutional frameworks to address the impact of emerging technologies.

There is a need to integrate cloud computing and emerging technologies such as Machine Learning (ML) into the country's digital roadmap across government MACs. Blockchain technology should be fully explored to ensure secure record keeping, such as land titles and management of identity. The IoT should be deployed within robust standards that allow for timely monitoring of the critical infrastructure to ensure efficient delivery of government services to the citizens.

With the increasing regional integration and data sovereignty, regulations and guidelines that address and integrate emerging technologies into cross-border data flows must enhance alignment with the African Continental Free Trade Area (AfCFTA), ECOWAS and other regional treaties and agreements. Clear safeguards must be in place to guard against data breaches and foreign surveillance and ensure that AI-driven automated decision-making is used across various industries, such as finance, healthcare and taxation, among others, in an accountable and transparent manner free from algorithmic bias and to ensure it reflects fairness and equity.

***Policy Prescription***

Government agencies will ensure that the values of justice, accountability, openness, and respect for human rights are upheld when using AI and other emerging technologies. They will conduct impact assessments to identify risks to privacy, ethical standards, and non-discrimination. All AI systems shall be auditable and subject to oversight by the Independent Information Commission.

## 7.3 Technical Capacity and Skills

Data analysis and business Intelligence are essential for the digital transformation of the country. Liberia suffers from the lack of skilled personnel, skills gaps, low digital literacy and a shortage of trained ICT professionals, cybersecurity experts, and data analysts, and the brain drain of ICT professionals. Sectors such as innovation and entrepreneurship, education, healthcare, insurance and agriculture, once effectively integrated, will enable tracking of economic growth and development.

Also, once the policy makers are capacitated with knowledge and expertise, they will be able to comprehend and use data-driven insights to make informed decisions.

***Policy Prescription***

The government shall:

a) Design specific training programmes to empower policy makers and staff of government MACs, especially the LISGIS and the Ministry of Finance, with technical skills for data-driven governance.
b) Develop a National ICT Training Program in collaboration with academia and other stakeholders to train 5,000 youth annually in coding, cybersecurity, and data analytics, with certification aligned to AU/ECOWAS and international standards in the next five years.
c) Launch a "Digital Talent Retention Fund" offering scholarships and career pathways to reduce the ICT brain drain.
d) Collaborate with academia to develop specialised certification programmes in data privacy, cybersecurity, cyber forensics, data analytics and cloud administration.
e) Facilitate international cooperations with other countries to enable professional exchanges and mentorship for key officials.

# 8.0 NATIONAL DATA MANAGEMENT FRAMEWORK

The Liberia National Data Management Framework (LNDMF) provides a layered and structured model which is designed to align with international standards while aligning with Liberia's unique institutional landscape and digital realities. It serves as a springboard for data-driven transformation that fosters data maturity within coordination mechanisms for the government MACs. The key strategic pillars to govern data management are:

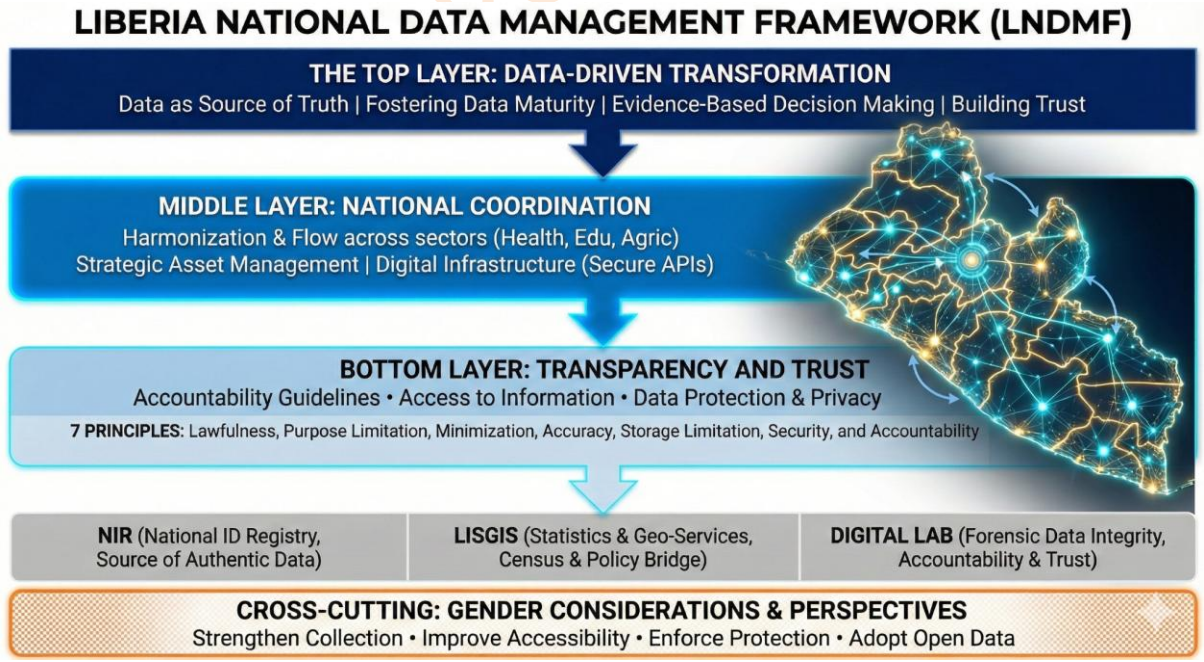
**National Coordination,** which is a framework that harmonises data practices across various sectors such as agriculture, health, and education to harness the transformative power of information for national growth.

**Strategic Asset Management** which provides a reference point for data optimisation in public, semi-public, and private sector entities. Data is a strategic asset which will contribute to socio-economic development and transform public service delivery.

**Digital Transformation** which is led by the LNDMF to ensure interoperability, security and accessibility to quality data that informs evidence-based decision making.

**Transparency** which is a basis for trust building through the use of clearly set guidelines for accountable handling of data within Liberia's digital transformation.

This framework will align and bridge the gaps that arise between government MACs, especially the National Identification Registry, the Liberia Institute of Statistics and Geo-Information Services, and the Digital Forensic Lab.




This chart is a layered tier structure. It is inspired by regional and international data protection and data security standards.

## 8.1 The Top Layer: Data-Driven Transformation

**Data as a Single Source of Truth:** Government shall integrate the NIR, LISGIS, and the Digital Forensic Lab for a unified high-quality data pool that prevents data disparities and ensures that every policy is based on accurate information.

**Fostering Data Maturity:** Digital data transformation shall cut across all the government MACs. Efforts shall be undertaken to completely move from paper-based record management to digitalisation to ensure easier storage and access, and to prevent loss of data. Data interoperability shall be core to ensure intra-governmental access and cooperation in data sharing and governance.

**Evidence-Based Decision Making:** The LNDMF shall use data that is evidence-based to foster strategic management of data as opposed to relying on data based is not empirical.

**Building Trust:** The LNDMF will lead all processes aimed at building trust by embedding transparency and Security through the Digital Forensic Lab into the data management processes. This will enhance trust amongst the public since participation will be enhanced and public services will be delivered much faster.

**Data Risk Management**: Governmental ministries and agencies shall use a risk-based strategy to protect sensitive and private information. Agencies must regularly evaluate data processing operations in order to spot possible hazards and put preventative measures in place. There must be procedures in place for promptly reporting and handling data breaches, including informing the Independent Information Commission and impacted parties as needed.

## 8.2 Middle Layer: National Coordination

Since data governance has been fragmented in different government MACs, coordination will harmonise data management processes and harness the transformative power of data. It will link different sectors such as health, education and agriculture. It will weed out duplication while ensuring a smooth flow of information across MACs, such as across the NIR and the LISGIS.

**Strategic Asset Management:** The aim is to shift the mindset of the public and private sector players that data is beyond paperwork and a strategic national asset. The LNDMF will ensure that all data is cleaned and accurate before storage and is maximally utilised as a reference point to drive and enhance socio-economic development.

**Data Quality and Standards**: All MACs shall ensure that data is accurate, complete, timely, and reliable. Metadata describing the origin, purpose, and context of data shall be maintained for all datasets. The Ministry, working with line MACs, will develop national standards for data classification, coding, and interoperability, which shall be applied consistently to facilitate seamless data sharing, integration, and reuse.

**Digital Transformation:** Efforts will be undertaken to ensure that the relevant technical infrastructure, like the secure APIs, provides assurance of data quality through data interoperability, security, and accessibility. This too will foster evidence-based decision-making.

**Open Data and Reuse**: To facilitate research, innovation, and public participation, government agencies shall make non-sensitive data available in machine-readable and accessible formats. Open data initiatives by MACs shall always seek to strike a balance between transparency and the protection of privacy and security.

## 8.3 Bottom Layer: Transparency and Trust

**Transparency and trust** are recognised social contracts that potentially enhance digital transformation. They are a basis for public confidence that their personal information and data are safe and handled responsibly. The LNDMF is proactively committed to transparency and requires government MACs to embrace data governance principles and rights. The key strategic components are:

a) **Accountability Guidelines**: Establishment of accountability guidelines to ensure that all government MACs with data hold it within the data protection and security standards.
b) **Access to Information:** Citizens have a right to know and to access their information within the Freedom of Information Act. Citizens can request their information as and when they want it. They have a right to correct any inaccuracies in their information.
c) **Data Protection and Privacy:** Data protection principles and rights within established legal safeguards, such as the Cybercrime Act, 2025 and the Personal Data Protection and Privacy Act, 2024 (bill) will be ensured. Efforts to prevent unauthorised access are core, and stringent data privacy measures will be undertaken.
d) **Principles of Data Protection:** In order to promote responsible data handling, all entities that handle personal and sensitive data must abide by the following principles:
    - **Lawfulness and Fairness:** Data shall be collected and processed in a lawful, fair, and transparent manner.
    - **Purpose Limitation:** Data shall only be collected for specific, legitimate purposes and not used beyond these purposes without proper authorization.
    - **Data Minimisation:** Only data necessary for the intended purpose shall be collected and retained.
    - **Accuracy and Reliability:** Data shall be maintained accurately and kept up-to-date.
    - **Storage Limitation:** Data shall not be kept longer than required for its intended purpose.
    - **Security and Confidentiality:** Data shall be protected against unauthorized access, alteration, loss, or destruction.
    - **Accountability:** Data controllers and processors shall be responsible for compliance and must be able to demonstrate adherence to these principles.

## 8.4 The Base

**National Identification Registry**

The NIR is the key custodian of data within the LNDMF. It is the source of authentic data. The framework allows easy verification of data and information within the government MACs.

NIR Data and its integration via APIs allow for easy provision of social services and ensure that services go to the right people.

**Liberia Institute of Statistics and Geo-Information Services (LISGIS)**

The LISGIS is the custodian of national statistical and spatial data. It manages census data and economic indicators and provides the basis for evidence-based decision-making. It is a key bridge between raw data and policy.

**Digital Forensic Lab**

This lab is the guardian of data integrity and trust. The lab provides technical expertise in investigation and provision of admissible evidence in case of data breaches, digital fraud or unauthorised access. With its central role, citizens' trust is built since it holds all those responsible for data breaches, fraud and unauthorised access accountable.

# 9.0 PROMOTING GENDER EQUITY AND DATA JUSTICE

## 9.1 Gender Equity

Gender considerations are core to Data Governance since they show the beneficiaries and help to check exclusion on gender lines. Where data governance is not gender inclusive, such as in data collection and analysis, the underrepresentation of vulnerable groups, such as women and girls in data governance processes, it has the potential to perpetuate gaps in data needed to monitor gender equality, especially in areas like labour market indicators, women's access to assets, and gender-based violence.

To ensure accountability across government MACs, there is a need for a combination of strong and standardised institutional frameworks, clear goals, purposes and processes, and a culture of transparency and responsibility. The specific roles, responsibilities, and performance expectations for each government MACs and the officials should be clearly defined.

There is a need to undertake efforts through initiatives like the launch of gender disaggregated statistics to enhance data accessibility and affordability, particularly for women in the digital space.

**Key Components for Gender Mainstreaming**

a) **Strengthen Data Collection:** Invest in strengthening gender-disaggregated data collection and analysis across all sectors to better inform policies and programs.
b) **Improve Data Accessibility:** Make data more accessible and affordable, especially for women, through subsidies or other initiatives to bridge the digital divide.
c) **Enforce Data Protection:** Implement and enforce robust data protection laws to ensure data security and privacy, and to build trust in the digital economy.
d) **Adopt Open Data Policies:** Adopt open data policies that require data to be published in machine-readable formats and with a clear data license.

## 9.2 Data Justice

Data justice serves to ensure equitable distribution of risks and responsibilities that arise from data driven systems. Data justice goes beyond rights of data subjects to cover aspects of data governance including the structural and collective impacts of data on often underlooked marginalised populace.

Effective implementation of data justice requires procedural justice and equal participation to ensure inclusive participation in digital systems. Within Liberia’s data governance, data justice is foundational for fairness, inclusiveness, transparency, and accountable use of data. It is also a basis for the advancement of human dignity, equality, and sustainable development.

Liberia's historical inequalities, disparities between urban and rural Liberian populations, gender gaps, and the marginalisation of vulnerable groups including women, persons with disabilities, informal sector workers, and rural communities have often dictated data justice and human rights. It is imperative that data infrastructure and technologies are designed and governed fairly and equitably to avoid discrimination, exclusion or harm for inclusive data-driven development.

To ensure that communities have meaningful visibility in data generation and usage, and to challenge harmful or inaccurate data practices, and access remedies for data breaches, the Government shall:

a) Take measures to ensure that the national data infrastructure and digital technologies are designed and deployed in ways that promote equity, inclusion, and non-discrimination, and do not disproportionately exclude or disadvantage marginalised or vulnerable groups.
b) Be intentional and designate two specialised roles to oversee data management and inclusion and equity and every MAC. The Data Protection Officer shall be charged with ensuring data protection within the established legal and regulatory standards while the Inclusion and Equity Officer shall be responsible for ensuring that data collection methodologies include maginalised populace.
c) Promote fair data practices across the public sector, including measures to prevent bias, discrimination, and inaccuracies in data collection, processing, analysis, and automated or algorithmic decision-making systems.
d) Require impact-based assessments, to identify and mitigate potential harms arising from large-scale data systems, digital identity frameworks, and data-driven public services, particularly those affecting access to essential services.
e) Be intentional on strengthening transparency and accountability in the use of public sector data, including through the adoption of clear documentation of data sources, methodologies, and decision-making processes that rely on data or automated systems.
f) Ensure that individuals and communities have accessible mechanisms to access information about data held on them, correct inaccuracies, object to unlawful or harmful processing, and seek redress where data misuse leads to rights violations or material harm.
g) Promote community participation and stakeholder engagement in the design, governance, and evaluation of national data systems, including consultation with civil society, academia, the private sector, and affected communities.
h) Support capacity building and data literacy through the use of both human and financial resource initiatives to enable citizens, especially women, youth, rural populations, and persons with disabilities, to understand, use, and benefit from data and digital technologies.
i) Encourage the ethical use of data for development, research, and innovation using open data initiative and ensure that data practices contribute to social justice, public trust, and inclusive economic growth.

# 10.0 STAKEHOLDER ENGAGEMENT AND PARTNERSHIPS

## 10.1 Implementation and Sustainability

The effective implementation and long-term sustainability of this Policy shall be anchored in strong institutional coordination, adequate resourcing, and continuous capacity development. The Government will provide overall leadership and oversight, ensure coherence across laws, policies, and institutions, and establish clear accountability mechanisms, including monitoring, evaluation, and periodic review.

Implementation shall be guided by measurable indicators aligned to the five African Union Data Policy Framework pillars, with regular public reporting on progress and outcomes.

Sustainability shall be promoted through predictable financing, integration of data governance requirements into public sector planning, budgeting, procurement, and donor-funded programmes, and the institutionalisation of privacy, security, and accountability safeguards by design and by default. Continuous skills development, stakeholder engagement, and public awareness shall be prioritised to build national ownership and resilience. Partnerships with development partners, the private sector, civil society, and academia shall be coordinated to avoid duplication, leverage comparative advantages, and ensure that data governance reforms remain inclusive, rights-respecting, and responsive to technological and societal change.

## 10.2 Academia

Academia can play a central role in strengthening Liberia's data governance ecosystem through research, teaching, innovation, and independent analysis. Universities, research institutions, and other academic bodies contribute to the generation of evidence, development of local expertise, and advancement of ethical, rights-respecting, and development-oriented approaches to data governance.

The Government therefore recognises academia as a strategic partner in the formulation, implementation, and review of this Policy and shall promote structured engagement with academic institutions to advance evidence-based policymaking, innovation, and inclusive national development.

In furtherance of this subsection, the Government shall:

a) promote structured collaboration with universities, research institutions, and other academic bodies to support evidence-based policymaking, data governance research, and innovation in the public interest;
b) facilitate academic research, analysis, and independent evaluation relating to data governance, data protection, digital transformation, artificial intelligence, and emerging technologies, subject to applicable ethical standards and legal safeguards;

c) support the integration of data governance, data protection, cybersecurity, digital ethics, and human rights into academic curricula, professional training programmes, and interdisciplinary research initiatives;
d) enable access by academic institutions to public sector data for research and educational purposes, in accordance with applicable laws, including safeguards relating to privacy, security, confidentiality, and intellectual property;
e) encourage partnerships between academia, public institutions, the private sector, and civil society to strengthen national capacity in data science, statistics, digital innovation, and responsible data use;
f) promote inclusive and locally grounded research agendas that address national development priorities and the data needs of women, rural communities, persons with disabilities, and other marginalised or vulnerable groups; and,
g) support the dissemination and uptake of academic research findings to inform policy development, legislative reform, institutional practice, and public awareness on data governance matters.

## 10.3 Civil Society Organisations

Civil Society Organisations (CSOs) in Liberia were widely affected by the civil war but have since transitioned to become watchdogs over the digital landscape in the country. The environment for CSO has been favourable, positioning them in a series of activities that aim to foster good governance. Notably, they have played important roles in areas of the right to information, consumer protection, citizens' charters, whistleblower protection, e-governance, report cards, democratic decentralisation and public interest litigation.

CSOs such as the Center for Media Studies and Peacebuilding (CEMESP) took part in processes of redefining the draft Personal Data Protection Act, 2024 to ensure that it reflects and aligns with regional efforts on data protection and governance.

The environment for CSOs to operate favourably and allow for monitoring of data governance amongst the private sector and the government players will be maintained and improved. In recognition of the accountability and transparency efforts of CSOs, the government shall:

a) Collaborate with CSOs to develop programmes to promote awareness, digital literacy and data skills, towards enhancing accountable data governance in the country.
b) Create a National Data Governance Council of a permanent nature that provides for CSO representation alongside the government MACs including the NIR, LISGIS, and MoPT in data governance oversight;
c) Integrate the role of CSOs in the DPPA especially the role of monitoring data privacy breaches;
d) Mandate and prescribe the need for the LISGIS and the NIR to release non-sensitive, anonymized datasets accessible to CSOs through a National Open Data Portal attained through upgrade of the Freedom of Information infrastructure; and
e) Fast track the allocation of part of the national ICT budget to building the technical capacity of CSOs in data governance.

## 10.4 Private Sector

The private sector such as telecommunication service providers, banks, hotels and other investors come into data governance and the digital economy on three fronts.

Firstly, telecommunication companies are gatekeepers since they are first contacts with the citizens. Telecommunication companies such as Lonestar Cell MTN and Orange Liberia have overtime collected a lot of data through SIM card and mobile money registration. They are also de facto setters of data management standards within their companies and their internal policies since a data protection authority is not functional

Secondly, they have compliance requirements to ensure sufficient safeguards of customer information. For instance, the Telecommunications Act of 2007 requires the companies to protect consumer information while the Central Bank of Liberia Regulations require financial institutions and e-payment service providers to strictly observe integrity and confidentiality of customer data.

Thirdly, they are relevant infrastructure and partners in the cybersecurity drive. They provide fibre optics and also manage data centres through which government data is transmitted. They are required to report any data breaches that emerge.

**The Government will:**

a) Continue working towards harmonisation of laws, regulations and policies to set common benchmarks for operations and personal data management. The benchmarks will align with the various policy frameworks and ensure common standards across the different private sector players including multinational companies and local startups.

b) Embrace and promote co-regulation and sandbox initiatives to create a favourable environment that checks on rigid laws that potentially stifle innovation on FinTech and Tech startups whose progress largely depends on data which is mainly controlled and regulated by the government.

c) The MoPT will continue to leverage and galvanise efforts of involving and ensuring active and effective participation of local SMEs in the National Digital Strategy (2025–2029) processes.

d) The government will continue to invest in shared infrastructure including the Digital Public Infrastructure (DPI) to reduce the burden of the private sector in investing in their own secure systems.

## 10.5 Media

The media is a public watchdog that contributes to accountability and transparency in service delivery and the building of public trust. It has a central role in monitoring and reporting how the state and the private sector operate and handle citizens personal information and data.

The media also plays a critical role in public education and awareness raising on data governance issues like data protection, cyber attacks and crimes, and surveillance. They demystify laws and policies and present them in local languages.

The government is committed to promoting a favourable environment for media operations. The government shall therefore:

a) Through collaboration with the Press Union of Liberia (PUL), ensure compliance with ethical standards in how journalists collect and store information within the established national and regional data protection and data governance standards

b) Align all data governance laws and policies to ensure that they promote journalism within open data standards and public interest requirements without necessarily gaging the work of journalists.

c) Leverage efforts to internally support the media sector especially community radio stations with financial resources. In this respect the government will operationalise the 0.25% of the national budget support to Community Radio Stations by enacting the Community Radio Reform Bill, 2025.

d) The MoPT will continue to leverage its partnership with the Press Union of Liberia (PUL) to integrate data protection and governance issues into the national journalism training modules.

e) Promote the Freedom of Information Act and enhance its utility to ensure that journalists use it to disseminate information and foster access to, and reporting of information on data governance and emerging issues.

## 10.6 Development Partners

Development partners play a critical enabling role in Liberia's data governance ecosystem, particularly in the context of the challenges faced including limited domestic resources, evolving institutional capacity, and the country's ongoing digital transformation agenda.

Through financial assistance, technical expertise, and policy support, they complement government efforts to establish a coherent, rights-respecting, and development-oriented data governance framework aligned with the African Union Data Policy Framework. Their engagement is especially relevant in supporting legal and regulatory reform, strengthening institutions responsible for data protection, cybersecurity, statistics, and digital services, and financing foundational data infrastructure.

In furtherance to this agenda, the government shall:

a) ensure that development partner support is coordinated, transparent, and aligned with national data governance priorities, including the harmonisation and operationalisation of data-related laws, regulations, and policies in accordance with national development objectives and applicable regional and continental frameworks.
b) facilitate the provision of technical and financial assistance by development partners to institutions responsible for data protection, cybersecurity, official statistics, digital public services, and oversight and accountability functions.

c) prioritise, plan for, and support investment, including through co-financing arrangements with development partners in secure, resilient, and interoperable national data infrastructure necessary for effective data management, sharing, and service delivery.
d) require that all development partner-funded programmes, projects, and digital systems implemented within Liberia comply with applicable laws and embed privacy, security, accountability, and human rights safeguards by design and by default.
e) promote responsible data value creation by directing development partner-supported initiatives towards evidence-based policymaking, innovation, and inclusive economic development, while ensuring the protection of personal and sensitive data.
f) encourage and support development partner initiatives that are inclusive and gender-responsive and address structural digital divides affecting women, rural communities, persons with disabilities, and other marginalised or vulnerable groups; and
g) provide clear legal and regulatory guidance to support lawful, secure, and trusted cross-border data flows, consistent with Liberia's international, regional, and continental obligations and national development priorities.

# 11.0 ENFORCEMENT, MONITORING AND EVALUATION

Within the current and emerging data governance frameworks such as the Personal Data Protection and Privacy Act, 2024, a robust Monitoring and Evaluation (M&E) framework is an essential requirement for a successful and sustainable digital transformation.

A clearly defined Roadmap must be developed and implemented. The roadmap which details operationalisation of the National Data Governance Policy has been developed and will guide implementation across the line government MACs.

With a systematic and well-implemented M&E plan, accountability and transparency will be enhanced and eventually build public trust in the management of data. The operationalisation and supporting the Independent Information Commission whose mandate is proposed for extension to overseeing the processing of personal data will reduce and minimise data breaches and strengthen data governance mechanisms.

In alignment with the African Union Data Policy Framework, M&E is critical for measuring the success of national data governance and digital strategies. A good M&E framework will foster the promotion and enforcement of the Data Protection and Privacy Act to assure citizens of the data rights. It will also guide activities relating to conduct of impact assessments by the state and civil society actors to evaluate data governance policies and how they are contributing to socio-economic development and digital transformation. This will essentially contribute to the newly introduced biometric systems or digital Ids.

The Ministry of Posts and Telecommunications in collaboration with the Independent Information Commission will develop a robust and exemplary Monitoring and Evaluation that aligns with the regional data governance policy frameworks especially the African Union Data Policy Framework to ensure that the transition of Liberia into the digital economy is progressive and yielding anticipated benefits of socio-economic development and digital transformation.

The framework will strive for specific, measurable results, achievability and relevance of time bound outcomes. Results reduced in reports will be provided to the legislature and CSOs to showcase policy performance and effectiveness so as to promote ownership of the policies and related processes. Trust in the digital systems will be built and won from the public and ultimately contribute to adaptation of emerging technological trends in alignment with national data governance strategies.

## 11.1 Independent Oversight and Enforcement

The Independent Information Commission shall provide oversight for the implementation of data governance, privacy, and protection obligations. The Commission shall have the authority to:

- Conduct audits and inspections of government and private sector entities that process data.

- Recommend corrective actions and impose administrative measures for non-compliance.
- Facilitate resolution of complaints raised by citizens or other stakeholders.
- Report regularly to the Parliament of the Republic of Liberia on the state of data governance in Liberia.

# Annex I: RELATED LEGISLATION AND DOCUMENTS

In the table below is a list of all legislation, policies, strategies and frameworks referred to in this policy.

| | |
|---|---|
| **Legislation On Data Governance in Liberia** | • The Constitution of Liberia of 1986<br>• The Telecommunications Act of 2007<br>• The Freedom of Information (FOI) Act, 2010<br>• The Electronic Transactions Law, 2002<br>• The Central Bank of Liberia (CBL) Payment System Act of 2014<br>• The Central Bank of Liberia e-Payment Regulations<br>• National Statistics and Geo-Information Act of 2004 |
| **Bills** | • Personal Data Protection and Privacy Act of 2024<br>• Cybercrime Act, 2025<br>• Community Radio Reform Bill, 2025. |
| **Policies and Strategies** | • The National ICT Policy (2019–2024)<br>• The National Digital Strategy (2025–2029)<br>• National Cybersecurity Strategy (2024–2029)<br>• National Development Plan (2025-2029) |
| **Regional and International Instruments** | • African Union Data Policy Framework<br>• African Continental Free Trade Agreement (AfCFTA)<br>• Continental Artificial Intelligence Strategy, 2024<br>• ECOWAS Supplementary Act, 2010 on Personal Data Protection within ECOWAS<br>• African Union Convention on Cyber Security and Personal Data Protection. |

# Document Control

| VERSION | DATE | AMENDMENT | AUTHOR |
|---|---|---|---|
| Final | March 2026 | | |

This is a living document. As and when changes emerge emerging data governance and the policy frameworks, this document will be reviewed and updated.

Upon approval, the National Data Governance Policy will be published.