**COUNCIL Of MINISTERS**

Resolution n.º [Insert Number]

In view and the need to provide an essential framework for ensuring that Mozambique fully harnesses the opportunities of the digital era, adapting to the guiding instruments of national development, continental commitments, and global best practices, the Government approves the **National Data Governance Policy and its Implementation Strategy**, in the use of the powers attributed to it by Article 203(1)(*f*) of the Constitution of the Republic, the Council of Ministers determines:

**Article 1** The National Data Governance Policy and the Strategy for its Implementation, attached hereto and forming an integral part of this Resolution, are hereby approved.

**Article 2** This Resolution shall enter into force on the date of its publication.

Approved by the Council of Ministers on [insert approval date]. Publish.

The Prime Minister, [insert current name].

## *DATA GOVERNANCE POLICY AND STRATEGY*

### 1. Introduction

**WHEREAS** the Republic of Mozambique, as a sovereign democratic state founded upon the rule of law, recognises that in the twenty-first century, data has emerged as a fundamental resource essential to good governance, sustainable development, and the advancement of human dignity.

**CONSIDERING** that the Government of Mozambique also considers that structured and coordinated governance of data is the foundation for building trust, improving public service delivery, fostering innovation, and safeguarding privacy and security in line with the Constitution and the laws of the Republic and is determined to ensure that Mozambique keeps pace with the rapid transformation of the digital economy, transforming data into an engine of development, equity, and transparency.

**ACKNOWLEDGING** that the effective governance of data as a strategic national asset is indispensable to realising the constitutional mandate to promote the general welfare, ensure domestic tranquillity, secure justice, and guarantee the fundamental rights enshrined in the Constitution of the Republic of Mozambique.

**RECOGNISING** that our nation stands at a transformative juncture where digital technologies and data-driven innovation present unprecedented opportunities to accelerate inclusive economic growth, strengthen democratic institutions, and enhance the quality of

life for all Mozambicans, while simultaneously presenting risks that demand careful constitutional safeguards.

**AFFIRMING** the unwavering commitment to the constitutional principles of human dignity, equality, transparency, accountability, and national sovereignty, which must guide all aspects of how the State collects, manages, processes, and protects data relating to our citizens and national interests.

**CONSCIOUS** that fragmented information systems, inconsistent data standards, inadequate governance frameworks, and insufficient capacity currently impede our nation's ability to harness data effectively for evidence-based policymaking, efficient service delivery, and equitable development;

**GUIDED** by the 2025–2044 National Development Strategy, approved by Resolution n.º16/2025, of May 12, and the Digital Mozambique Agenda, which establish data governance and digital transformation as pillars of sustainable development and national competitiveness.

**COMMITTED** to harmonising our national data governance framework with continental instruments, including the African Union Data Policy Framework, and with regional and international standards, including the principles embodied in the European Union General Data Protection Regulation, while asserting our sovereign right to determine how data within our jurisdiction is governed.

**DETERMINED** to ensure that all data governance activities respect and advance fundamental human rights, particularly the rights to privacy, dignity, security, and equitable access to information and digital services, as guaranteed by the Mozambican Republic Constitution and Law No. 3/2017, of January 9 – the Law of Electronic Transactions and aware that the Government is advancing a new generation of digital legislation, including draft laws on data protection, cybersecurity, cybercrime, and regulations on cloud computing, data centres, e-government and digital rights. These initiatives, together with strategies on digital transformation, open data, and artificial intelligence, highlight the urgency of adopting a coherent National Data Governance Policy and Strategy as the backbone for ensuring consistency, accountability, and trust across Mozambique's evolving digital ecosystem.

**RESOLVED** to establish data governance as a constitutional imperative that serves the public interest, promotes transparency and accountability in government, fosters innovation and economic opportunity, and ensures that the benefits of digital transformation reach every Mozambican, regardless of geographic location, economic status, or social background.

**HEREBY ESTABLISH** this National Data Governance Policy as the authoritative constitutional framework governing all aspects of data management within the Republic of Mozambique.

In 2013, the Southern African Development Community (SADC) developed a Model Law for data protection within the organization, which serves as a guide for the present data governance policy and strategy at national level. The model provides for the establishment

of national data protection authorities and also sets out general rules for processing personal data and duties for data controllers and processors, as well as rights for data subjects.

In recent years, Mozambique has adopted structuring instruments such as Mozambique's Law on Electronic Transactions - Law No. 3/2017, of 9 January, which establishes the legal framework for electronic communications, e-commerce, and the recognition of electronic documents and signatures. It provides legal certainty for digital interactions by granting electronic contracts and digital signatures the same validity as their paper-based counterparts.

While the referred law does not constitute a dedicated data protection statute, it introduces important safeguards for data security and privacy in the digital environment. Among its provisions are:

- **Obligations for service providers** to ensure the confidentiality, integrity, and availability of electronic communications and data processed through their platforms;
- **Recognition of electronic signatures and authentication mechanisms**, which reinforces the security of transactions and protects against identity misuse;
- **Requirements for secure storage and transmission of electronic information**, limiting unauthorized access and manipulation;
- **Support for e-government and digital services**, creating a foundation for trust between citizens, businesses, and the State.

Its relevance to data protection lies in the fact that it establishes technical and legal standards for safeguarding personal and transactional data in electronic environments. These provisions complement the broader framework still under development for personal data protection in Mozambique, while also aligning with regional and international best practices on secure digital transactions

Also, with the Resolution No. 39/2024, which approves the National Policy on Science, Technology and Innovation and establishes an implementation strategy Mozambique set clear targets for the development of ICT. The policy embraces a modern vision aligned with current technological progress, leveraging the opportunities of the Fourth Industrial Revolution to drive economic transformation and achieve the Sustainable Development Goals. The same is structured around six pillars:

- Strengthening the National System of Science, Technology and Innovation;
- Enhancing the capacity to adopt cutting-edge and emerging technologies;
- Promoting science, technology and innovation for the digital transformation of society;
- Strengthening the innovation ecosystem;
- Building and consolidating human capital; and
- Promoting international partnerships in science, technology and innovation.

Additionally, Mozambique approved the National Cybersecurity Policy and its Implementation Strategy, approved by Resolution no. 69/2021, of December 31 which strengthen the protection of critical information infrastructures and the fight against cybercrime.

At the regional and continental level, Mozambique is a signatory to the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention), which establishes common principles for the protection of personal data, the regulation of the digital economy, and cooperation in cyberspace. Internationally, milestones such as the United Nations Guidelines on Privacy in the Digital Age and the European Union General Data Protection Regulation (GDPR) constitute references of best practice that directly influence the design of national policies.

Despite these advances, structural challenges persist which justify the adoption of a National Data Governance Policy and Strategy:

- The dispersion of data across fragmented and often non-interoperable systems between ministries, agencies, and local authorities;
- Low levels of digital literacy in segments of the public administration and society, which undermine the full use of the potential of data;
- The absence of a consolidated normative framework for the protection of personal data, although efforts are underway to draft legislation and align with the Malabo Convention;
- The need to ensure that technological innovation — including artificial intelligence, cloud services, and big data applications — develops within ethical, transparent, and constitutionally compliant parameters.

The present National Data Governance Policy and Strategy thus emerges as a response to these challenges, establishing the principles, institutional mechanisms, and action priorities that will enable the country to consolidate digital sovereignty, ensuring that data produced within national territory is managed in line with the strategic interests of the State and the protection of citizens, and to also consolidate international and regional cooperation, ensuring that Mozambique positions itself as an active partner in SADC, African Union, and multilateral initiatives on data governance and data flows.

This instrument is not merely declarative: it constitutes a practical agenda, accompanied by an Implementation Strategy that defines institutional responsibilities, performance indicators, and phases of execution. This Strategy assumes a transversal character, binding all sectors of the State and setting clear guidelines for the private sector and civil society organizations that handle data of public relevance.

## Table of Content

# PART I: CONSTITUTIONAL FOUNDATIONS

### Recital 1: Constitutional Mandate and Legal Authority

WHEREAS Article 35 of the Constitution of the Republic of Mozambique guarantees every citizen the right to information and establishes the State's obligation to ensure access to information held by public entities, and Article 71 protects the right to privacy and personal data; and WHEREAS the Government possesses inherent constitutional authority to regulate matters affecting national development, public welfare, and the fundamental rights of citizens.

### Recital 2: Data as Constitutional Public Good

RECOGNISING that data generated by or relating to the activities of the State and its citizens constitutes a public good that must be stewarded with the same constitutional diligence applied to other national resources, and that effective data governance is essential to fulfilling the State's constitutional obligations to promote the general welfare and ensure equal protection under law.

### Recital 3: Doctrinal Foundation of Data Sovereignty

AFFIRMING that the concept of data sovereignty derives from the fundamental principle of national sovereignty enshrined in Article 11 of our Constitution, and that the Republic of Mozambique possesses inherent authority to govern data generated within its territorial jurisdiction and relating to its citizens, regardless of where such data may be processed or stored.

# PART II: EMPIRICAL FOUNDATIONS AND RATIONAL BASIS

### Recital 4: Evidence-Based Policy Imperative

FINDING that contemporary governance requires reliable, timely, and comprehensive data to support evidence-based policymaking, effective resource allocation, and accurate monitoring of progress toward national development goals, and that deficiencies in data governance directly impair the State's capacity to serve its citizens effectively.

### Recital 5: Digital Transformation Necessity

DETERMINING that Mozambique's transition to a knowledge-based economy and its integration into global digital markets require sophisticated data governance frameworks that ensure both the benefits and risks of digital transformation are managed in accordance with national interests and constitutional principles and RECOGNIZING the creation of the **Ministry of Communications and Digital Transformation** through Presidential Decree No. 01/2025, of January 25, as a pivotal step in institutionalizing this agenda, as it serves as the central authority for coordinating digital policies, fostering interoperability of government

platforms, promoting innovation through modern regulatory approaches, and safeguarding privacy and data protection, thereby linking the country's digital transformation directly to principles of data sovereignty, security, and citizen trust.

### Recital 6: Current Governance Deficiencies

DOCUMENTING systematic deficiencies in current data management practices, including: fragmented and incompatible information systems across government institutions; inconsistent data quality standards that undermine policy effective ness; inadequate protection of personal data and privacy rights; limited interoperability hampering cross-sector collaboration; and insufficient capacity for data analysis and decision-making;

## PART III: STRATEGIC OBJECTIVES AND POLICY RATIONALE

### Recital 7: Comprehensive Governance Framework

ESTABLISHING that effective data governance requires a comprehensive framework that addresses the entire data lifecycle, from collection and processing to storage, sharing, and disposal, with clear roles, responsibilities, and accountability mechanisms at every stage;

### Recital 8: Innovation and Economic Development

RECOGNISING that effective governance of national data assets is critical to stimulating innovation, fostering the growth of digital entrepreneurship, and supporting both SMEs and large enterprises across Mozambique;

FURTHER ACKNOWLEDGING the pivotal role of the private sector in unlocking economic value through the creation of new services, data-driven business models, advanced analytics, and public-private partnerships that can attract foreign investment, generate skilled employment, and enable Mozambican firms to compete regionally and globally;

EMPHASIZING that robust data governance ensures trustworthiness, transparency, and legal certainty, thereby enhancing investor confidence and establishing Mozambique as a preferred destination for responsible data-enabled investment and cross-border commercial opportunity, while conversely, inadequate or fragmented data practices risk impeding economic growth and limiting the nation's digital potential.

### Recital 9: Equity and Inclusion Imperative

DETERMINING that data governance must actively promote equity and inclusion by ensuring that the benefits of digital transformation reach all segments of society, including rural communities, marginalised populations, and vulnerable groups, and that data collection and analysis systematically address disparities and support targeted interventions;

# PART IV: INTERNATIONAL INTEGRATION AND COMPARATIVE STANDARDS

**Recital 10: Continental Integration Framework**
ACKNOWLEDGING our commitment to African Union integration objectives and our obligation to align national data governance practices with the AU Data Policy Framework while maintaining our sovereign authority to establish standards that reflect our national values and developmental priorities;

**Recital 11: International Best Practice Integration**
NOTING that leading data protection frameworks, including the European Union General Data Protection Regulation, the Organisation for Economic Co-operation and Development Privacy Guidelines, and International Organization for Standardization standards, provide valuable models for protecting individual rights while enabling beneficial data use;

**Recital 12: Cross-Border Data Flow Governance**
RECOGNISING that modern digital commerce and international cooperation require carefully regulated cross-border data transfers that protect national sovereignty and individual rights while facilitating legitimate economic and governmental activities;

# PART V: IMPLEMENTATION IMPERATIVES

**Recital 13: Institutional Capacity Requirements**
DETERMINING that effective implementation of this Policy requires establishing robust institutional frameworks, including a National Data Governance Council with constitutional authority, Chief Data Officers in all government institutions, and comprehensive training programs to develop national data governance expertise;

**Recital 14: Technological Infrastructure Necessities**
RECOGNISING that achieving the objectives of this Policy requires substantial investments in digital infrastructure, interoperable information systems, cybersecurity capabilities, and technical capacity that support efficient, secure, and accessible data management;

**Recital 15: Continuous Adaptation Requirement**
ACKNOWLEDGING that data governance frameworks must evolve continuously to address emerging technologies, changing threat landscapes, evolving legal requirements, and shifting societal expectations, requiring built-in mechanisms for regular review and updating;

# PART VI: CONSTITUTIONAL COMMITMENT AND ENACTMENT

**Recital 16: Public Interest Supremacy**
AFFIRMING that all provisions of this Policy shall be interpreted and implemented in accordance with the overriding constitutional principle that government action must serve the public interest and advance the common good of all Mozambicans;

**Recital 17: Fundamental Rights Protection**
GUARANTEEING that implementation of this Policy shall in no circumstances diminish or impair the fundamental rights guaranteed by our Constitution, and that any conflict between data governance objectives and constitutional rights shall be resolved in favour of constitutional supremacy;

**Recital 18: Democratic Accountability**
ESTABLISHING that all institutions and officials exercising authority under this Policy remain subject to democratic oversight, judicial review, and constitutional accountability mechanisms, ensuring that data governance serves democratic governance rather than replacing it.

# PART I: CONSTITUTIONAL FOUNDATIONS AND LEGAL AUTHORITY

# CHAPTER 1: LEGAL GENESIS AND CONSTITUTIONAL MANDATE

## Section 1.1: Citation, Short Title, and Legal Authority

1.1.1 Official Citation and Designation

This instrument shall be cited as the **"National Data Governance Policy of the Republic of Mozambique, 2025"** (hereinafter referred to as "the Policy") and may be referenced in abbreviated form as **"NDGP-2025"** in official documents, legal proceedings, and administrative communications.

1.1.2 Short Title and Common Reference

For purposes of legislative reference, administrative implementation, and public discourse, this Policy shall be known by the short title **"Data Governance Policy"** or **"DGP"** when the context clearly indicates reference to this national framework.

1.1.3 Constitutional and Legal Authority for Enactment

This Policy derives its authority from multiple convergent sources of constitutional and statutory power vested in the Government of the Republic of Mozambique:

### Primary Constitutional Authority:

- **Article 135** of the Constitution of the Republic of Mozambique, which grants the Council of Ministers competence to ensure the implementation of the country's domestic and foreign policy as defined by the Assembly of the Republic;
- **Article 179**, empowering the Government to promote economic and social development and satisfy the collective needs of citizens;
- **Article 71**, which mandates legislative action on the protection of personal data and establishes the constitutional foundation for data governance;

### Enabling Legislative Framework:

- **Law No. 3/2017 on Electronic Transactions**, which governs digital communications and establishes baseline requirements for electronic data handling;
- The **general legislative competence** of the Government under Article 203 of the Constitution to adopt regulations necessary for the effective administration of the State;

### International Legal Obligations:

- **African Union Convention on Cyber Security and Personal Data Protection** (Malabo Convention), ratified by Mozambique through Resolution No. 5/2019 of, June 20;

- **African Union Data Policy Framework**, adopted in 2022, which establishes continental standards for data governance and cross-border data flows;
- **International human rights instruments** incorporated into Mozambican law through Article 43 of the Constitution, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;

1.1.4 Hierarchical Legal Position

This Policy occupies a position of **constitutional derivative authority** within Mozambique's legal hierarchy, operating:

- **Below constitutional provisions**, which remain supreme and inviolable;
- **Above administrative regulations** and departmental guidelines, which must conform to this Policy's requirements;
- **As binding authority** for all government institutions, parastatals, and third parties operating under government contract or authorization;

## Section 1.2: Constitutional Basis and Enabling Legislation

1.2.1 Foundational Constitutional Provisions

The constitutional foundation for this Policy rests upon several interconnected provisions of the Constitution of the Republic of Mozambique that, when read harmoniously, establish both the necessity and authority for comprehensive data governance:

**Article 71 - Protection of Personal Data (Fundamental Rights)**

Article 71 of the Constitution provides the primary constitutional mandate for data protection, stating that:

*"(1) All citizens are entitled to the protection of their private life and have the right to honour, good name, reputation, protection of their public image and privacy.*
*(2) The law shall provide for the protection of personal data in computer records, and shall define the requirements for access to data banks and computer files, as well as for their creation and use by public and private entities."*

This provision establishes several critical constitutional principles:

- **Fundamental right to privacy** as an inherent human dignity protection;
- **Specific mandate for data protection legislation**, creating a constitutional imperative for frameworks such as this Policy;
- **Comprehensive scope** covering both public and private sector data handling;
- **Technical evolution recognition**, acknowledging that constitutional protection must adapt to technological advancement;

**Article 35 - Right to Information**

Article 35 guarantees citizens' right to information, establishing that:

*"Citizens have the right to be informed on matters of public interest through the mass media. The mass media shall not be subjected to censorship."*

This provision creates a **constitutional tension requiring careful balance** between data protection and information access rights, which this Policy addresses through its transparency and accountability provisions.

**Article 43 - Integration of International Law**
Article 43 incorporates international human rights instruments into domestic law, providing constitutional foundation for alignment with:

- **Universal Declaration of Human Rights** (Article 12 - privacy protection);
- **International Covenant on Civil and Political Rights** (Article 17 - privacy rights);
- **African Charter on Human and Peoples' Rights** (Article 8 - freedom of conscience and protection of privacy);

**Law No. 3/2017 on Electronic Transactions**
This legislation establishes the legal framework for digital communications and electronic data handling, providing:

- **Legal recognition** of electronic documents and digital signatures;
- **Security requirements** for electronic data transmission;
- **Consumer protection** provisions for electronic commerce;
- **Cross-border transaction** regulations affecting data flows;

1.2.3 Doctrinal Constitutional Interpretation
**Data Sovereignty as Constitutional Imperative**
The Policy's emphasis on data sovereignty derives from the constitutional principle of **national sovereignty** enshrined in Article 11 of the Constitution, which declares Mozambique as a sovereign state. This sovereignty extends to:

- **Territorial data jurisdiction** - authority over data generated or processed within Mozambican territory;
- **Personal data sovereignty** - protection of Mozambican citizens' data regardless of processing location;
- **Economic data sovereignty** - control over data contributing to national economic development;
- **Security data sovereignty** - protection of data affecting national security and public safety;

**Proportionality and Constitutional Balance**
Constitutional interpretation requires **proportionate balancing** of competing rights and interests:

- **Privacy vs. Security**: Balancing individual privacy rights with legitimate national security requirements;
- **Transparency vs. Confidentiality**: Harmonizing public information access with personal data protection;
- **Economic Development vs. Protection**: Enabling data-driven economic growth while preventing exploitation;
- **Innovation vs. Regulation**: Fostering technological advancement within appropriate governance frameworks;

Section 1.3: Relationship to National Development Framework

**1.3.1 Integration with the 2025-2044 National Development Strategy**

This Policy is intrinsically connected to and serves as an enabling instrument for Mozambique's **2025-2044 National Development Strategy,** which identifies digital transformation and data governance as critical components of sustainable development:

**Strategic Development Pillars Supported:**

**Economic Transformation and Diversification**

- **Data-driven economic analysis** enabling evidence-based policy formulation for industrial development;
- **Digital economy facilitation** through secure, trusted data exchange mechanisms;
- **Innovation ecosystem support** via open data initiatives and public-private data partnerships;
- **Investment attraction** through internationally recognized data protection standards;

**Human Capital Development**

- **Education system enhancement** through secure student data management and learning analytics;
- **Skills development tracking** via integrated workforce data systems;
- **Health outcomes improvement** through integrated health information systems;
- **Digital literacy advancement** supported by safe data handling practices;

**Infrastructure Development**

- **Digital infrastructure planning** informed by comprehensive national data collection;
- **Smart city initiatives** enabled by secure urban data management;
- **Rural connectivity enhancement** supported by geographic and demographic data analysis;
- **Climate-resilient infrastructure** development guided by environmental data systems;

1.3.2 Alignment with Digital Mozambique Agenda

The **Digital Mozambique Agenda** serves as the specific digital transformation strategy within which this Policy operates, establishing:

**Digital Government Services**

- **Interoperable e-government platforms** requiring standardized data governance;
- **Citizen service integration** demanding secure cross-agency data sharing;
- **Digital identity systems** necessitating comprehensive personal data protection;
- **Electronic service delivery** requiring trusted data handling mechanisms;

**Digital Economy Development**

- **Fintech and digital payments** requiring secure financial data governance;
- **E-commerce platform development** needing consumer data protection;
- **Digital entrepreneurship support** through data access and sharing frameworks;
- **Technology innovation hubs** enabled by research data collaboration;

**Digital Inclusion and Equity**

- **Universal access initiatives** requiring demographic data analysis;
- **Rural digital development** guided by geographic information systems;
- **Gender equality measurement** through disaggregated data collection;
- **Youth empowerment programs** supported by educational data integration;

1.3.3 Sectoral Development Integration

**Agriculture and Food Security**

This Policy enables **precision agriculture initiatives** and **food security monitoring** through:

- **Farmer registration systems** with secure personal data handling;
- **Crop monitoring data** integration across agricultural agencies;
- **Market information systems** with transparent data sharing protocols;
- **Climate adaptation strategies** informed by agricultural and meteorological data;

**Health System Strengthening**

The Policy supports **health system digitization** and **pandemic preparedness** via:

- **Electronic health records** with comprehensive privacy protection;
- **Disease surveillance systems** enabling rapid public health response;
- **Health research data** sharing with international partners under sovereignty safeguards;
- **Pharmaceutical supply chain** tracking through integrated data systems;

**Education and Human Resource Development**

Educational advancement is facilitated through:

- **Student information systems** with robust privacy protections;
- **Learning analytics platforms** enabling personalized education;
- **Teacher professional development** tracking and certification systems;
- **Research data collaboration** between educational institutions;

Section 1.4: International Treaty Obligations and Commitments

**1.4.1 African Union Framework Compliance**

**African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)**

Mozambique's ratification of the Malabo Convention through **Resolution No. 5/2019** creates binding international obligations that this Policy implements:

**Personal Data Protection Obligations:**

- **Consent and legitimacy** requirements for data processing;
- **Purpose limitation** and **data minimization** principles;
- **Data subject rights** including access, rectification, and erasure;
- **Security safeguards** and **breach notification** requirements;
- **Cross-border transfer** restrictions and adequacy determinations;

**Cybersecurity Coordination Requirements:**

- **National cybersecurity strategy** development and implementation;
- **Regional cooperation** on cyber threat intelligence sharing;
- **Critical infrastructure protection** including data system security;
- **Capacity building** and **international cooperation** on cybersecurity matters;

**African Union Data Policy Framework Implementation**

The **AU Data Policy Framework** adopted in 2022 establishes continental standards that this Policy incorporates:

**Fundamental Principles Integration:**

- **Data sovereignty** and **self-governance** capabilities;
- **Free data flow** balanced with **adequate protection** measures;

- **Cooperative governance** mechanisms across AU member states;
- **Equitable benefit sharing** from data-driven economic development;

**Operational Commitments:**

- **Harmonized data governance** frameworks across the continent;
- **Cross-border data transfer** mechanisms with appropriate safeguards;
- **Regional data cooperation** on matters of mutual interest;
- **Capacity building support** for data governance institutions;

### 1.4.2 Global Human Rights Framework Integration

**Universal Declaration of Human Rights (UDHR)**

Article 12 of the UDHR establishes the fundamental human right to privacy, which this Policy implements through:

- **Comprehensive privacy protection** mechanisms in data processing;
- **Individual consent** requirements and **purpose limitation** safeguards;
- **Security measures** preventing **arbitrary interference** with personal data;
- **Legal remedy** provisions for privacy violations;

**International Covenant on Civil and Political Rights (ICCPR)**

Article 17 of the ICCPR creates binding legal obligations for privacy protection that this Policy addresses:

- **Legal framework** establishment for privacy protection;
- **Effective remedies** for privacy violations;
- **Proportionality assessment** for data processing activities;
- **Non-discrimination** principles in data handling;

### 1.4.3 Economic and Trade Agreement Implications

**African Continental Free Trade Agreement (AfCFTA)**

The AfCFTA's digital trade provisions create specific obligations affecting data governance:

**Digital Trade Facilitation:**

- **Cross-border data flow** facilitation for legitimate commercial purposes;
- **Digital services** market access requiring data protection harmonization;
- **Electronic commerce** development with consumer data protection;
- **Intellectual property** protection in digital environments;

**Economic Integration Requirements:**

- **Regulatory harmonization** to reduce trade barriers;
- **Mutual recognition** of data protection standards;
- **Dispute resolution** mechanisms for data-related trade conflicts;
- **Capacity building** support for data governance institutions;

### 1.4.4 International Cooperation Frameworks

**United Nations E-Government Development**

Alignment with UN e-government best practices requires:

- **Government data transparency** initiatives;
- **Citizen service digitization** with privacy protection;
- **Inter-agency data sharing** protocols;
- **Sustainable development goals** measurement through data systems;

**International Organization for Standardization (ISO) Compliance**

This Policy incorporates relevant ISO standards:

- **ISO 27001** (Information Security Management Systems);
- **ISO 29100** (Privacy Framework);
- **ISO 8000** (Data Quality);
- **ISO 25012** (Data Quality Model);

**Bilateral and Multilateral Data Agreements**

The Policy establishes framework for:

- **Data sharing agreements** with development partners;
- **Technical cooperation** on data governance capacity building;
- **Research collaboration** with international institutions;
- **Cross-border law enforcement** cooperation on data-related crimes;

# CHAPTER 2: CONCEPTUAL ARCHITECTURE AND INTERPRETATIVE FRAMEWORK

## 2.1 Definitions and Legal Interpretation

### 2.1.1 Authoritative Definitions

For the purposes of this Policy, the following definitions are adopted, drawing on statutory texts and international frameworks, and prevailing doctrine:

- **"Data"**: Any representation of facts, information, concepts, or instructions in a form suitable for communication, interpretation, or processing, whether by human or automated means, and regardless of format or medium.
- **"Personal Data"**: Any information relating to an identified or identifiable natural person ("data subject"), including but not limited to, names, identification numbers, location data, online identifiers, or elements peculiar to the physical, physiological, genetic, mental, economic, cultural, or social identity of a person.
- **"Data Processing"**: Any operation or set of operations which is performed upon data, whether or not by automatic means, including collection, registration, organization, storage, adaptation, alteration, retrieval, consultation, use, dissemination, erasure, or destruction.
- **"Data Controller"**: The natural or legal person, public authority, or other body which, alone or jointly with others, determines the purposes and means of data processing.
- **"Data Sovereignty"**: The supreme and inherent right of the Republic of Mozambique to determine the legal, operational, and ethical parameters for the creation, collection, processing, transfer, and storage of all data within its jurisdiction and related to its nationals, regardless of processing location.
- **"Digital Rights"**: The bundle of constitutional, statutory, and treaty-based rights pertaining to individuals in the context of digital environments, including rights to privacy, data protection, access to information, freedom of expression, and protection from discrimination and surveillance.

Any undefined terms in this Policy shall be interpreted in accordance with the Constitution of Mozambique, relevant sectoral legislation, and the doctrine of purposive interpretation favouring the advancement of rights, digital inclusion, and national security.

### 2.1.2 Interpretative Principles

- This Policy shall be interpreted in light of its preamble, recitals, and referenced constitutional and international rights.
- In cases of ambiguity, an interpretation that protects the dignity, privacy, and freedoms of individuals, and advances national development goals, shall prevail.

## 2.2 Doctrinal Foundations of Data Sovereignty

### 2.2.1 Constitutional and Political Doctrine

Data sovereignty is founded upon Article 11 of the Constitution (national sovereignty); Article 71 (privacy and personal data), and reinforced by Mozambique's political and legal tradition of state sovereignty, independence, and self-governance.

- **National Data Jurisdiction**: The power to govern all data generated, processed, or stored within the territory of Mozambique, or affecting Mozambican citizens and entities, wherever located.
- **Personal Data Sovereignty**: Recognition that data about Mozambican citizens is a legal extension of the person, protected by the constitutional right to privacy and subject to Mozambican jurisdiction irrespective of processing venue.
- **Sovereignty and International Cooperation**: While recognizing the need for collaboration under the AU Data Policy Framework and international law, national sovereignty remains paramount for all foundational matters regarding data governance, security, and ethical use in digital environments.

2.2.2 Technological and Socioeconomic Rationale

Data sovereignty also rests on:

- The increasing centrality of data for economic growth, public policy, and national development.
- The risks posed by data colonialism, extraterritorial processing, and over-reliance on foreign digital infrastructure.
- The imperative to build national capacity technological, institutional, and human for autonomous data lifecycle management and innovation.

## 2.3 Constitutional Principles of Digital Rights

2.3.1 Enumerated Digital Rights under Mozambican Law

- Right to Privacy and Data Protection: Article 71 bestows an enforceable right to privacy and mandates legal protection of personal data.
- Right to Access Information: Article 35 upholds citizen access to public information, subject to privacy and security limitations.
- Freedom of Expression and Digital Participation: The right to digital expression, communication, and participation in digital society, implied within constitutional freedoms and the spirit of democratic participation.
- Protection from Arbitrary Interference and Profiling: Prohibition of unjustified state or private surveillance, profiling, discrimination, or algorithmic bias.
- Right to Remedy and Redress: Effective legal remedies for persons whose digital rights are violated, including by automated processing or through cybersecurity breaches.

2.3.2 Alignment with International and Regional Instruments

- Universal Declaration of Human Rights (Article 12)
- International Covenant on Civil and Political Rights (Article 17)
- African Union Data Policy Framework and Malabo Convention: Reinforcing local and regional protection principles and facilitating cross-border rights continuity.

## 2.4 Jurisprudential Hierarchy and Conflict Resolution

2.4.1 Hierarchy of Norms

The following interpretative hierarchy applies:

1. **The Constitution of Mozambique** is supreme; all rights, powers, and conflicts are resolved in accordance with its text and spirit.
2. **International Treaties** ratified by Mozambique, as incorporated via Article 43 of the Constitution, next provide mandatory interpretative authority, provided they do not derogate from constitutional rights.
3. **Statutory Law** most notably the Law of Electronic Transactions (No. 3/2017) governs detailed operationalization, so far as compatible with the Constitution and treaties.
4. **This Policy**, as a delegated instrument, binds all public bodies, parastatals, and authorized entities, and prevails over conflicting subordinate regulations.
5. **Jurisprudence** and jurisprudential doctrine (Supreme Court, Constitutional Council, and relevant international courts) guide interpretation where ambiguity or conflict arises.

2.4.2 Principles for Conflict Resolution

- **Supremacy of Fundamental Rights**: In case of conflict between digital innovation and fundamental rights (privacy, equality, dignity), rights shall prevail unless limiting measures are demonstrably necessary, proportionate, and prescribed by law.
- **Balancing and Proportionality**: The Policy and its interpretation shall reflect a balance between privacy/security, and openness/innovation, in line with best constitutional and international practice.
- **Interpretative Favour**: Where two or more plausible interpretations arise, the interpretation most compatible with Mozambique's constitutional values and international obligations shall be presumed correct.

# PART II: SUBSTANTIVE SCOPE AND JURISDICTIONAL ARCHITECTURE

## Chapter 3: Territorial and Personal Jurisdiction

### 3.1 Territorial Application and Extraterritorial Reach

3.1.1 National Territory

This Policy applies to all data processed, stored, transmitted, or otherwise handled:

- Within the physical borders of the Republic of Mozambique, including land, airspace, territorial waters, and all infrastructure under Mozambican control;
- By public institutions, government organs, parastatals, state-owned enterprises, and any private actors operating therein.

3.1.2 Digital Infrastructure with Local Effect

Any data infrastructure (servers, cloud platforms, data centres, network endpoints) located or functionally resident in Mozambique is subject to this Policy, irrespective of the nationality or residence of the data subject, controller, or processor.

3.1.3 Extraterritorial Reach
This Policy extends, consistent with Law No. 22/2021 and international custom, to acts of data processing that:

- Involve data about Mozambican citizens or legal persons, wherever located;
- Affect the interests, rights, or security of Mozambique or its people, or produce effects within Mozambican territory, even if initiated abroad;
- Are performed by foreign entities offering goods or services to, or monitoring the behaviour of, individuals in Mozambique.

## 3.2 Personal Jurisdiction Over Data Controllers and Processors

3.2.1 Subject Persons
This Policy binds:

- All natural or legal persons established, incorporated, or registered in Mozambique who act as data controllers, joint controllers, or processors;
- Any foreign natural or legal person, entity, or group that processes data covered by §3.1, if such processing is directed to or impacts Mozambican residents, institutions, or government affairs.

3.2.2 Obligations of Extraterritorial Entities
Foreign data controllers or processors who process Mozambican data or engage with Mozambican data subjects must:

- Designate a representative resident in Mozambique, with capacity to be served with legal process;
- Comply with all substantive and procedural requirements of this Policy, unless a recognized international agreement provides equivalent or higher safeguards.

3.2.3 Accountability and Liability
Data controllers and processors are jointly and severally liable for all compliance obligations under this Policy, regardless of delegation, outsourcing, or contractual arrangements, unless otherwise prescribed by law.

## 3.3 Cross-Border Data Flows and International Comity

3.3.1 Default Position: Controlled Transfers
Cross-border transfers of personal or sensitive data from Mozambique are permissible only if:

- The recipient state or entity provides an **adequate level of protection**, as determined by the competent Mozambican authority considering constitutional standards and the Data Protection framework in force in Mozambique.
- There are enforceable data subject rights and effective legal remedies in the destination jurisdiction.

3.3.2 Exceptions and Special Mechanisms
Transfers without adequacy determination require:

- Explicit, informed, and revocable consent of the data subject (except where overridden by law or vital public interest);
- Safeguards such as binding corporate rules, standard contractual clauses, codes of conduct approved by the national authority, or international frameworks to which Mozambique is party.

3.3.3 Regional and International Comity
In the spirit of international and continental digital integration:

- Data flows within African Union member states and AfCFTA partners may be facilitated pursuant to mutual adequacy or harmonized rules, provided Mozambican constitutional rights are preserved;
- Bilateral and multilateral agreements govern unique sectoral data flows in line with national interest, provided always that fundamental rights remain paramount.

3.3.4 Jurisdiction in International Disputes

All disputes involving transborder data flows, compliance failures, or breach of this Policy's provisions are subject to Mozambican court jurisdiction, except where a binding treaty prescribes otherwise and Mozambican sovereign interests are not undermined.

## 3.4 Diplomatic Data and Sovereign Immunity

3.4.1 Diplomatic Data Exemption

This Policy does not apply to the processing, storage, or exchange of official diplomatic correspondence, state secrets, or information relating to the core functions of foreign missions accredited to Mozambique, as protected under the Vienna Convention on Diplomatic Relations.

3.4.2 Sovereign Immunity

Nothing in this Policy shall be construed to derogate from the principles of sovereign immunity in international law, as recognized by Mozambican courts, in respect of data held by diplomatic missions, consular posts, or international organizations lawfully enjoying immunity in Mozambique.

3.4.3 National Security Data

Processing of data determined by competent authority to be a matter of state security, defence, or essential public interest is governed by specialized legislation and exempted from select provisions of this Policy, provided such exceptions remain necessary, proportionate, and subject to constitutional review.

# Chapter 4: Material Scope and Data Classification Taxonomy

## 4.1 Comprehensive Data Domain Classification

4.1.1 Foundational Data Domains

The Policy's material scope includes all data types fundamental to Mozambique's governance, development, economy, and public interest. Recognizing the diversity and unique risks inherent to each class, data is hereby classified as follows:

- **Personal Data**: Information relating to an identified or identifiable natural person, including sensitive categories (health, biometrics, identity numbers, etc.).
- **Administrative and Public Administration Data**: Data generated, used, or stored by governmental, regulatory, or public entities in the execution of their functions (registries, permits, executive records, fiscal data, etc.).
- **Geospatial Data**: Data representing locations, property boundaries, spatial features, topographic, environmental, or infrastructural information.

- **Statistical Data**: Data aggregated or anonymized for the purposes of official statistics, policy analysis, development planning, or research.
- **Open and Public Data**: Non-confidential data proactively released to the public domain for reuse, transparency, innovation (such as government budget data, environmental indicators, etc.).
- **Financial Data**: Data related to monetary transactions, banking, credit, taxation, capital market activities, public and private finance.
- **Sector-Specific Data**: Distinguished by domain, as elaborated below.

#### 4.1.2 Sectoral Data Classifications

To promote responsive, sector-specific governance and harmonization with regional and international best practice (including European Open Science Cloud, the Green Deal, and AU frameworks), the following special data categories are recognized[U1]:

- **Health Data**: Patient records, genomic data, health system analytics, public health surveillance, pandemic and epidemiological data.
- **Agricultural Data**: Land registry, crop yields, input and subsidy usage, agricultural extension, climate and meteorological data relevant for food security.
- **Manufacturing Data**: Industrial production records, supply chains, quality control, industrial IoT data, workplace safety and compliance.
- **Energy Data**: Generation, distribution, consumption, renewable sources, grid analytics, carbon and emissions data.
- **Mobility Data**: Transport flows, smart mobility, urban planning, vehicle registration, logistics and movement patterns.
- **Skills and Human Capital Data**: Educational records, vocational and professional certification, workforce analytics, employment data.
- **Tourism Data**: Visitor flows, accommodation records, events, service ratings, and related economic metrics.
- **Construction Data**: Building permits, project plans, supply chains, compliance certifications, accident statistics.
- **Media and Information Society Data**: Digital content, broadcast analytics, social media data, audience measures.
- **Cultural Heritage Data**: Museum inventories, archives, digital preservation, audio-visual and historical records.
- **Environmental and Green Deal Data**: Sustainability metrics, resource use, pollution and emission statistics, ecosystem and biodiversity indicators.
- **Research Data (including EOSC scope)**: Data produced in academic, industrial, or applied scientific efforts, whether structured for open access or subject to rights management.

### 4.2 Covered Entities (Government, Parastatals, Third Parties)

#### 4.2.1 Governmental Bodies

- All levels and branches of government (national, provincial, local).
- Regulatory authorities, commissions, administrative agencies.

#### 4.2.2 State-Owned Enterprises and Parastatals

- Enterprises majority or wholly owned by the State.

- Statutory bodies, public utility providers, or corporations with delegated public functions.

4.2.3 Private and Third-Party Actors

- Contractors, consultants, public-private partnerships, NGOs, academic or scientific organizations acting for or with government entities.
- Any entity (domestic or foreign) that processes, stores, analyses, or transmits covered data by virtue of a legal, contractual, or operational link to the state or its agencies.

**All covered entities bear direct legal responsibility for compliance with this Policy and subordinate legal instruments.**

## 4.3 Exclusions and Carve-Outs from Policy Application

4.3.1 National Security and Défense

- Data classified as state security, defence, intelligence, or law enforcement-sensitive are regulated by separate, specialized frameworks. Access to, and secondary use of, such data is strictly limited by applicable law.

4.3.2 Diplomatic and Sovereign Data

- Processing or transmission of data pertaining to foreign diplomatic missions, consular correspondence, or data afforded sovereign immunity under international law is exempted in accordance with international treaties and custom (cf. Vienna Convention).

4.3.3 Purely Personal or Household Data

- Data generated and used in a purely personal, family, or household context are excluded from policy scope, except where further processed for professional, public or economic purposes.

4.3.4 Exogenous Data and Foreign Sovereignty

- Data generated, stored, or processed entirely outside Mozambique and not relating to Mozambican entities, persons, or interests are generally excluded, except where defined under extraterritorial provisions (see Chapter 3).

4.3.5 Special Carve-Outs

- Scientific research data subject to established conventions of academic freedom and ethical review, unless otherwise mandated by law for public interest.
- Media reporting, editorial content, and artistic expression, subject to constitutional freedom of expression and information, unless processing falls within regulated data categories (e.g., personal data of non-public figures).

## 4.4 Gradations of Data Sensitivity and Protection Levels

4.4.1 Data Sensitivity Taxonomy

A four-level, mandatory sensitivity classification is established, which must be applied in all state and parastatal data handling and recommended as best practice for others:

1. **Public Data**: No confidentiality risk; explicitly intended for dissemination or open reuse, subject only to integrity and lawful use constraints.
2. **Restricted Data**: Disclosure would prejudice specific interests (organizational, sectoral); access limited to authorized roles/processes, audit trails required.

3. **Confidential Data**: Disclosure would cause material prejudice to state interests, individual rights, public security, or economic integrity. Requires high controls (encryption, logging, strict access, and retention and deletion practices).
4. **Secret/Classified Data**: National security, sovereign, or life-critical information whose disclosure would cause irreparable harm. Subject to highest legal and technical controls, including compartmentalization, redaction, mandatory reporting, and penalty regimes.

4.4.2 Protection Regimes and Required Measures

- **All Personal data** must receive adequate protection against unauthorized access, loss, or misuse, scaled by its classification and in accordance with Data Protection provisions in force in Mozambique.
- **Sensitive data (health, finance, security, minors, etc.)** are subject to additional statutory protections, including stricter consent, breach notification, regulatory reporting, and audit.
- **Sectoral guidance** may mandate further controls tailored to evolving risks and international good practice (e.g., European Open Science Cloud for scientific data, GDPR-like standards for personal data).

**Section 2. Scope and Applicability**

**Data Domains Covered**

All domains as listed above are included. Each sector cited public administration, health, agriculture, manufacturing, energy, mobility, skills, open science, green deal, tourism, construction, media, cultural heritage has designated data types classified and protected under this Policy and subordinate regulation[U2].

**Covered Entities**

Application is universal across government, public sector bodies, parastatals, third-party partners, and any actor who, by law or contract, handles covered data for or with legal persons in Mozambique.

**Exclusions and Boundaries**

Exclusions (diplomatic, defence, familial/private, purely exogenous data, protected media and art) are strictly construed and do not extend to circumvent obligations where public interest, law, or rights to remedy so require.

**Jurisdiction and Cross-Border Considerations**

All cross-border activities (data transfer, processing, cloud storage) are only lawful to the extent they fulfil Mozambican adequacy, safeguarding, and legal remedy requirements as established in this Policy and relevant international agreements (see Chapter 3).

# Chapter 5: Supreme Data Governance Authority

## 5.1 National Data Governance Council: Constitutional Status

5.1.1 Constitutional Foundation

The National Data Governance Council (NDGC) is hereby established as the supreme coordinating and oversight body for national data governance policy implementation. Its

creation is authorized under the general regulatory and organizational powers of the Council of Ministers and relevant Ministries as provided by the Constitution of Mozambique (notably Article 135, on governmental powers, and Article 71, on the protection of privacy and personal data), and complemented by statutory mandates under existing and future data-related legislation.

Whereas specific data regulatory functions—such as personal data protection—are conferred by relevant law upon the Autoridade Nacional de Protecção de Dados (ANPD), the NDGC's authority derives from this Policy and implementing acts, serving as the central platform for cross-sectoral coordination, standard-setting, and high-level strategic oversight across all governmental and parastatal entities.
and in furtherance of the state's obligation to protect personal data and regulate digital affairs as essential components of national sovereignty and development.

5.1.2 Legal Personality and Autonomy
The NDGC:

- Bears the status of an independent statutory body with legal personality, administrative, and financial autonomy, and the power to sue and be sued in its own name.
- Is insulated against undue influence and governmental interference in the discharge of quasi-judicial or regulatory functions, subject only to constitutional and lawful oversight.
- May enter into agreements, acquire assets, and manage resources as necessary for fulfilling its mandate.

5.1.3 Perpetuity and Abrogation
The NDGC exists in perpetuity unless expressly dissolved by legislation of equal or higher constitutional order and with due process ensuring continuity or lawful transfer of core functions.

## 5.2 Composition, Appointment, and Tenure Security

5.2.1 Membership Composition
The NDGC consists of not fewer than 11 and not more than 17 members chosen for expertise, integrity, and representativeness, including:

- Ex officio: The Minister or Deputy Minister responsible for digital transformation or communications.
- Standing representatives: Key ministries (Justice, Finance, Education, Agriculture, Health, Energy), the Data Protection Authority, and judiciary liaison (non-voting[U3]).
- Appointed experts: Information security, data science, ethics/law, civil society, academia, private sector, and regional or international organizations.

5.2.2 Appointment and Confirmation

- Members are nominated via transparent, merit-based processes, including public calls for expression of interest for non-ex officio seats.

- Appointment is formalized by Presidential Decree upon nomination by the Government, subject to confirmation by a two-thirds majority vote of the National Assembly for at-large/expert seats.
- Diversity of gender, geography, and sector is prioritized in the final composition.

5.2.3 Tenure, Renewal, and Removal

- Standard tenure is five years, renewable once, except for ex officio positions.
- Members may only be removed before term expiration by judicial order or qualified decision of the National Assembly for proven gross misconduct, incapacity, or violation of constitutional trust.
- The Council must maintain a public register of all appointments, renewals, removals, and reasons thereof.

## 5.3 Powers, Functions, and Decision-Making Procedures

5.3.1 Powers

The NDGC is vested with the supreme authority to:

- Issue, amend, and revoke mandatory data governance standards, sectoral codes, and interpretative guidelines for all covered entities.
- Direct, coordinate, and oversee implementation of the National Data Governance Policy and related statutes.
- Regulate data classification, sharing, cross-border transfer[U4], risk and impact assessment, and certification or accreditation of data-handling systems.
- Approve, suspend, or sanction the data governance activities and compliance status of government, parastatals, and significant third-party actors.
- Initiate or join legal proceedings to enforce compliance or defend the public interest in the courts of Mozambique.
- Facilitate national and international cooperation, including conclusion of cooperation agreements and representation at regional/global data fora.

5.3.2 Functions

The Council performs, in addition to above, the following:

- Regular policy reviews and submission of annual reports to the Government and Parliament.
- Oversight of key appointments for subordinate data governance offices/bodies.
- Promotion of data literacy, open data initiatives, ethical standards, and public awareness campaigns.
- Mediation and arbitration in cross-sectoral data disputes, with published decisions where appropriate.
- Recommendation of legislative and regulatory reforms based on technological, legal, or socioeconomic advancements.

5.3.3 Decision-Making Procedures

- All major decisions require quorum (majority of current membership) and, for standard-setting or sanctions, a supermajority (two thirds of voting members present).
- Dissenting views, where held by three or more members, must be recorded and made public unless subject to confidentiality for national security.

- Decisions of general application are published in an official, accessible, and searchable digital register.

## 5.4 Relationship with Executive, Legislative, and Judicial Branches

5.4.1 Executive

The NDGC:

- Advises, but is not subordinate to, any executive branch member or organ on policy and compliance issues.
- Must be consulted on any executive-led digitization, e-government, or cross-ministerial IT initiative directly implicating governance of covered data domains.

5.4.2 Legislative

- Submits annual policy and activity reports directly to the National Assembly.
- May be summoned by Parliamentary committees for oversight, questions, or review of major cross-sectoral data matters.
- Can propose legislative amendments and issue formal opinions on bills affecting data governance.

5.4.3 Judiciary

- Is subject to judicial review by the Supreme Court, Constitutional Council, and qualified courts, but its policy and sanction decisions are presumptively valid unless demonstrably arbitrary, ultra vires, or unconstitutional.
- Cooperates on matters of judicial evidence, data-related discovery, and advisory opinions at the intersection of law and technology.
- Maintains appropriate channel for confidential or privileged material as prescribed by law (in camera review).

# Chapter 6: Distributed Governance Architecture

## 6.1 Chief Data Officers: Institutional Mandate and Authority

6.1.1 Appointment and Constitutional Basis

Each ministry, major public agency, and parastatal must appoint an institutional Chief Data Officer (CDO[U5]), by formal executive order or statutory mandate, as the apex authority for data stewardship, governance, and compliance within their domain.

6.1.2 Powers and Duties

- **Policy Localization:** CDOs are responsible for localizing the National Data Governance Policy (NDGP) according to sectoral needs, institutional architecture, and operational complexity, subject to overarching NDGC oversight.
- **Strategic Planning:** Each CDO develops, implements, and periodically revises a sectoral Data Governance Strategy, covering data lifecycle management, quality control, risk assessment, and audit readiness.
- **Supervision and Compliance:** CDOs exercise oversight of all data-related activities, ensuring subordinate teams adhere to legal requirements, professional standards,

and sector-specific guidelines; CDOs have the authority to halt, revise, or escalate non-compliant data processes.
- **Reporting:** CDOs deliver biannual compliance and performance reports to the NDGC, including key metrics, incident notifications, and reform proposals.
- **Advisory Function:** Serve as principal advisor to agency leadership on data policy, emerging threats, data innovation opportunities, and regulatory change.
- **Capacity Building:** Drive professional training and data literacy initiatives within their organization and coordinate ongoing certification and standards adherence for data staff.

6.1.3 Independence and Accountability

While institutionally anchored, CDOs are protected from arbitrary removal; their tenure, performance review, and removal processes are governed by transparent, merit-based, and legally prescribed criteria, with judicial review available for contested removals.

## 6.2 Data Stewardship Network and Professional Standards

6.2.1 Data Stewards: Roles and Deployment

- **Designation:** Agencies appoint data stewards at operational, project, and domain levels to serve as the primary custodians for assigned datasets, systems, or services.
- **Core Tasks:** Data stewards ensure metadata quality, data lineage documentation, and compliance with access, retention, and archiving rules; steward networks are tasked with daily monitoring of quality controls and user permissions.
- **Coordination:** Each CDO forms and maintains a Data Stewardship Committee, meeting monthly, to harmonize standards, resolve operational issues, and share best practices.

6.2.2 Professional Standards and Continuous Improvement

- **Credentialing:** Data stewards must meet minimum professional certification in data governance or a recognized equivalent, subject to periodic renewal and upskilling.
- **Ethical Code:** Stewards adhere to a published professional code of data ethics, emphasizing impartiality, transparency, privacy, and duty to the public interest; major breaches subject to disciplinary procedure and, where applicable, professional sanction.
- **Peer Review:** Staged peer-review mechanisms allow cross-institutional learning, benchmarking, and continuous improvement of stewardship practices.

## 6.3 Sectoral Data Governance Bodies and Specialization

6.3.1 Sectoral Councils and Committees

- **Establishment:** Sector-specific data governance councils (e.g., health, agriculture, finance, education, environmental data) are created by regulation or NDGC directive to address field-specific risks, norms, and regulatory adaptations.
- **Representation:** Councils comprise sectoral CDOs, leading data architects, information security officers, relevant regulators, domain experts, and sanctioned civil society observers.
- **Mandate:** Responsible for the interpretation of policy as it applies to domain-specific laws and challenges (e.g., sensitive health information, agri-environmental data aggregation for climate reporting, financial data and anti-fraud controls).

6.3.2 Specialized Subcommittees

- **Emerging Technologies:** Create standing or ad hoc subcommittees for domains facing rapid technological advance (e.g., AI in healthcare, IoT in critical infrastructure, real-time mobility data).
- **Incident Response:** Maintain rapid-response protocols for sector-specific data incidents, ensuring agile and coordinated action in line with national standards.

6.3.3 Integration and Alignment

- Ensure sectoral policies and standards are consistent with the NDGC, but allow for justified variation due to scientific, legal, or operational necessity with escalation to the NDGC for dispute resolution.

## 6.4 Multi-Stakeholder Engagement and Civil Society Integration

6.4.1 Civil Society and Community Involvement

- **Consultative Forums:** The NDGC and CDOs must host regular public forums, inviting civil society, academic, indigenous, and private sector voices in agenda setting, policy review, and program evaluation.
- **Public Submissions and Hearings:** Mechanisms for written and oral submissions on major policy changes, new technology deployments, and sectoral data initiatives are standardized and must be broadly advertised.
- **Transparency Commitments:** Summaries of deliberations and final recommendations are published in accessible formats and periodically translated into relevant local languages.

6.4.2 Academia and Scientific Networks

- **Research Partnerships:** Encourage formal partnerships between sectoral bodies and universities or research institutes to foster evidence-based governance, promote open science, and enable rapid technology transfer.
- **Data Commons:** Where practical and legally compliant, promote open data platforms for collaborative science (e.g., participation in European Open Science Cloud, climate and Green Deal-aligned research).

6.4.3 Private Sector and International Engagement

- Involve private sector actors (including startups, technology firms, digital entrepreneurs) in sectoral innovation panels, open data hackathons, and regulatory sandboxes under NDGC oversight.
- Representation at regional/global policy fora (AU, SADC, UN) incorporates civil society delegates for legitimacy and transparency.

6.4.4 Monitoring, Feedback, and Accountability

- All stakeholder consultations must include mechanisms for structured feedback, documentation of outcomes, and clear government responses to substantive input.
- Civil society may trigger special NDGC review of contentious or high-impact projects via a petition process with threshold support.

# Chapter 7: Constitutional Data Principles

## 7.1 Data Sovereignty as Constitutional Imperative

### 7.1.1 Principle and Scope

Data sovereignty is affirmed as a fundamental expression of national independence, dignity, and the right of the people of Mozambique to exercise effective and exclusive authority over data generated, processed, or stored within its jurisdiction and relating to its citizens, government, or vital interests.

### 7.1.2 Constitutional Basis

- Rooted in Article 11 (National Sovereignty) and Article 71 (Privacy and Data Protection) of the Constitution.
- Reinforced by international commitments (AU Data Policy Framework, Malabo Convention, ICCPR) respecting the nation's right to self-determine its digital and data regulatory frameworks.

### 7.1.3 Operationalization

- The State may legislate, regulate, and enforce all aspects of data lifecycle management within its borders; no transnational, supranational, or private actor may derogate from these rights, save by explicit, democratically-conferred treaty or legal exception.
- Data of Mozambican citizens remains subject to Mozambique's legal protections regardless of location, processing venue, or cross-border flow a principle extended by statutory and treaty instruments (see Chapters 3–4).

## 7.2 Digital Dignity and Fundamental Rights Integration

### 7.2.1 Digital Dignity Principle

Every Mozambican is entitled to digital dignity, which extends inherent constitutional values of equality, honour, privacy, and development into digital and data-driven domains.

### 7.2.2 Rights Integration

- **Right to Privacy and Data Protection:** Data is not only an economic asset, but an extension of the person, protected by Law and constitutional doctrine.
- **Freedom of Expression, Access to Information, and Non-Discrimination:** All data governance must be implemented in a manner that advances, and never unjustifiably restricts, these rights.
- **Protection from Arbitrary Interference and Profiling:** No data processing, especially through automated or algorithmic means, may violate the dignity, autonomy, or legitimate expectations of persons.

### 7.2.3 Vulnerable Groups and Inclusion

Data principles expressly recognize and mandate additional safeguards for marginalized, at-risk, or underrepresented populations, in alignment with Mozambique's obligations under international humanitarian and human rights instruments.

## 7.3 Proportionality and the Necessary and Proportionate Test

7.3.1 Constitutional Test

No data governance measure legislative, regulatory, administrative, or technical may restrict fundamental rights or the legitimate interests of persons or entities unless it can be shown to be:

- **Necessary:** There is a clear, constitutionally valid public or private purpose requiring intervention.
- **Proportionate:** The measure is the least restrictive means available to achieve the stated objective and is not excessive relative to the risk or harm.
- **Prescribed by Law:** The restriction or measure must be based on accessible, clear, and predictable legal rules, subject to judicial review.

7.3.2 Burden and Review

- The burden of demonstrating necessity and proportionality falls upon the State or the regulating entity[U6].
- All material restrictions or intrusions on data rights are subject to robust, independent review (administrative and judicial), with written reasons required for any derogation.

7.3.3 Periodic Reassessment

Data governance interventions of significant scope or impact are subject to periodic reassessment for continued necessity, proportionality, and compatibility with updated constitutional norms, technological advances, and evolving national priorities.

## 7.4 Democratic Accountability and Transparency Mandates

7.4.1 Public Reason-Giving and Participation

- All major data governance decisions (such as the adoption of standards, data sharing agreements, or cross-border transfer frameworks) must be accompanied by public, accessible justification and opportunity for consultation or challenge.
- Data governance agencies must maintain searchable public registers of standards, decisions, and compliance actions, subject only to necessary confidentiality exceptions.

7.4.2 Right to Explanation and Remedy

- Individuals must be informed, in accessible language and with reasonable notice, of any data processing initiative that materially affects their rights or interests; meaningful remedies for errors, misuse, or abuse must be provided.
- Judicial and administrative review is mandatory and must be available to any affected person, group, or institutional litigant.

7.4.3 Oversight by Representative Bodies

- Parliamentary committees and independent auditors/ombudspersons have standing authority to review data governance agencies, policies, implementation, and performance, and to publish findings.
- Periodic public reporting and external audits are mandated to maintain continuous public trust and fidelity to democratic governance.

# Chapter[U7] 8: Operational Governance Principles

## 8.1 Data Quality as Public Trust Obligation

8.1.1 Principle and Rationale

Data quality is affirmed as both a constitutional and fiduciary duty of all state organs, public authorities, parastatals, and entrusted private actors. High-quality data is necessary to foster public trust, ensure sound policy and decision-making, and guarantee the rights and dignity of individuals.

8.1.2 Dimensions of Data Quality

All entities are explicitly obligated to ensure:

- **Accuracy:** Data must faithfully reflect the real-world facts or events it purports to describe.
- **Completeness and Consistency:** Records must be comprehensive and logically aligned across systems, avoiding fragmentation or contradictions.
- **Timeliness:** Data must be regularly updated and accessible within decision-relevant timeframes.
- **Reliability and Verifiability:** Processes must exist for continuous validation, error correction, and auditability throughout the data lifecycle.

8.1.3 Public Trust and Accountability

- Data quality failures are not merely technical lapses but breaches of public trust, with the potential for significant societal, economic, or individual harm.
- Institutions are required to maintain transparent mechanisms for citizens to challenge, correct, or inquire about data affecting them, and periodic quality audits must be conducted and published as a matter of public record.

## 8.2 Interoperability and Systemic Coherence

8.2.1 Principle

Seamless interoperability technical, semantic, legal, and organizational among state systems and between sectors is a core requirement for coherent digital governance, resource efficiency, and national resilience.

8.2.2 Mandatory Coherence Measures

- **Common Standards:** All data systems shall adopt NDGC-prescribed standards for data formats, taxonomies, and interfaces, harmonized where feasible with African Union, international, and European frameworks (such as the European Open Science Cloud).
- **Open APIs and Protocols:** Agencies must utilize, where possible, open or standardized APIs to facilitate secure exchange and usage of data across institutional and sectoral boundaries.
- **Meta-Data and Traceability:** All critical datasets must carry metadata records that enable clear determination of provenance, context, modifications, and legitimate linkage to other datasets.

8.2.3 Governance for Coherence

A standing Interoperability Committee, reporting to the NDGC, oversees and enforces systemic coherence, arbitrates disputes, and manages transitions during systems upgrades or mergers.

## 8.3 Innovation Facilitation and Economic Development

8.3.1 Innovation as Governance Duty

All public authorities must actively cultivate an environment where data-driven innovation can flourish serving as both incubators of digital entrepreneurship and stewards of responsible risk.

Data Processor Accountability in Innovation Facilitation and Economic Development

In recognition of the critical role that data processors play in Mozambique's digital transformation, this Policy mandates that all data processors whether public, parastatal, or contracted private entities are subject to specific duties supporting national innovation and growth objectives. These duties are anchored in the principle that processors are not merely service providers, but strategic partners responsible for the ethical, secure, and productive stewardship of public data resources.

1. Contractual and Regulatory Obligations

All agreements for data processing services entered into by public authorities must:

- Explicitly require processors to comply with the objectives of the National Data Governance Policy, including provisions related to open data, support for research and innovation, and adherence to sectoral data sharing standards.
- Oblige processors to implement systems and workflows that enable lawful data reuse, responsible data anonymization, and interoperability with national platforms, facilitating access for Mozambican innovators, startups, and researchers.
- Mandate regular reporting to the contracting authority and the NDGC on contributions toward policy objectives, such as metrics on data quality improvements, partnership support, or open API provisioning.

2. Participation and Collaboration

Processors contracted by government or public bodies must:

- Participate in NDGC- or Ministry-led innovation forums, hackathons, and regulatory sandboxes to share expertise, demonstrate tools, and/or pilot new technologies using data under their stewardship.
- Contribute to pilot projects and public-private partnership initiatives by providing technical know-how, anonymized datasets for responsible experimentation, and capacity-building sessions for local developers and researchers.

3. Incentives and Recognition

- Public tenders and renewal of processing contracts shall award additional scoring or renewal priority to processors who demonstrate sustained, auditable impact on innovation outcomes (e.g., enabling open data release, facilitating research, supporting digital start-ups, or transferring skills to local staff).
- The NDGC shall maintain a public registry of "innovation-compliant processors," granting official recognition and providing eligibility for participation in advanced projects or regulatory sandboxes.

4. Monitoring, Audit, and Accountability

- All processor activities related to supporting innovation must be documented and subject to annual NDGC audit. Compliance failure such as blocking access to reusable datasets, neglecting interoperability obligations, or failure to participate in mandated capacity-building shall constitute grounds for contract termination, sanctions, or ineligibility for future public sector contracts.
- The NDGC may publicly report on processor contributions, highlight best practices, and require remedial action plans for underperformance.

5. Alignment with Economic Development Goals
- Processors are directed to align data management practices with Mozambique's Digital Transformation and Economic Development strategies, including support for local digital industries, fair access, reduction of digital divides, and the responsible encouragement of "data entrepreneurship."

### 8.3.2 Catalytic Policies

- **Open Data and Reuse:**

In fulfilment of Mozambique's national commitment to digital transformation and economic modernization, the Data Governance Policy mandates a comprehensive framework of catalytic policies designed to harness the full societal, developmental, and commercial value of data. These policies are structured to create a dynamic, secure, and inclusive ecosystem for responsible innovation, while preserving public trust and fundamental rights.

1. Open Data and Facilitated Reuse

All government ministries, agencies, and parastatals are required to identify, prepare, and proactively release non-sensitive datasets for public access and legitimate reuse. The NDGC, in cooperation with sectoral regulators, shall publish a schedule and standards for open data release. Datasets selected for publication must be:

- Subject to rigorous pre-release review to ensure that personal, commercial, security, or otherwise sensitive information is fully protected consistent with relevant law and applicable sectoral laws.
- Formatted in standardized, machine-readable formats, with comprehensive metadata to maximize usability, discoverability, and interoperability for researchers, businesses, and the general public.
- Accompanied by clear licensing terms (preferably open and royalty-free), which outline permissible reuses and attribution requirements, consistent with international best practice (such as Creative Commons or equivalent Mozambican Open Data License).
- Maintained through a centralized digital portal administered by the NDGC, with periodic updates, feedback channels, and mechanisms for dataset users to request new releases or report quality issues.
- Supported by public awareness campaigns to educate stakeholders including civil society, entrepreneurs, and local communities about available datasets and opportunities for value creation, civic engagement, and problem-solving.

2. Structured Public-Private Partnerships

To encourage sustainable, inclusive innovation and maximize the impact of national data resources, the Policy establishes a preferential framework for structured, fair, and transparent public-private collaboration:

- The NDGC, in partnership with relevant ministries, shall issue annual calls for proposals inviting academia, startups, established technology firms, and civil society organizations to engage in projects that leverage public data for societal or economic benefit.
- Model agreements and procurement templates will be made available to ensure clarity on intellectual property, confidentiality, data protection, and revenue-sharing matters, as well as clear dispute-resolution mechanisms.
- Strategic initiatives such as regulatory sandboxes, sectoral hackathons, and collaborative pilot programs shall be coordinated under NDGC oversight, with evaluation criteria emphasizing public interest, capacity building, and measurable outcomes (e.g., improved government service delivery, increased employment, knowledge transfer).
- All partnership activities are subject to NDGC-led monitoring, periodic audit, and transparent public reporting of objectives, funding, performance, and results, in order to safeguard against undue influence, rent-seeking, or conflicts of interest.

3. Regulatory Experimentation and Innovation Sandboxes

Recognizing the accelerating pace of technological change and the importance of adaptive governance, the Policy provides for regulators to establish legally sanctioned frameworks for controlled experimentation:

- The NDGC, together with sector-specific regulators, may authorize regulatory sandboxes time-limited, closely supervised environments in which innovators can trial new data-driven technologies or business models (such as fintech, digital identity systems, IoT, or artificial intelligence) under temporarily relaxed regulatory constraints.
- Entry to the sandbox is conditional on submission and acceptance of detailed risk assessments, data protection measures, and consumer safeguards, with strong criteria for reversibility and safe early exit.
- Regulators will define success criteria and maximum durations for sandbox participation; participants must commit to continuous compliance monitoring and corrective action in case novel harms or privacy/security risks arise.
- At the conclusion of each sandbox or controlled trial, regulatory authorities shall publish evaluation reports detailing lessons learned, regulatory adjustments made, scalability assessments, and recommendations for wider implementation or withdrawal.
- Results of regulatory sandboxes are to be used systematically to inform ongoing upgrades to Mozambican data policy, sectoral law, and technical standards establishing a virtuous circle of policy learning and progressive legal adaptation.

8.3.3 Metrics and Accountability

Outcome metrics job creation, research outputs, startup success, productivity gains must be tracked, and periodic review of legal and infrastructural bottlenecks is mandatory, with findings reported to the NDGC and Parliament.

## 8.4 Inclusivity and Digital Equity Imperatives

8.4.1 Principle

Data governance policy is expressly mandated to advance social and geographical inclusion, ensuring all Mozambicans, regardless of gender, region, language, age, or ability, partake in and benefit from the nation's digital transformation.

8.4.2 Operational Mechanisms

- **Barrier Reduction:** All digital services and datasets under the Policy must be made accessible in multiple languages, and platforms must minimize technical barriers for rural and marginalized populations.
- **Equitable Data Collection:** Disaggregated data reflecting key social, economic, and demographic factors is required for policymaking, to actively identify and remediate inequality or exclusion.
- **Targeted Investment:** Additional resources must be directed to literacy, training, infrastructure, and connectivity in under-served regions or groups, with regular public reporting on inclusivity goals and progress.

8.4.3 Participatory Monitoring

Stakeholder and civil society oversight of digital equity is not optional: structured participation, impact assessment, and community feedback mechanisms must be embedded in all major digital or data initiatives, and findings must directly inform further investment or policy correction.

# Chapter 9: Data Lifecycle Governance Regime

## 9.1 Data Collection: Lawfulness, Purpose Limitation, and Minimization

### 9.1.1 Principle of Lawfulness

No data may be collected by any covered entity except where expressly permitted or required by law, regulation, or lawful contract subject always to constitutional scrutiny. All data collection activities must be:

- Predicated on a clear statutory or regulatory basis,
- Authorized by the data subject's explicit, informed, and freely given consent (where applicable), or
- Justified by a legitimate public interest or overriding legal obligation, demonstrably necessary and proportionate to its aims.

### 9.1.2 Purpose Limitation

Data may be collected solely for specified, explicit, and legitimate purposes, as declared at the point of collection or as prescribed by law. Use or further processing for secondary purposes is strictly prohibited, save where:

- The data subject provides explicit, advance consent,
- Necessary to protect a vital interest of the data subject or another person,
- Required for the performance of a legal duty or contract, or
- Mandated by a court order or statutory authority.

### 9.1.3 Data Minimization

All data collection shall be strictly limited to that which is objectively necessary for the declared or legally-authorized purpose. Indiscriminate or "bulk" data collection, untethered to necessity or proportionality, is expressly prohibited and subject to penalty.

## 9.2 Data Processing: Security, Integrity, and Authorized Use

### 9.2.1 Security Obligations

Covered entities must implement and document appropriate technical and organizational measures to secure data against unlawful access, loss, alteration, disclosure, or destruction. Minimum protections include:

- Encryption at rest and in transit for sensitive data,
- Role-based and audit-trailed access control systems,
- Continuous monitoring, incident detection, and response protocols,
- Periodic security and vulnerability assessments.

### 9.2.2 Data Integrity and Accuracy

All processed data must be maintained in an accurate, complete, and up-to-date state. Covered entities shall establish mechanisms for:

- Routine verification and correction,
- Permitting data subjects, upon adequate identification, to access, challenge, and correct inaccurate or obsolete records,
- Prompt[U8] notification to affected parties and regulators of discovered data integrity breaches.

9.2.3 Authorized Use and Accountability

- Data may only be used and processed by individuals or systems with formal, documented authorization commensurate with the data's classification level.
- Unauthorized processing or use constitutes a breach of statutory duty and attracts administrative, civil, and, where prescribed, criminal liability.
- All processing activities must be logged, with audit records retained as required by law for subsequent oversight and investigation.

## 9.3 Data Sharing: Interoperability Standards and Access Protocols

9.3.1 Lawful Disclosure and Access

- No sharing or disclosure of data shall occur except with a demonstrable lawful basis and in compliance with sectoral and cross-border provisions outlined in this Policy.
- All data sharing agreements, intra-governmental transfers, and public releases are subject to NDGC-approved protocols and must honour purpose limitation, minimization, and protection requirements.

9.3.2 Interoperability and Standards

- Data must be formatted, structured, and exchanged according to NDGC-specified national and international interoperability standards, ensuring semantic clarity, traceability, and integrity.
- All digital interfaces for sharing (APIs, file protocols) must implement authentication, access control, standardized logging, and, where appropriate, secure federated identity solutions.

9.3.3 Access Rights and Procedures

- Only duly-authorized public officials, data stewards, or vetted private/commercial entities may access, request, or process shared data, subject to audit and, where applicable, pre-established data access boards or independent review.
- Data access privileges must be regularly reviewed and promptly revoked upon the end of legitimate operational need.

9.4 Data Retention and Disposal: Legal Obligations and Procedures

9.4.1 Mandatory Retention Periods

- Covered entities must retain data only for the minimum period required by the explicit legal, regulatory, or contractual purpose for which it was collected/processed.
- All mandatory retention periods must be specified in internal policy or registry, with justifications publicly available and subject to challenge.

9.4.2 Secure Archival and Integrity Protection

- Archival of data must guarantee ongoing protection of confidentiality, integrity, and accessibility so long as retention is lawfully required. Use of obsolete or insecure storage media is prohibited.

9.4.3 Lawful and Irreversible Disposal

- Upon expiry of the lawful retention period, data must be securely and irretrievably destroyed or anonymized in compliance with NDGC-approved standards (including documentation of destruction/anonymization events).
- Data subject to legal dispute, audit, investigation, or subject access request must not be destroyed pending resolution.

9.4.4 Documentation and Auditability

All retention, archival, and disposal actions must be fully documented, systematized, and available for inspection by authorized regulators, auditors, and, where appropriate, affected data subjects.

# Chapter 10: Privacy and Security Architecture

## 10.1 Privacy by Design: Mandatory Implementation Standards

### 10.1.1 Principle and Mandate

All public and private bodies falling within the Policy's scope are legally obligated to implement "privacy by design and by default": privacy, data minimization, and protection measures must be proactively embedded into all systems, processes, services, and lifecycles, not retrofitted.

### 10.1.2 Mandatory Standards

- **Systemic Integration:** Privacy controls, such as consent management, purpose limitation, access control, and data minimization, must be integrated from the earliest stage of system or service development.
- **Transparency and User Agency:** Design must prioritize transparency users/data subjects must be informed of data flows, collection purposes, sharing, and retention in clear language at or before point of collection, with mechanisms for withdrawal of consent or objection as of right.
- **Technical Controls:** Pseudonymization, encryption, granular role-based access, and secure, documented interfaces are mandatory for any processing involving sensitive or personal data.
- **Documentation:** All privacy engineering choices and compliance steps must be comprehensively documented and auditable by the Data Protection Authority or NDGC.

### 10.1.3 Enforcement and Remedies

Failure to evidence privacy by design in system audits, during breach response, or in NDGC/ANPD review constitutes a strict liability violation subject to statutory and administrative penalties, including suspension or withdrawal of system authorization.

## 10.2 Cybersecurity Framework and National Security Interface

### 10.2.1 Baseline Obligations

- **National Cybersecurity Standards:** All data-bearing systems must comply with, at minimum, cybersecurity standards specified by the relevant national cybersecurity agency, the NDGC, and international norms (e.g., ISO 27001).
- **Continuous Monitoring:** Real-time monitoring, anomaly detection, and response protocols must be operational for all critical and sensitive data assets, with mandatory incident escalation procedures.
- **Personnel Vetting and Training:** All personnel with elevated privileges or system access must undergo regular security clearance, background checks (where justified by risk), and cybersecurity training.

### 10.2.2 Interface with National Security

- **Obligatory Reporting:** Immediate reporting of significant security incidents, attempted or actual compromise, or suspected state-level threat actors to the designated national security focal point.

- **Intelligence Partnership:** Where digital assets are likely to impact critical infrastructure, public safety, or national defence, the NDGC must maintain explicit and secured liaison with relevant security agencies, with clear demarcations on permissible surveillance and information sharing strictly limited to constitutional and statutory bounds.

10.2.3 Penalty Regimes
Negligence, under-protection, or unauthorized circumvention of national cybersecurity obligations will trigger sanctions ranging from remedial orders and mandatory system shutdowns to personal civil and criminal liability of culpable executives and officials.

## 10.3 Data Protection Impact Assessment Regime

10.3.1 Mandatory Assessment Triggers
- **Scope:** Prior to launching any new data processing operation, system, or project that may present a high risk to rights or freedoms of data subjects including automated profiling, large-scale data aggregation, cross-border flows, or deployment of emerging technology a formal Data Protection Impact Assessment (DPIA) is mandatory.
- **Content:** DPIAs must evaluate purpose, necessity, proportionality, risks, intended safeguards, impacts on vulnerable groups, and proposed mitigation strategies.

10.3.2 Procedural Duties
- **Submission and Review:** All DPIAs must be submitted to the NDGC or the Data Protection Authority for approval prior to commencement of processing.
- **Public Interest and Transparency:** For significant operations, NDGC or ANPD may require summary publication of key DPIA findings, subject only to overriding public or national security interests.

10.3.3 Ongoing Compliance and Re-Assessment
Material changes to systems or repeated incidents require re-assessment or urgent review, with immediate rectification where new risks or inadequacies are found.

## 10.4 Cross-Border Transfer Mechanisms and Adequacy Determinations

10.4.1 Baseline Prohibition Absent Adequacy or Safeguards
No covered entity may transfer personal or sensitive data outside Mozambique except where:
- The recipient jurisdiction is recognized by the NDGC (in consultation with the Data Protection Authority) as providing an adequate level of protection, and
- All contractual and technical safeguards are in place to ensure rights, redress, and effective remedies for Mozambican data subjects.

10.4.2 Alternative Transfer Mechanisms
Where adequacy is not established:

- Transfers require enforceable safeguards (e.g., legally binding instruments, standard contractual clauses, codes of conduct with binding commitments, or explicit, informed, and revocable consent of the data subject for specific transfers).
- Transfers demanded by compelling public interest must be specifically authorized by the NDGC, with published justification.

10.4.3 Regulatory Approval and Ongoing Monitoring

- All entities engaging in repeated or systemic cross-border transfers must maintain detailed logs, submit periodic transfer impact reports, and make records available for inspection by the NDGC or regulators at any time.
- Any actual or suspected breach during or after transfer must be reported immediately, with remedial action and notification to affected individuals as determined by law.

# Chapter 11: Monitoring and Compliance Architecture

## 11.1 Continuous Compliance Monitoring Systems

11.1.1 Mandatory Internal Controls

All covered entities must institute and maintain internal compliance programs, including:

- Automated and manual systems for continuous monitoring of all data processing, retention, sharing, and disposal within their operational domain.
- Real-time alerts for policy, legal, or technical non-compliance, with escalation procedures to responsible data officers and the NDGC or sectoral oversight bodies.
- Scheduled internal compliance checks, documented corrective action protocols, and risk reassessment following incidents or regulatory updates.

11.1.2 Supervisor Responsibility

Chief Data Officers are personally responsible for the institutional integrity of compliance systems at all times; wilful or reckless neglect is grounds for removal, sanction, or referral to prosecutorial authorities.

11.1.3 Third-Party and Partnership Oversight

Entities engaging in data sharing or outsourcing must ensure all counterparties adhere to identical compliance standards, verified through contracts, due diligence, and where appropriate on-site inspection or certification.

## 11.2 Audit Framework and Independent Oversight

11.2.1 NDGC/ANPD Compliance Audit Regime

- The NDGC (assisted by the Data Protection Authority) shall conduct both scheduled and random audits of all covered entities, with unfettered access to systems, documentation, and personnel required for verification.
- Special audits are mandated in the event of major incidents, repeated minor violations, or credible whistle-blower complaints.

11.2.2 Independence[U9] and Non-Interference

- Audit teams are institutionally insulated from the executive branch or audited entity, with legal protections against retaliation and reporting lines directly to the NDGC.
- All findings, save those classified on national security grounds, must be recorded, summarized, and after due process made available to the public.

11.2.3 Sectoral and External Audit

- For entities in regulated sectors (e.g., finance, health, energy), sectoral regulators may require additional independent audits aligned with NDGC requirements.
- The NDGC may commission or recognize international audits or peer reviews, especially for systems running transnational or cross-border data functions.

## 11.3 Performance Metrics and Governance Maturity Indicators

11.3.1 Metrics Obligations

All covered entities must regularly measure, document, and report on key indicators, including but not limited to:

- Data quality (accuracy, completeness, timeliness, integrity rates)
- Compliance incidents (number, severity, resolution timeframe)
- Data subject request response times and satisfaction
- Security incidents and breach handling effectiveness
- Audit findings and percentage of recommendations implemented
- Sector-specific innovation and inclusivity outcomes (where relevant)

11.3.2 Governance Maturity

- Entities and oversight bodies must assess their data governance maturity annually using NDGC-issued frameworks, which benchmark structural, operational, cultural, and outcome-based progress on a transparent scale.
- Maturity self-assessments are subject to NDGC audit and shall inform remediation plans and institutional improvement mandates.

## 11.4 Public Reporting and Transparency Obligations

11.4.1 Publication Requirements

- All compliance reports, executive audit summaries, and key performance indicators are published in a publicly accessible, digital, and searchable registry maintained by the NDGC.
- Reports must be issued in accessible language, with summaries in at least the two most widely spoken national languages.

11.4.2 Public Notification and Engagement

- The NDGC and covered entities must publish annual and extraordinary compliance notices, alerting the public to significant new risks, regulatory changes, or persistent deficiencies.

- Civil society and citizen feedback on reporting quality and substance must be solicited, documented, and used as part of the NDGC's continuous improvement process.

11.4.3 Priority of Transparency

- Absent a legally-demonstrable and NDGC-confirmed state security necessity, transparency is presumed; attempts to shield compliance or audit failures from legitimate public scrutiny are grounds for investigation and serious sanction.

# Chapter 12: Enforcement Powers and Sanctions Regime

## 12.1 Administrative Enforcement Powers and Procedures

12.1.1 Investigatory Authority

The NDGC, acting through its enforcement arm or designated sectoral regulator, is vested with full investigatory powers summoning documents, compelling testimony, conducting on-site inspections (announced or unannounced), and seizing evidence wherever there is reasonable suspicion or prima facie indication of a substantive violation.

12.1.2 Interim and Preventive Measures

Upon discovery of probable violations:

- The NDGC may issue immediate suspension orders, block ongoing data processing, freeze data flows, or require emergency security measures, pending full investigation.
- Mandatory reporting to the NDGC is required for entities upon recognizing material breaches, with non-compliance itself constituting a violation.

12.1.3 Adjudication and Due Process

- All enforcement actions must be communicated in writing, with clear factual basis and citation of the specific legal standard violated.
- Affected parties possess the right to timely notice, access to evidence, the opportunity to be heard, and effective internal review prior to final administrative sanction.
- Final determinations of the NDGC are binding and enforceable, subject only to statutory or constitutional judicial review.

## 12.2 Civil Sanctions and Monetary Penalties

12.2.1 Fine Determination and Ranges

- The NDGC may impose graded monetary penalties on any entity or responsible individual for violations of data governance requirements, proportionate to the gravity, recurrence, intent, economic advantage gained, and whether the subject took timely remedial action.
- Maximum statutory fines are adjusted for inflation and sectoral risk, with higher ceilings for egregious or systemic violations, cross-border infractions, or repeat offenders.
- Civil penalties are enforceable as debts due to the state and may be accompanied by public naming and shaming in the NDGC register.

12.2.2 Restitution and Damages

- The NDGC may direct wrongdoers to pay actual or statutory damages to data subjects or other affected parties where tangible harm or unlawful enrichment can be demonstrated.
- Orders of restitution are enforceable in the courts and subject to garnishment, lien, or asset freeze as warranted.

## 12.3 Criminal Referral Mechanisms and Prosecutorial Coordination

12.3.1 Referral Triggers

- Where facts indicate probable commission of an intentional or grossly negligent criminal act (e.g., knowing misuse or sale of data, obstruction of enforcement, destruction of evidence, or wilful sabotage of systems), the NDGC refers the matter for prosecutorial investigation.
- Coordination agreements ensure continuity between administrative, civil, and criminal investigations, with shared access to evidentiary records, custody protocols, and protection of chain-of-custody integrity.

12.3.2 Witness and Whistle-blower Protection

- Any individual providing material evidence to the NDGC or prosecutors in data-related matters is afforded all statutory whistle-blower and witness protections, including anonymity guarantees, non-retaliation, and, where necessary, safe-harbour protections from parallel civil liability.

12.3.3 Joint Operation Protocols

- The NDGC is authorized to join task forces with law enforcement, sectoral regulators, and security services for cases implicating organized cybercrime, national security, or international cooperation needs, in strict compliance with procedural and fundamental rights safeguards.

## 12.4 Remedial Orders and Compliance Mechanisms

12.4.1 Corrective and Structural Orders

- The NDGC may issue binding corrective measures, including, but not limited to: mandatory technical remediation, executive or staff training obligations, appointment of outside data protection monitors, termination of unlawful processing, data rectification, and deletion of unlawfully held data.
- Persistent non-compliance may trigger ongoing NDGC monitoring and incremental fines until compliance is verified.

12.4.2 Consent Decrees and Settlement Authority

- The NDGC may negotiate and enforce remedial consent decrees or undertakings, tailored to specific cases and including clear performance metrics, reporting duties, and stipulated penalties for breach of undertakings.

12.4.3 Publicity and Deterrence

- All final enforcement actions, monetary penalties, and remedial orders must be summarized in the public NDGC register, save where judicial order prohibits publication on exceptional grounds.
- The NDGC may issue public warnings naming entities or individuals as necessary to prevent ongoing or anticipated harm to the public or national interests.

# Chapter 13: Rights, Remedies, and Judicial Review

## 13.1 Individual Rights and Legal Standing

13.1.1 Enumerated Rights

Every data subject regardless of nationality, residency, or status whose data are processed, stored, or otherwise touched by activities under this Policy, is expressly vested with the following enforceable rights:

- **Right to Information and Access**: To be informed of, and gain access to, data held about them, including the logic of automated processing.
- **Right of Correction and Erasure**: To demand timely rectification, completion, or deletion of inaccurate, out-of-date, or unlawfully held data.
- **Right to Object and Restrict Processing**: To object, at any time, to processing for direct marketing, profiling, or any use incompatible with stated purposes or law.
- **Right to Data Portability**: Where legally relevant, to receive personal data in a structured, commonly used, and machine-readable format and to transmit those data to another controller without hindrance.
- **Right to Redress**: To lodge complaints with the NDGC or Data Protection Authority, obtain effective administrative or judicial remedies, and receive compensation for material or non-material damage suffered due to violations.

13.1.2 Legal Standing

Any individual, group, or legal person directly or indirectly affected by data governance practices or decisions including civil society and class action representatives possesses standing (locus standi) to seek remedies or challenge acts and omissions under this Policy.

## 13.2 Administrative Appeals and Review Procedures

13.2.1 Internal Review

- All covered entities must maintain a formal, accessible process for written complaints, requests, or objections, with prescribed timelines for resolution and reasoned decisions.
- Unresolved disputes are appealable to the relevant CDO or sectoral regulator, who must render a final administrative determination within 30 days, documented and furnished to the complainant.

13.2.2 NDGC and Data Protection Authority Review

- Appeals from adverse or unsatisfactory decisions by covered entities may be presented to the NDGC or Data Protection Authority, which exercise quasi-judicial review powers investigating facts, summoning evidence, and ordering remedial measures or interim relief.
- All NDGC (or DPA) decisions must be reasoned, subject to further judicial review, and, except where lawfully confidential, published in redacted form.

## 13.3 Judicial Review of Data Governance Decisions

13.3.1 Right of Appeal

- Any party aggrieved by NDGC, Data Protection Authority, or sectoral regulator decisions including failure to decide may apply for judicial review in the competent Mozambican court.

- Judicial review is available for both questions of law and fact, including legitimacy of sanctions, remedies, or policy compatibility.

13.3.2 Procedural Safeguards

- Applications for review are free from prohibitive fees or standing restrictions and may be submitted directly by individuals, organizations, or legal counsel.
- Courts must provide for expedited procedures where fundamental rights, irreparable harm, or urgent public interest is demonstrated.

13.3.3 Remedies on Judicial Review

Upon finding for the applicant, courts are empowered to:

- Annul, set aside, or modify any challenged decision, sanction, or order;
- Mandate specific action, including reconsideration, data correction, or systemic remedial measures;
- Award costs, damages, or compensation as appropriate;
- Refer constitutional questions to the Constitutional Council as required.

## 13.4 Constitutional Challenges and Supremacy Clause Application

13.4.1 Constitutional Questions

Where a party asserts that any policy, regulation, enforcement action, or omission violates, or is inconsistent with, the Constitution especially Articles 71 (Privacy & Data Protection), 35 (Access to Information), or 11 (Sovereignty) the matter may be referred to the Constitutional Council for authoritative interpretation and binding resolution.

13.4.2 Supremacy Clause

- The Constitution of Mozambique is the supreme law; any statute, regulation, or administrative act or omission inconsistent with it is null and void to the extent of the inconsistency.
- All courts and authorities must interpret and apply this Policy, and any other data-related instruments, in a manner consistent with constitutional rights and values.
- Where an apparent conflict arises, the rights, principles, and protections expressed or implied by the Constitution prevail.

13.4.3 Interim Relief and Safeguards

Pending final adjudication of constitutional challenge, courts are empowered to grant interim or conservatory relief as necessary to prevent irreparable harm to the applicant or to vindicate public interest.

## Chapter 14: Amendment, Review, and Constitutional Evolution

### 14.1 Amendment Procedures and Constitutional Requirements

16.1.1 Formal Amendment Pathways

- Amendments to this Policy may only be initiated by:
    - Resolution of the NDGC, supported by a two-thirds majority;
    - Legislative proposal enacted by the National Assembly under standard statutory process;
    - Executive proposal, subject to NDGC prior consultation and parliamentary approval.

14.1.2 Due Process and Constitutional Safeguards

- All amendment proposals shall be published for public comment, with a minimum 60-day consultation period and comprehensive NDGC assessment prior to adoption.
- Amendments must preserve consistency with the Constitution especially Articles 71, 35, and 11 and are subject to constitutional review by courts or the Constitutional Council prior to coming into legal force.
- Any amendment materially limiting fundamental rights or shifting legal duties shall require express justification under the necessary and proportionate test, including comparative international analysis.

14.1.3 Emergency Amendments

- In cases of urgent public interest, national security, or critical technological disruption, NDGC may recommend provisional amendments to the Executive, valid for up to 120 days, with immediate referral to the Parliament for permanent disposition.

### 14.2 Periodic Review Mandates and Evaluation Criteria

14.2.1 Directive Review Cycle

- The NDGC shall conduct a comprehensive review of this Policy and its implementation every three years, with mandatory interim assessment at one-year intervals in the first five years of operation.
- Review must include audit of effectiveness, compliance statistics, sectoral impacts, equity and inclusion, emerging risks, and international best practice alignment.

14.2.2 Evaluation Criteria

- Criteria for review include: legal compliance, constitutional compatibility, user and stakeholder satisfaction, efficiency of operational mechanisms, readiness for technological changes, and alignment with regional and global frameworks and treaties.

14.2.3 Adaptive Recommendations

- Review outcomes must be published, with detailed recommendations for amendment, extension, or repeal, feeding directly into NDGC, executive, and parliamentary processes for formal update or revision.

### 14.3 Technological Adaptation and Future-Proofing Mechanisms

14.3.1 Innovation Mandates

- NDGC is required to establish a standing Technology and Law Review Committee, tasked with tracking, evaluating, and recommending policy, procedural, or legal

adaptation to new technologies (AI, quantum computing, cloud infrastructures, IoT, blockchain, etc.).

- Targeted "regulatory sandboxes" and pilot studies for emerging data technologies shall be authorized, with open reporting and mandatory integration of lessons learned into formal policy review.

14.3.2 Rapid Response Options

- NDGC may issue temporary technical directives or waivers to address unforeseen technological risks or opportunities, subject to public notification and subsequent parliamentary ratification within 12 months.

## 14.4 Integration with Emerging Legal Frameworks

14.4.1 Harmonization and International Linkages

- The Policy shall be systematically harmonized with newly adopted regional (AU, SADC), continental, and global statutes, conventions, protocols, and standards.
- NDGC must maintain an "Emerging Legal Frameworks Register," tracking new instruments and their impact, with annual reporting to Parliament and public.

14.4.2 Policy Supremacy and Reconciliation

- In case of conflict or divergence between this Policy and newly ratified legal frameworks, constitutional supremacy applies subject to NDGC/Parliament determination and, if necessary, referral for constitutional interpretation.

14.4.3 Opt-In and Opt-Out Protocols

- Where emerging frameworks offer options or protocols for member states, Mozambique's NDGC shall conduct risk-benefit assessments and public engagement before opting in or out, documenting all decisions and legal impacts.

Chapter 15: Legal Integration and Hierarchical Positioning

## 15.1 Relationship to Constitutional Law and Fundamental Rights

15.1.1 Constitutional Primacy

- This Policy is expressly subordinate to the Constitution of Mozambique and shall be interpreted, applied, and enforced consistently with constitutional rights including, but not limited to, the rights to privacy, honour, information access, equality, due process, and sovereignty (Articles 71, 35, 11, and others).
- Where any provision of this Policy or implementing regulation is found by competent judicial authority to conflict with constitutional principles, the Constitution prevails; such provisions are void to the extent of inconsistency.

15.1.2 Safeguarding Fundamental Rights

- All Policy duties, powers, and obligations are subject to the "necessary and proportionate" test as required by constitutional jurisprudence.
- Covered entities, regulators, and the NDGC are required to ensure ongoing compatibility through regular review, compliance mapping, and explicit rights-based justifications for all substantive rulemaking.

## 15.2 Integration with Administrative Law and Procedure

15.2.1 Administrative Law Alignment

- The Policy and all NDGC, sectoral regulator, and entity decisions and processes are subject to Mozambique's general administrative law, including rules of evidence, public comment, transparency, official notification, and appeals.
- Administrative acts taken under this Policy must be reasoned, documented, and open to internal and judicial review.

15.2.2 Procedural Directives

- All processes affecting rights, obligations, or sanctions shall comply with rules of fairness, neutrality, and efficiency, as codified in Mozambique's administrative code and sectoral regulations.

15.2.3 Recordkeeping and Archival Requirements

- Entities must maintain full procedural records for all substantive decisions, subject to administrative inspection, audit, and public access save for cases of legally justified confidentiality.

## 15.3 International Law Integration and Treaty Compliance

15.3.1 Treaty Incorporation and Effect

- This Policy is interpreted and enforced in light of Mozambique's commitments under ratified international treaties and instruments, including the African Union Data Policy Framework, Malabo Convention, ICCPR, and relevant UN standards.
- Where international obligations confer higher standards of protection, these are incorporated by reference and supersede domestic Policy provisions absent express reservation.

15.3.2 Harmonization and Mutual Recognition

- NDGC and sectoral entities are mandated to harmonize frameworks, rules, and procedures with regional and international best practices, ensuring compatibility for cross-border data flows, cooperation, and dispute resolution.
- Where conflicting obligations arise, NDGC must initiate formal reconciliation and, if necessary, refer for constitutional interpretation.

## 15.4 Conflict of Laws and Supremacy Provisions

15.4.1 Conflict of Law Resolution

- In cases of conflict between this Policy and other national statutes, administrative regulations, or sectoral rules, the following hierarchy prevails:
    1. Constitution of Mozambique;
    2. Ratified International Treaties with direct effect;
    3. This Policy and implementing regulations;
    4. Sectoral or agency-specific orders, subject to NDGC certification.

## 15.4.2 Supremacy Clause Application

- Actions and decisions taken under subordinate statutes, rules, or executive orders are lawful only to the extent they do not derogate from rights, principles, and standards established by this Policy as interpreted in harmony with superior laws.
- Competent courts, including the Constitutional Council, are empowered to annul, amend, or reconcile conflicting rules, with NDGC required to update the Policy and its registry in response.

### 15.4.3 Residual and Catch-All Safeguards

- Any ambiguity, lacuna, or unaddressed conflict is to be resolved in favour of fundamental rights, constitutional interpretation, and the public interest.
- NDGC, Data Protection Authority, and relevant courts are directed to issue interpretive guidance and formal legal opinions where uncertainty persists.

# PART 2

# Implementation Strategy

# Chapter 16: Implementation Roadmap and Strategy

## 16.1 Phased Implementation Schedule and Milestones

### 16.1.1 Directive Launch Sequence

Upon ratification of the Data Governance Policy, the Ministry in collaboration with the National Data Governance Council (NDGC) shall, within thirty (30) days, publicly issue an Implementation Directive. This directive will set forth a sequenced schedule of milestones, specifying responsibilities, outputs, and review dates for policy rollout across all relevant entities.

The phased approach shall consist of no fewer than five (5) definitive stages:

- Institutional Setup and Coordination: Establishment of governance bodies, assignment of Chief Data Officers, and formalization of sectoral coordination frameworks.
- Foundational Training and Capacity Initiation: Immediate commencement of standardized training programs for data governance professionals, accompanied by institution-wide awareness campaigns and skills audits.
- Early-Pilot and High-Priority Sectors Go-Live: Rapid deployment of data governance protocols in priority sectors, launching initial pilots to test processes, technologies, and compliance mechanisms.
- Full Multi-Sector Operationalization: Broad implementation of standards, compliance measures, system upgrades, and interoperability platforms throughout government, parastatals, and covered partners.
- Continuous Review and Iterative Enhancement: Scheduled evaluations using documented performance metrics, stakeholder consultations, and lessons-learned feedback to refine policies, correct deficiencies, and escalate best practices.

Each implementation phase shall include detailed deliverables (e.g., sectoral standards, compliance diagnostics, interoperable system deployment), clearly identified responsible bodies, stakeholder engagement requirements, and a set of measurable outputs such as real-time compliance rates and audit outcomes.

### 16.1.2 Adaptive Milestone Options

Recognizing diversity in readiness and resource allocation, this Strategy authorizes all entities to submit requests for milestone acceleration, phased sectoral delays, or partial go-live scenarios subject to rigorous NDGC review and approval. Entities must demonstrate objective justification, including risk analyses and capacity assessments, for any deviation from the standard sequence.

In circumstances involving rapid technological innovation, unforeseen emergencies (such as public health crises or cybersecurity incidents), or special NDGC-determined circumstances, milestones may be expedited in line with a pre-approved NDGC emergency protocol. The

NDGC will maintain public records of all deviation requests and resolution outcomes to ensure transparency and ongoing accountability.

- Entities may propose phased acceleration, delayed sectors, or partial go-live in cases of proven readiness, risk, or resource constraint subject to NDGC approval.
- Rapid innovations or emergency action (e.g., pandemic or cyber incident) may trigger expedited milestones under NDGC emergency protocols.

### 16.2 Institutional Capacity Development Programs

#### 16.2.1 Directive Training Requirements

All covered entities are required within sixty (60) days of Policy commencement to submit a comprehensive training program proposal for their data governance personnel. This includes Chief Data Officers (CDOs), sector data stewards, IT and legal staff, and leadership. Training must encompass legal, technical, operational, and ethical competencies.

The NDGC shall coordinate development and national deployment of certifiable curricula, blending theoretical and functional modules. Certification will be required for initial assignment, with regular interval recertification and documented participation in ongoing education.

#### 16.2.2 Modular Capacity Options

To ensure inclusivity and accessibility, entities are permitted to partner with accredited universities, professional institutes, and certified private trainers, so long as programs meet or exceed NDGC's national standards. Training delivery may utilize in-person, remote, blended, or mobile platforms according to organizational and geographic context.

The NDGC will provide guidance and support for skill assessment and competency tracking, emphasizing gender parity, rural outreach, and inclusivity modules as mandatory components for national equity in digital literacy and data stewardship. Entities may partner with accredited academic institutions, professional bodies, and regulated private trainers, provided programs meet minimum NDGC curricula requirements.

### 16.3 Financial Resources and Budgetary Allocation

#### 16.3.1 Mandated Funding Directions

The Ministry of Finance, working jointly with NDGC, shall allocate dedicated, protected budget lines for the Data Governance Policy's implementation. This encompasses staffing, technology investment, training, regulatory activities, and public awareness initiatives. Annual funding thresholds for mission-critical infrastructure, pilot projects, and investments in marginalized or rural communities must be published and tracked, with NDGC scrutinizing for sufficiency and transparency.

#### 16.3.2 Flexibility and Supplementary Options

Entities are encouraged to pursue additional resource mobilization, including but not limited to: donor grants, international programs, and public-private partnerships. All supplemental

funding must be managed and reported in line with NDGC's financial transparency and sovereignty safeguarding guidelines.

Requests for budget reallocation between phases or sectors will be considered on submission of a risk and efficacy analysis, with NDGC approval contingent on assurance of continued compliance and organizational resilience.

## 16.4 International Cooperation and Technical Assistance

16.4.1 Directive Engagement Protocols

The NDGC and the Government are mandated to actively pursue bilateral, regional, and multilateral cooperation with recognized international partners. Such engagement is intended to promote the adoption of global best practices, technical upgrades, and sustainable capacity development.

- Priority domains for technical collaboration include:
- Cybersecurity program strengthening,
- Interoperability and standards harmonization,
- Regulatory sandboxes for innovation pilots,
- Promoting digital inclusion,
- Open data initiatives and platforms.

16.4.2 Assistance Options and Safeguards

Permissible forms of assistance comprise staff exchanges, joint pilot deployments, technology transfer, targeted expert missions, and technical clinics. All such arrangements must be pre-cleared by the NDGC whenever they impact Mozambican legal, ethical, or data security infrastructure.

Mozambique is authorized and encouraged to participate in leading continental and global data governance for a including AU, SADC, UN, and EOSC to leverage regional integration and secure donor opportunities. All international technical engagements must be documented, evaluated for legal compliance, and reported in the NDGC's annual review.

## Chapter 17: Transitional Provisions and Temporal Application

## 17.1 Pre-Existing Data: Legal Audit and Compliance Directive

17.1.1 Mandatory Audit of Legacy Data

All data in the possession, custody, or control of any covered entity, where such data have been collected, held, processed, or stored prior to the effective date of this Policy ("pre-existing data"), shall be subject to a compulsory compliance audit to ensure conformity with prevailing legal standards. The audit must be completed within ninety (90) days from the date this Policy enters into force.

Entities must identify, catalog, and assess pre-existing data for lawful basis, relevance to current purposes, and conformity to new protection standards.

17.1.2 Assessment, Cataloguing, and Legal Basis Determination

Each entity is required to:

- Identify and systematically catalogue all pre-existing data assets and repositories, whether physical or digital, relevant to its organizational mandate.
- Assess each category or set of pre-existing data against statutory requirements relating to lawfulness of collection, adequacy and relevance to current processing purposes, necessity, and conformity with established data protection, privacy, and security obligations.
- Data which was lawfully collected and processed under prior regimes may continue to be used, provided usage remains compatible with original purposes, no new risks are introduced, and corrective measures (such as enhanced access controls or consent renewals) are completed within six months.
- For data whose continued use would violate fundamental rights or new statutory requirements, entities must either regularize (e.g., re-consent, minimize, anonymize) or securely dispose of such data, subject to NDGC or Data Protection Authority approval.

17.1.3 Rectification and Remediation Protocols

If, on audit, pre-existing data are found:

- To have been collected, retained, or processed without legal basis, lacking consent, or being incompatible with the purposes permitted under this Policy, the entity must, within sixty (60) days of audit completion, effect corrective remediation. Remedial action may include secure erasure, anonymization, explicit consent renewal, or adjustment of processing purposes to conform to the requirements of this Policy.
- To comply substantially with the Policy but require technical compliance (e.g., updating security controls, metadata standards, or access protocols), all necessary adjustments must be completed and documented within the implementation timeframe specified by the NDGC.

17.1.4 Reporting and Oversight Requirements

Entities shall submit to the NDGC a written report certifying completion of the legacy data audit, summarizing findings, and listing all remedial actions executed. Reports must be

subject to inspection, and entities remain subject to random or targeted NDGC review and enforcement measures.

17.1.5 Continuing Obligations

No provision of this Policy shall be construed as permitting the continued processing, retention, or use of pre-existing data in violation of current legal standards. All covered entities are under a positive legal obligation to ensure ongoing alignment of legacy data with the requirements and protections established herein.

## 17.2 Legacy System Migration and Compatibility Requirements

17.2.1 Technical Migration Schedule

All covered entities shall, within ninety (90) days of the commencement of this Policy, prepare, document, and submit to the NDGC a comprehensive migration plan addressing all information technology systems, system architectures, and electronic databases which were operational prior to the entry into force of this Policy ("legacy systems").

The migration plan shall, at a minimum, identify each relevant legacy system, assess its present state of compliance with the interoperability, data security, and privacy requirements set forth in this Policy, and set forth a detailed timetable for phased upgrades or replacement. Such upgrades must be sequenced so as to maximize continuity of public service and minimize risks to data integrity or protection.

Legacy systems identified by the entity or NDGC as critical or presenting a high risk either by volume or sensitivity of the data processed, or the importance of the supported function shall be migrated, upgraded, or otherwise brought into full compliance with this Policy on an expedited basis. The migration of such critical systems shall be completed no later than one hundred eighty (180) days from the date of Policy commencement, unless the NDGC, upon formal request, grants a temporary extension. Any request for extension must be justified by demonstrable operational or financial constraints and shall be subject to oversight by a third-party auditor approved by the NDGC.

17.2.2 Compatibility Options

In situations where immediate, full migration of legacy systems is not technically or economically feasible, entities are authorized, under NDGC supervision, to implement temporary compatibility measures. These measures may include, but are not limited to, secure application programming interfaces (API bridges), data quarantining protocols, or the maintenance of parallel systems for clearly defined, transitional periods.

All such arrangements must be:

- Documented with a formal justification and approved by the NDGC,
- Structured to ensure that no core requirements for data protection, system security, or auditability are circumvented or compromised during the period of temporary operation, and

Clear and time-bound end dates and measurable milestones for full migration or decommissioning.

Any procurement or deployment of new or replacement systems to support migration efforts must receive prior certification by the NDGC to confirm compliance with all applicable technical, privacy, and interoperability standards mandated under this Policy. No new system shall be launched into live operation until such certification has been formally issued, and ongoing compliance shall remain subject to NDGC review and audit.

All steps in the migration and compatibility process must be documented, and periodic progress reports must be submitted to the NDGC until the legacy system is fully compliant or has been decommissioned, ensuring continuous oversight and legal accountability throughout the transition period. Where full migration is not immediately feasible, entities may implement API bridges, data quarantining, or temporary parallel systems, provided such arrangements are time-bound, documented, and do not compromise core privacy, security, or auditability standards.

Procurement of new systems must be NDGC-certified for compliance before deployment.

## 17.3 Interim Governance Arrangements

17.3.1 Transitional Bodies and Delegated Powers

During the period between the commencement of this Policy and the full operationalization of the National Data Governance Council (NDGC), the Ministry designated under this Policy, or a formally appointed Task Force, shall exercise interim authority over data governance and enforcement. The interim body shall be vested with all powers necessary to ensure continuity of governance, compliance oversight, and regulatory enforcement as provided by law.

The interim body must operate strictly subject to transparent oversight and shall submit regular written reports to all relevant government stakeholders, documenting decisions, compliance actions, incidents, and measures adopted during the transition period. Existing authorities responsible for data protection, audit, and incident response functions may continue to act under standing orders issued prior to this Policy, provided all such actions are rigorously documented and the transition of responsibility is clearly managed.

Upon establishment of NDGC structures, all records, decisions, and activities of transitional bodies must be transferred for comprehensive review. The NDGC shall have the authority to audit, confirm, amend, or revoke any interim measures taken, ensuring legal continuity and full accountability.

17.3.2 Rapid Response and Conflict Resolution

Where urgent or unforeseen governance gaps emerge during the transition for instance, major data breaches, high-profile compliance disputes, or cross-sectoral coordination failures the interim body is authorized to issue interim orders, directives, or corrective actions necessary to safeguard legal rights, public interest, and data protections.

Any interested party affected by such interim measures retains the right of appeal or review once the NDGC becomes fully operational. All appeals or requests for formal reconsideration shall be administered in accordance with standard NDGC procedures and timelines.

All transitional governance arrangements authorized by this section shall expire automatically or be subject to NDGC ratification within a period not exceeding twelve (12) months from the effective date of this Policy. Upon expiration or ratification, sole and exclusive authority for all governance, enforcement, and adjudication functions shall vest in the NDGC and its designated structures, with immediate termination of all interim powers.

## 17.4 Sunset Clauses and Review Triggers

17.4.1 Sunset of Transitional Measures

All transitional measures established under this Policy including, but not limited to, legacy data provisions, migration exceptions, and interim governance authorities shall be strictly time-limited. Each such measure shall automatically expire on the pre-set date specified within the relevant section of this Policy or, where not otherwise specified, no later than twelve (12) months following the effective date of the Policy.

Extensions to any transitional provisions shall be permissible only upon the passage of a formal resolution by the NDGC, based on a clearly documented and published justification. Any such extension must be limited in duration, justified by compelling operational, technical, or legal necessity, and subject to ongoing oversight. The NDGC shall ensure that, not less than sixty (60) days prior to the scheduled expiration of any transitional measure, public notice is given regarding any proposed extension or substantive modification. This notice period must include an opportunity for public comment, with all submissions reviewed and summarized as part of the record prior to a final decision.

Upon expiration of transitional measures, the rights, obligations, and governance authorities established by permanent provisions of this Policy shall operate without exception or derogation, and all affected entities must achieve full compliance with the current standards and governance framework.

17.4.2 Review Triggers and Adaptive Flexibility

The NDGC is under a mandatory obligation to conduct a comprehensive review of all transitional arrangements, data migration progress, and associated compliance outcomes no later than one (1) year following the effective date of this Policy, and annually thereafter until sectoral and systemic compliance is fully certified.

Such review shall assess the effectiveness, efficiency, risks, and continued necessity of all outstanding transitional measures. The NDGC must publish the results of each review, together with recommendations for amendment or repeal of transitional provisions, and a timetable for achieving final compliance.

Any significant legal, technological, or security development arising during the transition such as major legislative reforms, introduction of disruptive technologies, or systemic breaches shall automatically trigger a special review by the NDGC. Where such a review finds that current transitional provisions are inadequate or inappropriate under the new circumstances, the NDGC is empowered and required to recommend amendments, accelerate or curtail sunset dates, or otherwise adjust the transition framework in the public interest and in line with constitutional requirements.

# Chapter 18: Commencement and Legal Effect

## 18.1 Commencement Dates and Effective Periods

18.1.1 Directive for Entry into Force

The provisions of this Policy shall come into legal force and effect either (a) on the effective date specified in the enabling Presidential Decree or Parliamentary Act, or (b) if not otherwise designated, no later than sixty (60) days following the date of formal adoption and publication in the Official Gazette of Mozambique (Boletim da República).

Where this Policy establishes distinct commencement or implementation timelines for different sectors, chapters, or obligations, the NDGC shall, within fifteen (15) days of enactment, issue and publish a comprehensive schedule specifying the phased commencement dates, the scope of each phase, and the entities to which those dates apply.

18.1.2 Duration and Continuity

This Policy, and all legal obligations and rights established herein, shall remain in continuous legal effect unless and until formally amended, repealed, or superseded by lawful authority. Any express sunset clause, expiry date, or review-triggered modification identified within this or any transitional chapter of the Policy must be strictly observed and publicly announced with a minimum of thirty (30) days' notice prior to the cessation or amendment of any affected provision.

## 18.2 Legal Publication and Official Gazette Requirements

18.2.1 Mandatory Publication

The full and original text of this Policy as well as all subsequent substantive amendments, revisions, or abrogation must be duly published in the Official Gazette prior to gaining legal effect. Only upon such publication shall the Policy, or any change to it, be deemed enforceable by the NDGC or any covered entity. The NDGC shall further ensure timely and supplementary publication of the Policy, its amendments, and commencement schedules in accessible digital formats, with direct notification to all government departments, parastatals, third-party partners, and registered stakeholders.

18.2.2 Notice and Awareness Measures

The NDGC, jointly with responsible ministries, shall implement public education and notification campaigns to ensure that all government bodies, stakeholders, and the general public are adequately informed of new obligations, effective dates, compliance requirements, and available legal remedies under this Policy.

## 18.3 Binding Effect and Legal Hierarchy

18.3.1 Universal Applicability

This Policy is legally binding on all government departments, agencies, parastatals, and third-parties falling within its defined scope, without exception, save where a constitutional or statutory exemption is unequivocally established. No contract, agreement, regulation, or subordinate policy may diminish, derogate from, or nullify any right, duty, or obligation set forth in this Policy.

18.3.2 Hierarchical Enforcement

It is the duty of all enforcement authorities including the NDGC, courts, and sectoral regulators to apply this Policy with priority in cases of ambiguity, overlap, or conflict among governing instruments, subject always to constitutional supremacy.

## 18.4 Severability and Savings Provisions

18.4.1 Severability Clause

If any section, clause, or provision of this Policy is declared unconstitutional, invalid, or otherwise unenforceable by final judgment of a court of competent jurisdiction, such judgment shall not affect the validity, enforceability, or continued effect of the remaining provisions. The NDGC shall be required to promptly prepare and submit corrective amendments, subject to constitutional review and public participation in accordance with established review procedures.

18.4.2 Savings of Prior Law and Acts

All acts lawfully done, rights accrued, obligations incurred, and legal proceedings commenced under pre-existing regimes prior to the effective date of this Policy shall remain valid and enforceable, subject to the provisions on transitional arrangements. Existing subordinate regulations, directives, or administrative instructions not inconsistent with this Policy shall be preserved and continue to have effect until duly replaced or repealed in accordance with relevant legislative or regulatory processes.

# Annexes

## Annex A: Glossary of Key Data Governance Terms

**Access Right:** The legally vested right of a data subject to obtain, from the controller, confirmation as to whether or not personal data concerning him or her are being processed, and, if so, to access the data and receive associated information as prescribed by law.

**Adequacy (Data Transfer):** The formal determination by a competent Mozambican authority (NDGC or Data Protection Authority) that a foreign country, territory, or specific international organization offers a level of personal data protection essentially equivalent to the standards and safeguards required under Mozambican law. Required prerequisite for lawful cross-border transfer of personal or sensitive data, as per relevant law in force in the Republic of Mozambique.

**Anonymization:** The process of irreversibly altering personal data so that an individual can no longer be identified directly or indirectly, by any means reasonably likely to be used, by either the controller or any other person. Anonymized data are excluded from the definition of personal data under Mozambican law (unless re-identification is possible).

**Biometric Data:** Personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a person, which allow or confirm the unique identification of that individual (e.g., fingerprints, facial images, iris scans).

**Chief Data Officer (CDO):** The designated senior official, appointed within a Mozambican state organ, agency, or parastatal, who is responsible for strategic leadership, oversight, and institutional compliance with national data governance frameworks.

**Consent:** Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which the data subject, through a statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her. For minors or legally incapacitated individuals, consent must be provided by a legal guardian, subject to additional requirements.

**Controller (Data Controller):** Any natural or legal person, public institution, agency, or other body which, alone or jointly with others, determines the purposes and means of processing personal data. Under Mozambican law, all public bodies and service providers collecting or using personal data in Mozambique are subject to the obligations of a controller.

**Cross-Border Data Transfer:** Any movement of personal data outside the territory of Mozambique, through electronic or physical means, including transfers to cloud services, foreign governments, international organizations, or multinational companies.

**Data Breach (Personal Data Breach):** Any incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Immediate notification to the Data Protection Authority and affected subjects is mandatory in cases of material risk.

**Data Classification:** The legal and operational assignment of data into defined categories such as public, restricted, confidential, or secret/classified based on legal sensitivity, potential impact, sectoral requirements (health, finance, national security, etc.), and applicable Mozambican or international law.

**Data Governance:** The comprehensive set of policies, processes, standards, and organizational structures establishing how data are managed, protected, shared, and utilized as a strategic asset across all sectors of Mozambique. The National Data Governance Council (NDGC) is the apex oversight body for such frameworks.

**Data Lake / Repository:** Centralized or federated digital storage solution where large volumes and diverse types of data (structured, semi-structured, unstructured) are securely held and made available for authorized analytics, exchange, and operational use.

**Data Minimization:** The obligation that collected and processed data shall be adequate, relevant, and limited to what is strictly necessary for the purposes for which they are processed.

**Data Portability:** The right of a data subject to receive personal data concerning him/her, which he/she has provided to a controller, in a structured, commonly used, and machine-readable format, and to transmit those data to another controller without hindrance.

**Data Processor:** Any natural or legal person, public authority, or body that processes personal data on behalf of the controller, under a contract or other legal act. Processors are subject to direct legal liability for breaches of Mozambican legal requirements.

**Data Protection Impact Assessment (DPIA):** A formal process by which a controller or processor evaluates the likely impact of a proposed data processing operation especially those presenting high risks to individuals' rights and freedoms including risks to data privacy and security, and outlines mitigation steps. Mandatory for large-scale or sensitive data initiatives.

**Data Steward:** A designated specialist tasked with day-to-day management, protection, and quality assurance of data assets, ensuring compliance with Mozambican policy, sectoral standards, and best practice.

**Data Subject:** Any identified or identifiable natural person whose personal data are processed, collected, or held by a controller or processor within or on behalf of Mozambican institutions.

**De-identification:** The process of removing or obfuscating personal identifiers from data to reduce risk of identification, but unlike anonymization, may still allow linkage or re-identification under certain conditions.

**Interoperability:** The technical, semantic, organizational, and legal ability of diverse information systems, agencies, and sectors to securely exchange, interpret, and reuse data,

in accordance with Mozambican and applicable international standards. Critical for integration of national e-government, health, education, and financial data systems.

**Metadata:** Structured information describing the characteristics, contents, origin, and management of a dataset, facilitating search, classification, and auditability.

**Open Data:** Data proactively released by Mozambican public authorities for free public use, reuse, and redistribution, typically under a standardized open license, with due regard for privacy, commercial, and security exceptions.

**Personal Data:** Any information relating to an identified or identifiable natural person including names, identification numbers, location data, online identifiers, and one or more factors specific to the individual's physical, physiological, mental, economic, cultural, or social identity as defined by relevant data protection law in force in the Republic of Mozambique.

**Privacy by Design / Privacy by Default:** The principle that privacy protections must be integrated from the earliest stages of system design and organizational process creation, and default settings should ensure maximal privacy protection without the need for user action.

**Processor (Data Processor):** See above. May include IT vendors, cloud service providers, analytics firms, and outsourced managed service providers operating under Mozambican or bilateral law.

**Profiling:** Any automated processing of personal data intended to evaluate, analyse, or predict aspects concerning a person's performance, interests, behaviour, health, or movements. Profiling is subject to heightened scrutiny and, in most cases, opt-out and impact assessment mechanisms.

**Pseudonymization:** The processing of personal data so that the data can no longer be attributed to a specific data subject without separate supplementary information, provided that such information is kept separately and subject to technical and organizational measures.

**Public Data:** Data sets released by, or available from, Mozambican government institutions without restriction for access or use, typically not containing any confidential, personal, or sensitive information.

**Regulatory Sandbox:** A controlled environment established by Mozambican authorities to allow innovative digital or data-driven initiatives such as fintech, e-government pilots, or AI applications to be tested under regulatory supervision before full-scale rollout.

**Retention Period:** The legally or contractually mandated period for which data must be stored, after which erasure, anonymization, or reduced accessibility is required.

**Sensitive Data (Special Categories):** Personal data that, due to its nature or statutory definition, is subject to heightened legal protection (e.g., data revealing racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, genetic or biometric data, health status, or sex life).

**Supervisory Authority (Data Protection Authority):** The independent national authority designated under the law, responsible for overseeing, enforcing, and advising on all matters relating to data protection and privacy compliance in Mozambique.

## Annex B: Register of Laws, Standards, and Frameworks

**1. National Statutes and Principal Legal Instruments:**
Constitution of the Republic of Mozambique (2004, as amended)
The supreme law establishing fundamental rights including the right to privacy (Article 71), access to information (Article 35), and national sovereignty (Article 11) and the framework for administrative, judicial, and legislative powers.

**Law No. 3/2017: Electronic Transactions Law:**
Legal basis for digital and electronic transactions (including e-commerce), recognition of electronic signatures, digital authentication, and obligations around the security of electronic communications and e-government services.

**2. Regional and International Treaties and Protocols**
**African Union Data Policy Framework (2022):** Sets continental standards for data protection, free data flow with trust, cross-border interoperability, and harmonization of regulatory approaches among AU member states.

**African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, 2014):** Ratified by Mozambique; legally binding for cybersecurity, personal data protection, cybercrime, and cross-border data regulation within the African context.

**SADC Model Law on Data Protection (2013, for reference):** Southern African guideline baseline for harmonizing member states' laws on data privacy, rights, data protection authorities, and cross-border transfers.

**International Covenant on Civil and Political Rights (ICCPR, 1966):** United Nations treaty, ratified by Mozambique, enshrining the right to privacy (Article 17) and due process (Article 14) as fundamental global norms.

**Universal Declaration of Human Rights (UDHR, 1948):** Non-binding, globally recognized articulation of privacy (Article 12), information, and dignity rights.

**Relevant World Bank, WHO, and UN standards:** For sectoral reforms, project-based data safeguards, and policy guidance (e.g., for national health information systems).

**3. ISO and International Technical Standards**

**ISO/IEC 27001: Information Security Management Systems:** Internationally recognized best practice for establishing, maintaining, and improving information security, risk management, and data protection.

**ISO/IEC 27002:** Code of Practice for Information Security Controls
Detailed control objectives and recommended controls for cybersecurity implementation.

**ISO/IEC 27701:** Privacy Information Management System (PIMS); Extension to ISO 27001 providing requirements for establishing, maintaining, and continuously improving a privacy-specific ISMS.

**ISO/IEC 29100: Privacy Framework:** Standardized framework for privacy policies, controls, and system requirements across cloud, government, and private sector operators.

**ISO 8000: Data Quality**: Requirements and best practices to ensure data accuracy, completeness, consistency, and reliability throughout its lifecycle.

**ISO/IEC 25012: Data Quality Model:** Guidance for measuring and benchmarking key quality attributes of government and sectoral data.

**4. Implementing Regulations and Guidance (Mozambique)**
**National Data Governance Council (NDGC) Regulations**

- NDGC Standard No. 1/2025: National Interoperability Standards for E-Government Systems
- NDGC Guidance 02/2025: Data Protection Impact Assessment (DPIA) Template and Methodology
- NDGC Regulation 03/2025: Security Incident Notification and Breach Response Requirements
- NDGC Circular 04/2025: Open Data Licensing and Publication Procedures

**Sectoral or Agency-Specific Regulations**

- Ministry of Health Data Governance Manual (latest edition)
- Finance Sector Data Sharing and Retention Guidelines
- Ministry of Education Student Data Protection Framework

**Audit Templates and Forms**

- Data Privacy Compliance Checklist
- Data Asset Inventory and Catalogue Template
- Mandatory Breach Notification Form
- Annual Training and Competency Certification Roster

## Annex C: National Data Classification Matrix

Mozambique's data governance regime requires all data assets across public and parastatal sectors to be classified according to risk, confidentiality needs, and legal mandates. The NDGC shall issue periodic updates and sectoral adaptations.

| Level | Description | Examples | Required Controls |
|---|---|---|---|
| Level 1: Public Data | Data intended for unrestricted public dissemination; no identifiable risk of harm to individuals, state, or business interests. | Budget summaries, statistical indicators, open legislation, public transport schedules | No restrictions; ensure accuracy and prevent unauthorized alteration; source and version metadata required. |
| Level 2: Restricted Data | Data not intended for broad release; inappropriate disclosure could affect efficiency, legal compliance, or specific interests. | Internal policy memos, preliminary reports, staff rosters, procurement details | Access on "need-to-know" basis; maintain usage logs; periodic review for declassification. |
| Level 3: Confidential Data | Data whose unauthorized disclosure could cause legal, reputational, or material prejudice to individuals, institutions, or the state; includes most personal, commercial, or pre-decisional government data. | Health records, social protection files, judicial documents, procurement bids | Encryption in storage and transit; strong authentication; restricted authorized access; audit logs; regular consent/legitimacy reviews. |
| Level 4: Secret/Classified Data | Disclosure could severely prejudice national security, essential state interests, or risk life and safety; regulated under law or executive orders. | National security plans, intelligence data, diplomatic cables, protected whistle-blower files | Access only by cleared personnel; physical and digital compartmentalization; biometric/multifactor authentication; regular NDGC security audits; documented destruction protocols upon expiry. |

**Sectoral Exceptions & Examples:**

- Education: Student assessment data is Confidential, but aggregated school performance may be Public.
- Health: Patient identity and diagnosis is Confidential, national morbidity rates may be Public.
- Financial: Bank client data is Confidential, anonymized inflation indices are Public.
- Construction: Unsafe building reports may be Restricted, critical infrastructure blueprints may be Classified.

The NDGC, in coordination with sector regulators, will issue sector-specific classification guides reflecting legal/regulatory nuance.

## Annex D: Data Quality and Metadata Standards

The NDGC prescribes mandatory quality management and audit benchmarks for all digital and physical data sets, grounded in ISO and regional standards.

**1. Data Quality Audit Templates**

Each dataset will be periodically audited for:

- **Accuracy:** Sampling and cross-verification (e.g., comparison of entry against source documentation).
- **Timeliness:** Date of last update and frequency of scheduled data refresh. Outdated data staged for review or removal.
- **Completeness:** Required fields present, missing or null values minimized, required attachments linked.
- **Consistency:** Cross-database harmonization checks; absence of conflicting records.

*Sample audit tool:*

| Field Name | Required? | Value/Range | Nulls/Errors | Time Since Last Update | Cross-Check Result |
|---|---|---|---|---|---|
| Name | Yes | Alpha | 0/1000 | <7 days | OK |
| ID Number | Yes | Numeric | 1/1000 | <30 days | OK |

**2. Metadata Fields (Standard for Government Datasets)**

- **Origin**: Source organization or system.
- **Collection Date / Occasion**: Timestamp, program/project reference.
- **Processing History**: Record of amendments, merges, derivations.
- **Retention Period and Expiry**: Standard (per sector/legal requirement).
- **Access Conditions**: Required clearance/classification.

**3. Certification Procedure**

- Agencies seeking quality certification must undergo annual NDGC/sectoral review of major datasets.
- Passing: Certification badge for datasets, authorization to publish or share externally.
- Failing: Mandated corrective measures and restricted access; NDGC/sectoral re-inspection required before restoration.

## Annex E: Data Privacy and Security Baselines

Minimum mandatory controls are set and subject to NDGC and sectoral regulation adaptation.

**1. Mandatory Controls**

- **Encryption:** All Confidential and Classified data encrypted at rest and in transit with government-approved algorithms.
- **Authentication:** Multifactor authentication for all personnel accessing Level 3/4 data; regular credential review/cycling.
- **Breach Notification:** Immediate internal reporting of suspected/confirmed breaches; notification to NDGC and affected subjects within 72 hours as per data protection relevant law.
- **Incident Response:** Pre-approved plan for every major IT system; periodic simulation drills.
- **Physical Security:** Access controls for server rooms and physical files; video surveillance, access logs retained 2 years minimum.

**2. Secure Remote Processing Guidance**

- **Teleworking:** Authorized only via secure VPN or encrypted channels; endpoint security software mandatory; no storage of Confidential or Classified data on personally-owned devices.
- **External System Integration:** Third-party connection permitted only after NDGC certification and data protection contract signing; real-time logging for all inbound/outbound data flows.
- **Cloud Access:** Only certified providers located in, or with approved equivalence in, "adequate" jurisdictions; routine penetration testing and security compliance review.

## Annex F: Data Ethics Framework

1. Core Principles
   - Fairness: Data must be handled equitably, without unjust bias, discrimination, or the creation or perpetuation of structural inequalities especially with respect to gender, region, language, disability, or minority status in Mozambique.
   - Transparency: Processing purposes, methodologies (including algorithms), data sources, and decisions must be clearly communicated to individuals and affected communities. Proactive disclosure is encouraged, except where constrained by law.
   - Accountability: All entities and staff involved in data processing and decision-making are answerable for their actions, must document rationale, and submit to impartial audit or review.
   - Harm Minimization: Risks of material, psychological, reputational, or digital harm to individuals or groups from any use of data must be assessed, minimized, and remediated where they arise.
   - Respect for Autonomy: Data subjects retain the right to informed consent, objection, access, correction, and meaningful participation in how their data is used.
2. Case Studies and Precedents
   - Mozambican Example:
     *Inequitable allocation of agricultural subsidies, based on incomplete or biased rural data collection, remedied by NDGC-mandated data quality audits and targeted post-distribution review.*
   - International Example:
     *European health authority sanctioned for unjustified exclusion of non-citizen patients from health datasets; best remedy included institutional retraining, new consent strategies, and open patient engagement sessions.*
3. Reporting and Escalation Pathways
   - Whistle-Blower Protections:
     Statutory guarantee for any public servant or contractor reporting ethical breaches or misuse of personal data, including interim anonymity and protection against retaliation. NDGC operates a secure, confidential whistle-blower reporting portal.
   - Complaint Channels:
     Public and data subjects may file ethical or legal complaints through the NDGC's online platform, physical collection points in each ministry, or via designated Data Ethics Committees.
   - Independent Review:
     The NDGC shall maintain a standing Data Ethics Review Board (DERB), comprised

of legal, technical, community, and civil society representatives. DERB reviews complex or high-risk cases, issues binding recommendations, and publicly reports on case outcomes.

Annex G: Implementation Schedules and Organization Charts
1. Phased Roadmap Tables
*(Sample entries to be tailored to each sector and assigned timeline)*

| **Phase** | **Milestone/Deadline** | **Responsible Body** | **Key Outputs / Deliverables** |
|---|---|---|---|
| Institutional Setup | 30 days post-ratification | Ministry, NDGC | Appointed CDOs, sectoral working groups |
| Foundational Training | 90 days post-ratification | All covered entities, NDGC | Training completed for all stewards, compliance staff |
| Early Pilot Rollouts | 6 months post-ratification | Priority ministries, NDGC | Pilot compliance audits, metrics dashboards |
| Full Operationalization | 12 months post-ratification | All ministries/agencies | Integration of data systems, first annual review |
| Iterative Enhancement | Ongoing | NDGC, sectoral bodies | Quarterly review, improvement reports |

2. Organization Charts
- NDGC Structure:
  - Chairperson (appointed by government)
  - Vice-Chair(s): CDO representatives from major sectors (health, finance, education, etc.)
  - Committees: Legal/Policy, Technical, Ethics, Public Engagement
  - Secretariat/Support staff
- Chief Data Officers (CDO) Network:
  Visual map showing CDOs for each relevant sector reporting up to NDGC, with direct lines to ministry leadership and horizontal connections among sectoral CDOs for cross-agency coordination.

3. Sample Budget and Capacity Audit Templates

| Category | Year 1 | Year 2 | Year 3 | Notes |
|---|---|---|---|---|
| Staffing (CDOs, stewards) | $X | $Y | $Z | Includes benefits, training |
| IT Infrastructure | $X | – | – | One-time capital outlay |
| Training | $X | $Y | $Z | Annual mandatory upskilling |
| Public Awareness | $X | $Y | $Z | Media, stakeholder forums |

Capacity Audit Checklist:

- Number of staff certified in data governance
- Percentage of systems classified/migrated
- Compliance audit pass/fail status
- Completion rates for ethical and legal training
- Public engagement/complaint response metrics

Annex H: References and Cross-References

1. Framework Documents
   - Law No. 3/2017 (Electronic Transactions)
   - Constitution of Mozambique
   - AU Data Policy Framework (2022)
   - Malabo Convention (AU, 2014)
   - SADC Model Law on Data Protection (2013)
   - ICCPR, UDHR
2. Operational Guides
   - NDGC Data Governance Policy Handbook
   - NDGC Standard Operating Procedures Manual (latest edition)
   - Templates for DPIA, breach notifications, audit checklists
   - Publicly accessible FAQ database
3. Periodic Review Schedules
   - Three-year mandatory policy review (Chapter 16)
   - Annual review of transitional compliance (Chapters 15 & 17)
   - NDGC publication calendar (electronic and physical distribution)