MAURITIUS NATIONAL DATA STRATEGY

2025 - 2029

Data Protection Office

MINISTRY OF INFORMATION TECHNOLOGY, COMMUNICATION AND INNOVATION

Contents

PREFACE

In an increasingly data-driven world, our economy is leveraging vast amounts information to enhance governance, improve service delivery and foster national progress. This "National Data Strategy" meticulously prepared by the Data Protection Office serves as a crucial guiding document specifically tailored to promote efficiency across all sectors of the economy. It aligns seamlessly with the overarching vision articulated in the Government Programme 2025-2029: A Bridge to the Future and complements the strategic directions set forth in the Digital Transformation Blueprint for Mauritius 2025-2029. Together, these foundational documents declare our collective commitment to building an inclusive, citizen-centric and forward-looking digital Republic.

The strategy acknowledges that data is a non-depletable national asset whose value is amplified through responsible collection, robust management and strategic application across all operations. It provides a comprehensive framework to overcome challenges such as data silos and trust deficits while capitalizing on opportunities presented by Mauritius dynamic digital landscape. Presently, data is fragmented, duplicated and unsynchronized with a lack of robust information architecture hampering the responsiveness of our services and obstructing systematic data sharing. Promoting Mauritius strategic location as a trustworthy jurisdiction for data handling, reinforcing the nation's commitment to digital trust and security as outlined in the Government Programme, focusing on a modern public sector in the Digital Transformation Blueprint and building unwavering trust in digital systems is our mission.

The governance framework details the core pillars that will underpin a secure, transparent and advanced digital economy. From fostering data literacy and ensuring robust data security to integrating AI-powered tools and establishing a harmonized national database, it underscores the importance of standardized processes, strong governance and collaboration to achieve a unified approach to data management. To address fragmentation, government is committed to transforming data into a valuable national asset, making it imperative to establish a single source of truth for the Whole-of-Life, Whole-of-Government and Whole-of-Enterprise with enhancing data governance, streamlining secure sharing practices, strengthening data security protocols and promoting their effective use as key priorities. Specifically, the Digital Transformation Blueprint's "Enabler 5: National Data Strategy powered by Artificial Intelligence and Analytics" provides the foundational pillar for these efforts. This enabler emphasizes the establishment of a Data Management Office (DMO) to centralize data governance, the modernization of public service delivery through unified data hubs and the implementation of a Freedom of Information Act to enhance transparency and public access to government data. These efforts are designed to ensure that no citizen is left behind in our journey towards a smarter and more connected Mauritius. AI demands data sharing to realise G2G, G2B, B2B, G2C and B2C end-to-end services whilst respecting fundamental human rights.

The Data Protection Office extends its sincere gratitude to the World Bank, European Union and local stakeholders for their valuable recommendations and insights to the National Data Strategy. Their contributions have been instrumental in shaping this document and will undoubtedly guide and strengthen its subsequent implementation.

The Data Protection Office urges all stakeholders to internalize and implement the principles and guidelines set forth in this National Data Strategy, where data fuels effective governance, responsive e-services and ultimately, a more prosperous and digitally empowered Mauritius.

Abbreviation	Full form
AI	Artificial Intelligence
B2B	Business-to-Business model
B2C	Business-to-Consumer (model)
CPD	Central Population Database
C2C	Consumer-to-Consumer (model)
DGF	Data Governance Framework
DMU/DMO	Data Management Unit/ Data Management Office
DPA	Data Protection Act
DPO	Data Protection Office
GAI	Generative Artificial Intelligence
GDPR	General Data Protection Regulation
G2B	Government-to-Business model
G2C	Government-to-Citizens model
ICT	Information and Communication Technologies
IOT	Internet of Things
ML	Machine Learning
NDS	National Data Strategy
UNCTAD	United Nations Conference on Trade and Development
MITCI	Ministry of Information Technology, Communication and Innovation

1.0 Introduction

1.0 INTRODUCTION

1.1 Background

Data management has long been a crucial factor in the production of goods and services, playing a key role in the economic and social systems of Mauritius. As a critical factor of production, data complements both labour and physical capital. Unlike traditional resources, data is non-depletable—its usage by multiple entities does not reduce its availability or value but instead enhances it. The true value of data lies in the vast amounts of machine-readable information generated across various sectors, shaping economic and social activities within the country.

In the modern digital era, Mauritius economic growth is increasingly driven by the collection, analysis, distribution and utilization of digital data—an ecosystem referred to as the data economy. The unique property of data allows simultaneous access and use by millions, fostering innovation and efficiency. The data value chain in Mauritius includes data acquisition (deriving new sources of data), secure storage and warehousing, modelling and analysis, visualization, transmission and protection. These processes culminate in digital intelligence which drives informed decision-making, innovation and competitiveness.

The UNCTAD 2019 Digital Economy Report highlights that data's true value emerges when it is transformed into digital intelligence and monetized through commercial applications. Therefore, productivity in Mauritius digital economy depends on the strategic application of digital intelligence across different sectors. This intelligence acts as the "digital capital" of today, driving economic growth through various forms of data monetization.

Mauritius National Data Strategy (NDS) establishes a framework for transforming both personal and non-personal data into a strategic asset. The strategy recognizes data as "a powerful asset" whose value is defined by its responsible use, particularly in the context of rapidly advancing digital technologies like AI, IoT and big data analytics. By effectively harnessing the vast amounts of data generated across public and private sector through the NDS, Mauritius can unlock new economic opportunities, enhance digital transformation and drive sustainable national development and prosperity.

1.2 The Rationale of the National Data Strategy

The world is witnessing the growing influence of data as a key driver of economic growth in the digital era. While these present immense opportunities, it also raises concerns about data protection, where participants in the data economy face challenges such as trust deficits, security risks and privacy breaches. This highlights two critical challenges: **data utility and data protection**. While data utility fosters innovation, economic growth and social development, data protection ensures that personal and sensitive data are handled securely, safeguarding citizens' privacy. Striking the right balance between these two aspects is essential to fully harness the benefits of data.

Mauritius has made significant strides in data protection and privacy, aligning with global efforts to ensure the responsible management of personal data. The implementation of the Data Protection Act (DPA) and adherence to international standards, notably data protection principles and rights which are the backbone of the European Union's General Data Protection Regulation (GDPR) and Council of Europe Convention 108+ (Mauritius is a party to the Convention) have reinforced the country's commitment to safeguarding data privacy while fostering a secure digital ecosystem. Moreover, the planned recast of the DPA along with possible changes in the Constitution will further align data protection standards in Mauritius with European standards. These measures are contributing to the emergence of a dynamic data-driven economy, necessitating a comprehensive national strategy to optimize the opportunities presented by the data economy.

Recognizing the dual importance of data utility and protection, the NDS has been developed as a framework to create an enabling environment for both aspects. The strategy outlines actionable plans to ensure the privacy of Mauritian citizens and international stakeholders while leveraging data as a key driver of innovation, productivity, digital services, job creation, global competitiveness and economic prosperity. It serves as a guiding document to shape Mauritius digital future by supporting policy development, fostering a robust data market and strengthening the country's position as a regional hub for data-driven economic activities.

As Mauritius continues its digital transformation journey, the NDS presents opportunities to accelerate the adoption of emerging technologies for data collection, storage, analysis, protection and usage. By doing so, it enhances research and innovation, digital services, economic growth, job creation and overall societal well-being. The strategy positions Mauritius to fully embrace the potential of a data-driven economy, ensuring that the Government, private sector and citizens can securely and efficiently harness data for national development and global competitiveness.

1.3 Challenges and Opportunities in the Mauritian Context

Mauritius faces both opportunities and challenges in the context of data and the data-driven economy. The strategic aspirations, enablers and initiatives for the implementation of the NDS will take into account these challenges and opportunities. The aim of NDS is to transform these challenges into opportunities and leverage them to optimize

Mauritius participation in the data economy, thereby maximizing the value of data to fuel the country's digital economy.

1.3.1 Challenges

The NDS acknowledges several challenges that hinder Mauritius from fully engaging with and benefiting from the data economy:

Culture: 01

In both the public and private sectors, there is a tendency to keep data restricted, limiting its use and reuse. Data is often seen as a valuable resource that should not be easily shared. The NDS seeks to promote a cultural shift by raising awareness about the importance of data utility, encouraging open data and enhancing value creation for data owners and potential users.

Trust: 02

A significant trust deficit exists regarding data protection, privacy, breaches and security, especially among consumers in the digital economy. The NDS aims to build trust by implementing robust mechanisms that ensure consumer protection, data privacy and security while also minimizing monopolistic practices and anti-competitive behaviour.

Dominance of data-haves: 03

Government agencies, large corporations, multinational companies and development partners control much of the data landscape in Mauritius. This dominance creates barriers for smaller businesses to access and compete in the data economy. NDS aims to foster a more inclusive data economy where the SME sector in Mauritius can also access data, ensuring a mutually beneficial environment for all, including citizens.

Global data economy requirements: 04

As the world promotes both data privacy and cross-border data flows, balancing these competing demands presents a challenge. Mauritius will focus on enhancing digital infrastructure and capabilities such as cloud computing, edge computing and fiber optics to meet these global requirements. The goal is to position Mauritius as a leader in data protection and cross-border data flows in Africa.

A single harmonized and integrated national database: 05

The creation of a unified and harmonized national database for citizens and other national data is essential for the success of the NDS. This harmonization will enhance effective service delivery, support humanitarian and social development programs and improve national security. NDS will emphasize the need for integrated databases to support Mauritius participation in the global digital economy.

Data literacy, capabilities, intelligence and insights: 06

Data literacy and the ability to use technologies that optimize data collection and transformation into actionable insights are crucial. NDS will ensure that data literacy and capabilities are developed to foster effective data management across all stages, from collection to analysis and encourage the adoption of emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), Big Data and Blockchain.

1.3.2 Opportunities

Mauritius has several opportunities that can accelerate its participation in the data economy:

01

Population: Mauritius is relatively small but with a dynamic population. As of the latest census, the country has a growing number of young people who are key drivers of social and economic activities in the digital space. Meeting the needs of this population will drive data activity across government, private sectors and civil society promoting a vibrant data economy.

02

Increase in Mobile and Broadband Penetration: With the rise in mobile phone usage, there is a significant increase in broadband penetration, leading to the creation of vast amounts of digital data. These digital footprints provide the foundation for a thriving data economy in Mauritius.

03

Growth of Digital Platforms and Services: As new digital platforms emerge across Mauritius, there are increasing opportunities to capture value from data. These platforms not only offer services but also create data that can be leveraged for growth while ensuring data protection.

04

Mobile ID: The Mobile ID in Mauritius is a key initiative aimed at providing secure digital authentication for citizens, enabling them to access a range of services, such as e-government and financial transactions, through their mobile phones. It offers a secure and convenient way for citizens to verify their identity without needing physical documents. The Mobile ID is part of Mauritius broader efforts to digitize public services, improve access and enhance security for online transactions. The strategy aims to improve public service delivery through digital platforms, foster innovation and establish a regulatory framework to ensure data sovereignty and trust. Both the Mobile ID and the NDS play central roles in advancing Mauritius digital agenda and positioning it as a leader in digital governance.

1.4 Data Definitions

The NDS follows the principles outlined in Information Science Literature, where data is seen as part of a hierarchy that connects to information and knowledge. Data is defined as:

1. Unfiltered symbols or signals generated from all living and non-living things within the nation's borders, including natural and human activities in Mauritius;
2. Collected through either physical or digital methods from the activities of the Mauritian Government, private enterprises, development partners, multinational companies and individuals within or outside the territory of Mauritius;
3. Converted into digital formats and transformed into information through computing processes;
4. The information is utilized to enhance people's experiences, skills, decision-making and thinking models, which can result in the creation of products and services, among others;
5. Contributing to the body of knowledge in research and innovation that can be applied and re-applied by individuals for governance, business performance, social and economic growth and sustainable development in Mauritius.

The NDS classifies data, either in a state of rest, in motion, or in use, as follows:

1. Personal or non-personal data;
2. Private and public data;
3. Data for commercial, governmental and developmental purposes across various sectors and industries;
4. Real-time data collected via sensing technologies;
5. Data used by corporations, including corporate data, human resources data, technical data and merchant data;
6. Structured and unstructured data;
7. Instant and historical data;
8. Volunteered, observed and inferred data;
9. Sensitive and non-sensitive data related to the country;
10. Business-to-Business (B2B), Business-to-Consumer (B2C), Government-to-Consumer (G2C) or Consumer-to-Consumer (C2C) data.

1.5 Strategic Context

The NDS outlines the importance for Mauritius to actively engage in the data economy, highlighting the challenges that hinder the nation from fully utilizing the opportunities within the data economy. By doing so, Mauritius can generate value that contributes to innovation, sustainable economic growth and social development. In addition to the National Data Standards, there are several key laws, policies and standards that help regulate data management, protection and privacy. These include:

Data Protection Act 01

Cybersecurity and Cybercrime Act 02

Information and Communication Technologies (ICT) Act 03

Electronic Transactions Act 04

Digital Transformation Blueprint 2025 - 2029 05

Public Procurement Act 06

Consumer Protection (E-commerce) Act 07

Statistics Act 08

Industrial Property Act 2019 09

Copyright Act 10

1. **Data Protection Act:** This is a key piece of legislation that governs the collection, processing, storage and sharing of personal data in Mauritius. It is aligned with international standards such as the European Union's General Data Protection Regulation (GDPR) and Council of Europe Convention 108+ that provide individuals with rights over their personal data.

2. **Cybersecurity and Cybercrime Act:** Mauritius has established a robust legal framework to address cybercrime through the enactment of the Cybersecurity and Cybercrime Act 2021. The Cybersecurity and Cybercrime Act 2021 plays a crucial role in enhancing cyber resilience, protecting critical information infrastructure and ensuring data security. It establishes key bodies like the National Cybersecurity Committee to combat cyber threats and safeguard digital assets. The National Cybersecurity Strategy is a national policy aimed at improving cybersecurity measures across the country, protecting critical infrastructures and ensuring a secure environment for digital services and information.

3. **Information and Communication Technologies (ICT) Act:** This act covers issues related to cybercrimes, information security and the regulation of the ICT sector. It addresses the legal framework for electronic transactions and digital signatures within the ICT sector.

4. **Electronic Transactions Act:** This act facilitates the use of electronic commerce in Mauritius by setting the legal framework for digital contracts, digital signatures and electronic records. It enhances the legal standing of electronic transactions.

5. **Digital Transformation Blueprint 2025 - 2029:** A strategic roadmap that outlines government's commitment to modernising public services, empowering our people through technology, strengthening national competitiveness and safeguarding the values of trust, inclusion and sustainability of our democratic values.

6. **Public Procurement Act:** Although primarily focused on public procurement, this act also contains provisions related to data security and transparency in public-sector dealings, including ICT and e-government projects.

7. **Consumer Protection (E-commerce) Act:** This act provides a legal framework to protect consumers engaging in electronic commerce in Mauritius, which includes provisions about data security, electronic transactions and the protection of consumers' personal information.

8. **Statistics Act:** It establishes Statistics Mauritius as the central authority for official statistics, responsible for collecting, analyzing and disseminating data to support policymaking. It ensures confidentiality and data protection by restricting unauthorized disclosure. It mandates collaboration across government bodies for accurate data collection and imposes legal obligations and penalties for non-compliance to maintain data integrity. Overall, the Act provides a framework for producing high-quality, reliable statistics to support informed decision-making in Mauritius.

9. **Industrial Property Act 2019:** It establishes a framework for protecting industrial property rights—including patents, utility models, circuit layouts, breeder's rights, designs, marks, trade names and geographical indications.

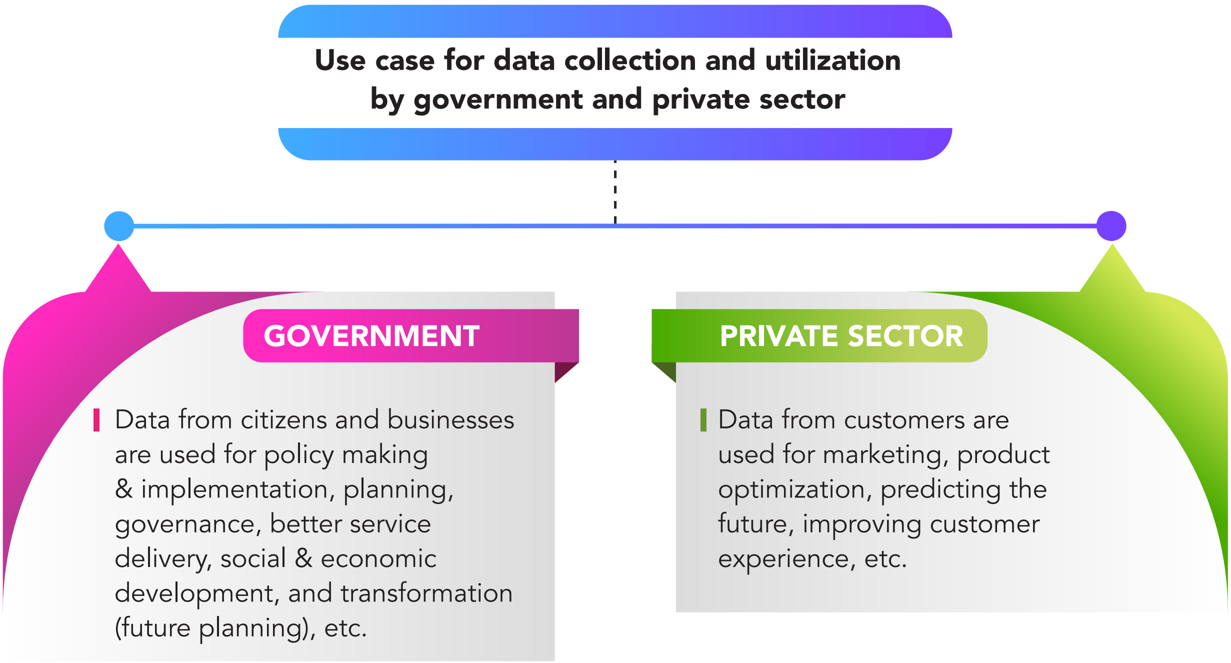
10. **Copyright Act:** The Act provides a comprehensive legal framework for the protection of literary, artistic and scientific works, ensuring that creators have the rights to control the use of their works and derive economic benefits from them.

1.6 Strategy Development Method

The NDS has been developed by benchmarking african and global trends, as well as the local context and priorities of Mauritius. It also underwent reviews by experts and stakeholders through consultations and co-creation, public engagement and workshops.

1.7 The Scope and Applicability

The NDS will focus on developing and utilizing data as a national resource to drive value creation and enhance global competitiveness for Mauritius. It will also ensure the protection and privacy of data subjects. The scope of the NDS will encompass data from both the public (government) and private (businesses and individuals) sectors. While the public and private sectors generate, collect, store and use data for different purposes, there will be consistency and alignment in the way data is applied across both sectors.



Use case for data collection and utilization by government and private sector

GOVERNMENT

Data from citizens and businesses are used for policy making & implementation, planning, governance, better service delivery, social & economic development, and transformation (future planning), etc.

PRIVATE SECTOR

Data from customers are used for marketing, product optimization, predicting the future, improving customer experience, etc.

Figure 1.0: Example of Public and Private Sectors Data Use Case

1.8 Data Sharing

Data sharing for the NDS is a critical component in the governance of a country, especially when aiming to enhance the efficiency, transparency and innovation within public services and the private sector. The NDS will promote efficient data sharing which is crucial for modernizing government operations, fostering innovation and delivering better services to citizens. By ensuring effective governance, legal compliance and robust infrastructure, the government can harness the full potential of data to drive growth and improve outcomes in multiple sectors.

The scope of data sharing between the public and private sectors will be cross-sector in nature. Data governance frameworks vary in their approach to exclusive data-sharing arrangements with private sector entities. These frameworks differ specifically regarding the sharing of commercially sensitive, statistically confidential and personal data. Some frameworks strictly prohibit such exclusive arrangements, while others permit them only under exceptional circumstances—namely, when necessary to provide a public interest service or product that would otherwise be impossible to deliver. When such exclusive sharing is allowed, the decision must adhere to principles of transparency, equal treatment, and non-discrimination. Additionally, any exclusivity granted should be limited to a specific timeframe rather than permanent.

Data sharing will be organized into five categories that represent the core framework for collaboration and partnerships between key stakeholders. The categories are:

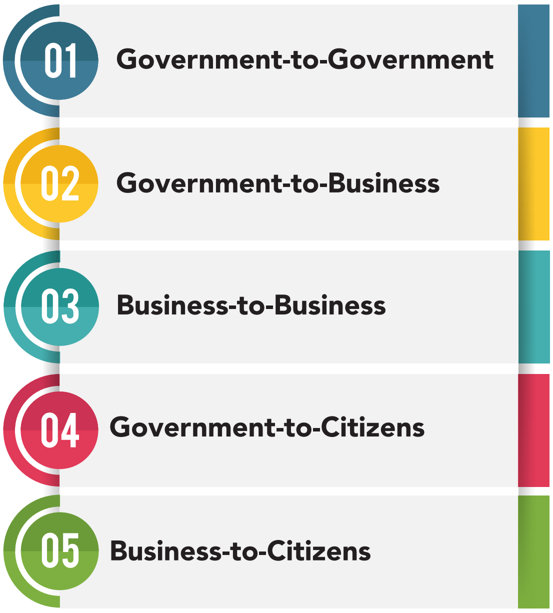

01 Government-to-Government
02 Government-to-Business
03 Business-to-Business
04 Government-to-Citizens
05 Business-to-Citizens

Figure 2.0: Categories of Stakeholders

- **Government-to-Government Model:** The aim of G2G data sharing in Mauritius is to facilitate the exchange of data between Ministries and Departments, where relevant and appropriate, with proper safeguards in place to enable efficient and effective use of data for service delivery and informed decision-making. Ministries and Departments must proactively identify and address any procedural, regulatory, legal and cultural challenges to sharing data within government entities and with external partners.

- **Government-to-Business Model:** The objective of G2B data sharing is to foster collaboration between public institutions and private businesses by making public data available to businesses and vice versa. This aims to design and implement innovative services that benefit the public and align with their interests. An appropriate business model can be developed to facilitate this exchange. Both parties must comply with the relevant legal and regulatory requirements to ensure secure collaboration and the proper use of shared data.

- **Business-to-Business Model:** The B2B data sharing model ensures that businesses exchange or trade data with other businesses to offer value-added services and create new opportunities based on mutually agreed business models. Parties involved must comply with legal and regulatory standards to maintain secure and responsible data-sharing practices.

- **Government-to-Citizens Model:** G2C data sharing ensures that government institutions make public data accessible to individuals or citizens for social and economic purposes. Both parties must adhere to the applicable legal and regulatory provisions to ensure proper engagement and data use.

- **Business-to-Citizens Model:** B2C data sharing allows businesses and private organizations to share data with individuals or citizens who require it for social and economic purposes. The parties involved must follow and comply with the relevant legal and regulatory provisions to ensure secure and responsible data-sharing practices.

The Info Highway is the Government-to-Government (G2G) and Government-to-Business (G2B) data-sharing platform in Mauritius. It operates under a publisher-subscriber model, where government institutions publish verified data for authorized subscribers. The government will extend subscriber access to private sector entities under strict regulatory, security and compliance conditions to foster innovation while protecting data integrity. It is also proposed to include data governance requirements for subscribers and publishers along with data governance for Info Highway.

Policies and frameworks have been developed for data sharing where individuals can grant, track and revoke permissions via Mo Kloud, digital authentication platforms and API-based approvals.

2.0 NDS Aspirations

NDS aspirations are founded and built on the following:

Mission

To harness the economic and social value of data for the advancement of Mauritius

01

Vision

To make Mauritius a global leader in the data economy, translating into prosperity for all Mauritians

02

Goals

To make data as accessible, shareable and actionable as possible for all stakeholders who need it for economic and social benefits in Mauritius

03

2.1 Strategic Statement

The strategic statement of this NDS is:

Data is our next valuable national resource

2.2 Value Proposition

The NDS will offer the following benefits to data owners, government stakeholders, businesses and individuals in Mauritius:

1. **Ownership:** Data subjects will retain ownership of their data and have the absolute right to it, except in cases where national interests are involved.
2. **Security and Privacy:** The security and privacy of citizens' data will be a top priority in all data usage for developmental or innovation purposes.
3. **Public Good:** Data will be accessible to all, with its use benefiting the public good and fostering societal advancement.
4. **Shared Value:** There will be a fair and equitable distribution of the value generated from data use. No single entity or platform will monopolize data usage.
5. **Job Creation:** An enabling environment will be created to position data as a major source of employment and economic growth.
6. **Global Competitiveness:** Mauritius will harness the economic and social value of both local and international data to enhance its global competitiveness. The NDS will promote the growth of data-driven and data-mining organizations within the country.

2.3 Guiding Principles

NDS's guiding principles are:

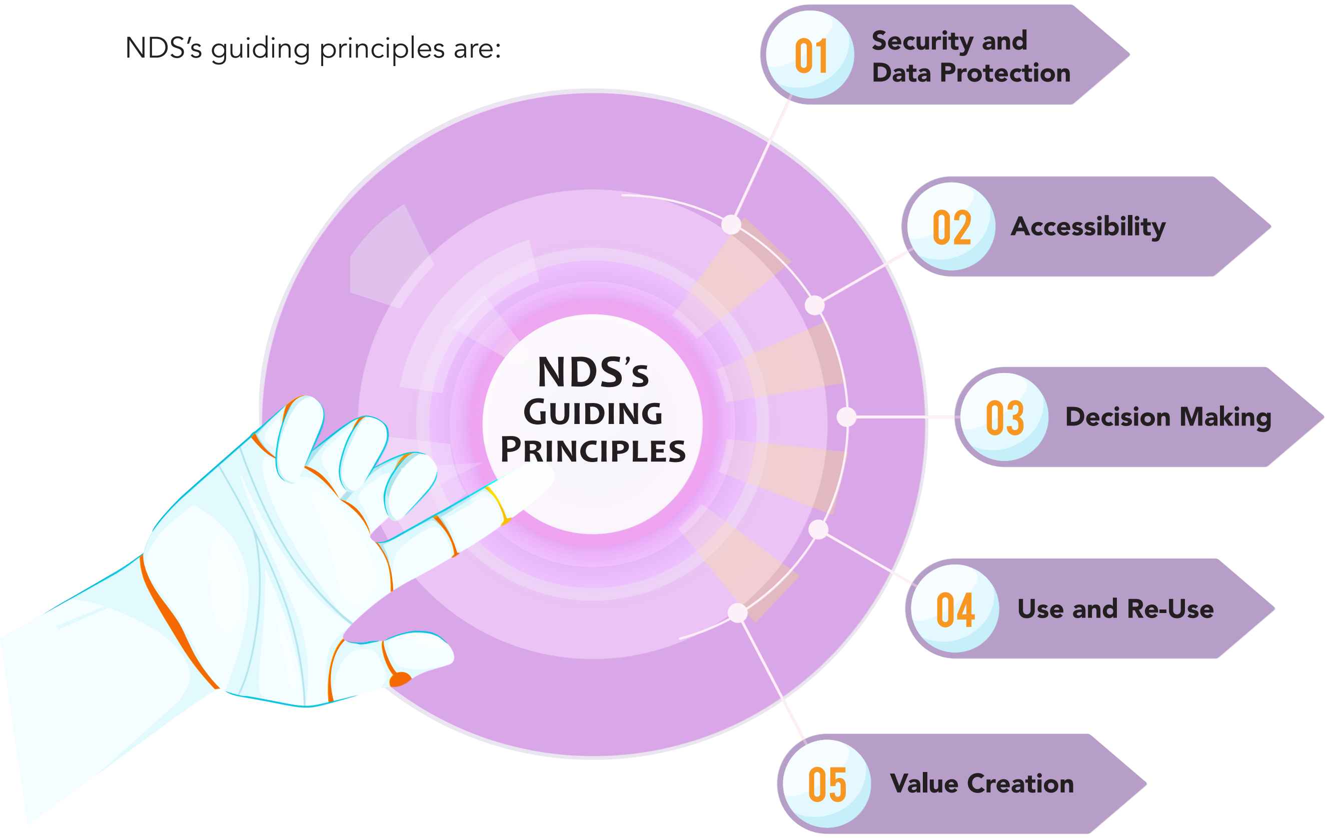


Figure 3.0: NDS's guiding principles

2.4 Strategic Objectives

1. Raise awareness about the importance of data as a national resource for creating new value in Mauritius.
2. Mobilize and build a data economy ecosystem as a key component of Mauritius digital economy ecosystem.
3. Ensure a unified and consistent source of national data to improve government service delivery in Mauritius.
4. Ensure consistency in data governance across all organizations in Mauritius.
5. Integrate data literacy and skills into the digital literacy and skills framework within the Mauritian educational system.
6. Develop, adopt and implement data security strategies, standards, programs and activities to enhance data security within both government and businesses in Mauritius.
7. Create and deploy new mechanisms to ensure adherence to and compliance with laws, regulations and rules governing data usage in Mauritius.
8. Improve compliance with existing legal and regulatory frameworks on data protection laws in Mauritius.
9. Develop open data strategies, guidelines, programs and activities to increase open data within government and businesses, fostering greater transparency and innovation.
10. Facilitate an enabling environment for increased investment and enhancement of data infrastructure capabilities in Mauritius.
11. Develop strategies and programs to accelerate the use of data for research and development, innovation and social and economic activities in Mauritius.
12. Orchestrate initiatives that enhance Mauritius competitive advantage and contribution to the data economy on both the continental and global stages.

2.5 Specific Objectives

1. Raise awareness and shift mindsets about the importance of data for sustainable social and economic growth to a number of Mauritians.
2. Increase data literacy and skills.
3. Enhance data security in government and businesses.
4. Improve data privacy for citizens.
5. Increase open data in both government and private sectors.
6. Boost investment and capabilities in data infrastructure.
7. Expand the use of data for research and development, innovation and social and economic activities.
8. Increase Mauritius contribution to the global data economy.
9. Improve Mauritius competitiveness in the global digital economy.

3.0 NDS Pillars

In pursuit of the mission to address the challenges and capitalize on the opportunities identified in the NDS, ten pillars have been established. These pillars will serve as key structures to drive the acceleration of achieving the NDS goals in Mauritius. Each pillar will be supported by various implementation strategies. The pillars are:

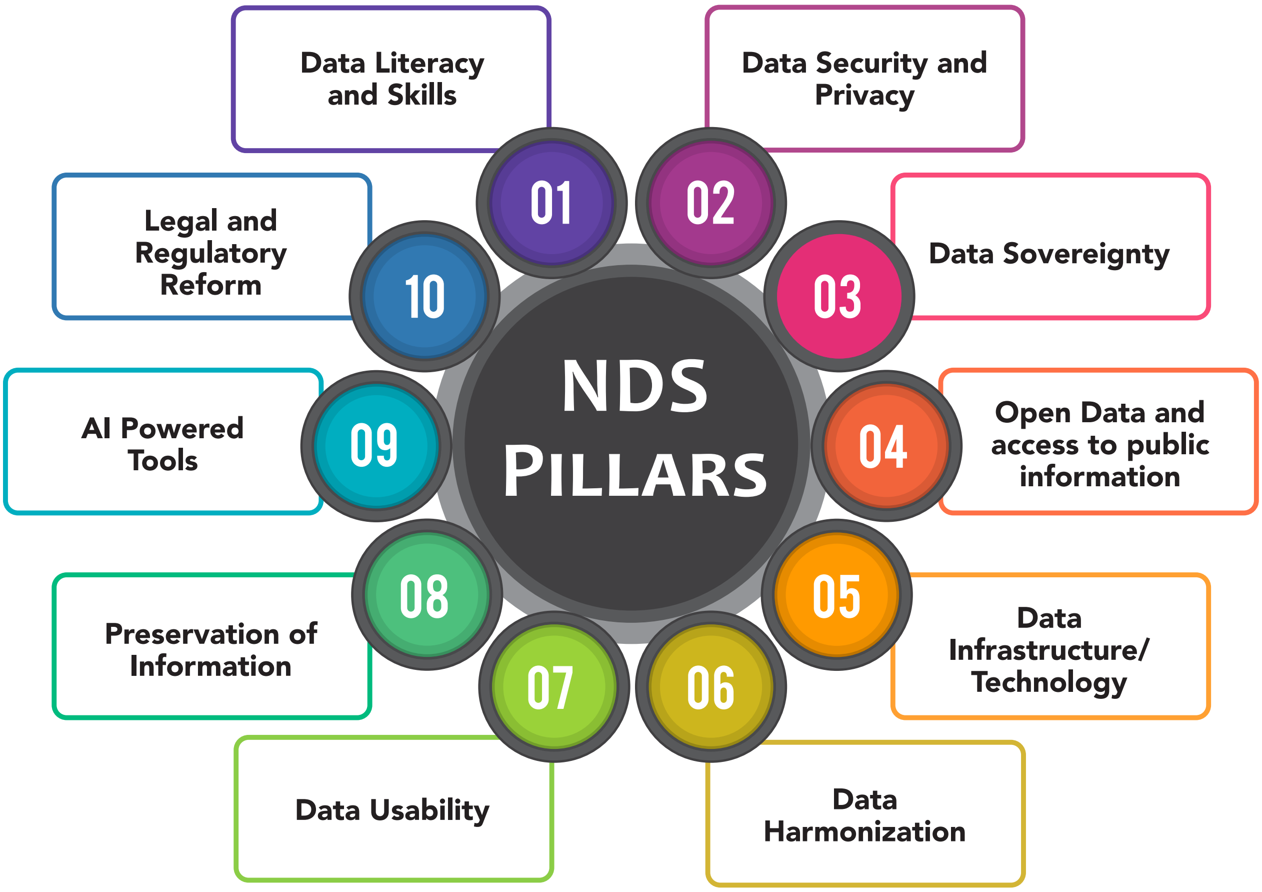

NDS PILLARS
01
Data Literacy and Skills
02
Data Security and Privacy
03
Data Sovereignty
04
Open Data and access to public information
05
Data Infrastructure/ Technology
06
Data Harmonization
07
Data Usability
08
Preservation of Information
09
AI Powered Tools
10
Legal and Regulatory Reform

Figure 4.0: NDS Pillars

3.1 PILLAR 1: Data literacy and skills

The objective of this pillar is to ensure that citizens, government and private organizations in Mauritius acquire the relevant knowledge and skills to effectively use data as a resource for development. Data literacy and skills refer to the ability to read, collect, validate, store, analyse, securely transmit, protect and derive knowledge from data. There is a national need to educate all citizens, as well as private and government organizations, about the importance of data and how to effectively use and manage it. This includes integrating data literacy as part of the curriculum in Mauritius educational system and embedding data science, Artificial Intelligence (AI) and cybersecurity across all levels of the national education system, complemented by robust upskilling and reskilling programs to ensure a future-ready workforce equipped with critical data competencies. Such actions will ensure data is recognized as a valuable resource for national progress and will prepare citizens for data-related job opportunities in the global digital economy.

3.2 PILLAR 2: Data security and privacy

The objective of this pillar is to address information security and cybersecurity risks associated with data management in Mauritius. To effectively realize the benefits of data, it is essential to implement a robust data security strategy and embed "Security by Design" and "Privacy by Design" principles into all new and existing data systems and applications. Data security refers to safeguarding the confidentiality, integrity and availability of data. It also extends to protecting the privacy of data owners, ensuring data is not processed or disclosed without consent. Data security strategies in line with the Data Protection Act must be adopted by both government and private organizations in Mauritius to ensure the protection of data and its owners from security risks. Care must be taken to ensure that data security measures do not create unnecessary barriers to data use.

3.3 PILLAR 3: Data sovereignty

The objective of this pillar is to address data ownership, classification, control and access as they relate to data residency and localization, in accordance with national laws and regulations in Mauritius. Data Sovereignty ensures that data generated within Mauritius or by Mauritians, whether inside or outside the country, is subject to the laws governing data use in Mauritius. It is a critical aspect of data privacy and enables the country to regulate who can access sensitive data. Data sovereignty supports data residency, ensuring that local data is governed by national laws and policies.

Governments often implement data localization requirements seeking to protect citizens or other national interests from various data-related risks, such as cybersecurity threats, foreign surveillance and the unfair exploitation of data by foreign corporations. Data localization measures, however, frequently align with protectionist agendas, potentially affecting trade and undermining the economic and democratic potential of the free and open internet and its infrastructures for businesses and individuals. Data localization requirements obstruct most cross-border data flows, and these negative impacts are especially pronounced in cases where they are conceived strictly - a trend which is particularly common in the low- and middle-income countries. For instance, a study by the OECD and WTO suggests that removing existing data localization measures would lead to a rise in exports by 0.26% and GDP by 0.18%. Gains for low-income economies would be larger, with GDP rising by over 1% upon removing data localization measures. It is recommended that NDS defines the specific circumstances under which data localization measures are justified. It is also proposed that government data be hosted locally.

3.4 PILLAR 4: Open data and access to public information

The objective of this pillar is to create an environment that facilitates the seamless use of data collected by the government, businesses and individuals for development and innovation, without compromising data security and privacy. Promoting open data will foster economic value, increase transparency, stimulate business development, build trust between citizens and organizations and improve public service delivery. To leverage the economic potential of data in Mauritius, government and private organizations must make national data accessible to the public, encouraging innovation and public engagement. A Freedom of Information Act is part of the government programme 2025 - 2029 and the MITCI Blueprint.

Open data principles should include:

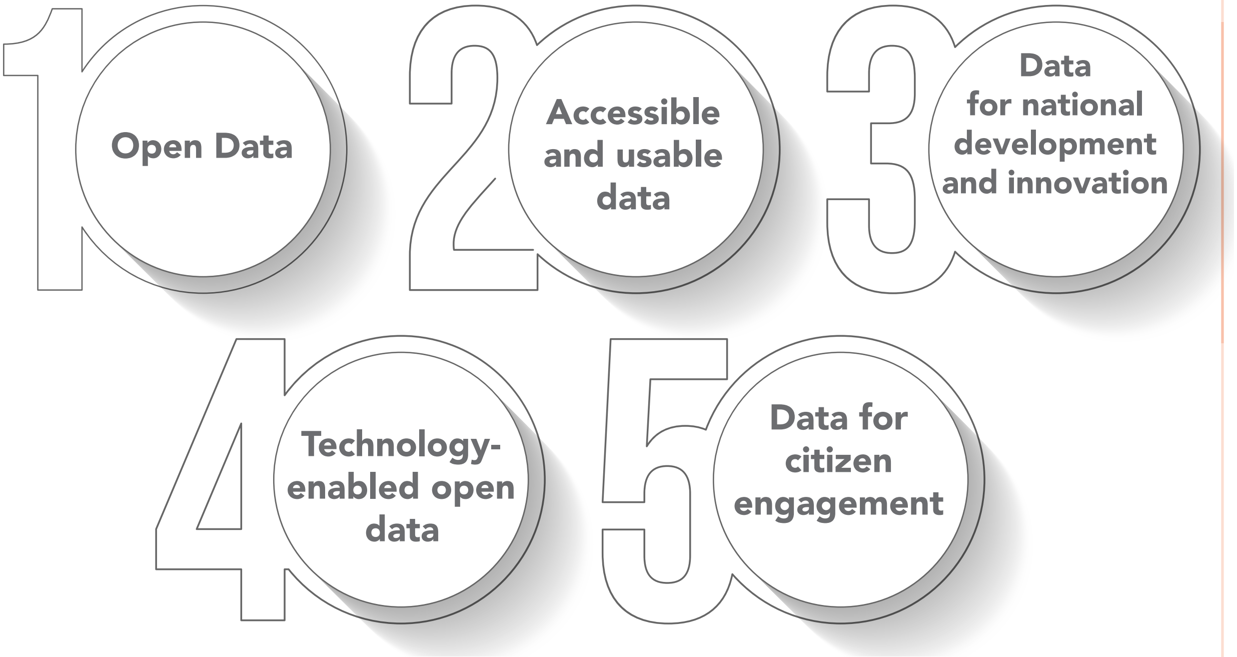

1
Open Data
2
Accessible and usable data
3
Data for national development and innovation
4
Technology-enabled open data
5
Data for citizen engagement

Figure 5.0: Open Data Principles

The National Open Data Policy, established in May 2017 by the Ministry of Information Technology, Communication and Innovation outlines the framework for releasing and managing government datasets as open data. This policy document details the creation of a National Open Data Portal, adhering to ICT security standards and initially set up on the Government Portal's SharePoint platform, to serve as a central point of contact for datasets released as Open Data. The policy also indicates a future consideration for an open-source based Open Data Portal to provide greater flexibility. The National Open Data Portal is the primary platform for data discovery and access for all new datasets to prevent individual governmental agencies from establishing their own separate portals, ensuring a unified and consistent approach to data access and potentially leveraging the existing infrastructure and established technical standards, such as the use of CSV and XML formats for data release. The Central Open Data Team (CODT), responsible for administering the National Open Data Portal and setting standards for Open Data, plays a crucial role in integrating the current platform with the broader NDS objectives. The National Open Data Policy needs to be reviewed in line with the open data principles of the NDS.

The NDS must also incorporate robust anonymization standards to mitigate the inherent risks of re-identification in datasets, even when personal data has undergone anonymization. These re-identification risks can arise when:

- It is possible to distinguish the data relating to an individual from all other information contained in the dataset. For instance, the dataset specifies height of an individual was 6 feet 5 inches, which would make it easier to identify an individual in a small dataset even if no other personal information is provided.
- Anonymized data is linked and combined with other publicly available information. For instance, researchers have been able to re-identify 43% of known patients by matching de-identified data sets against news reports.
- In some cases, it may be possible to infer a link between two pieces of information in a set of data, even though the information is not expressly linked.

Such re-identification risks necessitate technical standards on anonymization and the extent to which it needs to address re-identification risks.

3.5 PILLAR 5: Data infrastructure

The objective of this pillar is to create an enabling environment for increased investment and deployment of technologies and infrastructure that accelerate the use of data for development and innovation in Mauritius. Effective data management requires investment in digital technologies such as green data centers , secure resilient operating centers, data transmission networks (e.g., fiber optics, 5G, satellite), databases, IoT, big data analytics platforms and AI. To accelerate innovation and support high-impact research and development, it is critical to ensure broad and sustained access to High-Performance Computing (HPC) infrastructure for advanced analytics and AI model training. Although several enabling technologies are already in place, strategic emphasis should be placed on local production to lower costs and strengthen national security. Furthermore, integrating government digital infrastructure into a unified system will minimize resource duplication and enhance the efficiency of public service delivery.

3.6 PILLAR 6: Data harmonization

The objective of this pillar is to harmonize national data across various sectors for effective management, improved public service delivery and the creation of new business models and for most services in Mauritius. Fragmented national data, such as citizens' personal data, demographic data and national security information, hampers the effective use of data for development. Data harmonization involves reconciling and integrating disparate data sources to create a consistent and single source of data for use by government and businesses. By addressing this fragmentation, Mauritius can improve resource management and service delivery, leveraging harmonized data to provide more efficient and transparent public services.

The Central Population Database (CPD) is the official citizen identity repository of Mauritius, structured with distinct data components governed by respective authorities. All government agencies requiring access to citizen civil data must access CPD via secure, authorized channels like the Info Highway. No modifications are permitted outside the designated data sources.

An Address Data System (ADS) to support the CPD system has to be created and be a single authentic source of information on the validity of addresses and ensure the correctness and uniform way of address representation.

3.7 PILLAR 7: Data usability

The objective of this pillar is to provide the resources, capacity and environment needed to unlock the full potential of data for social and economic growth and innovation in Mauritius. Data usability ensures that data is established as a useful resource for value creation, supporting economic and social development. Strategies will be implemented to maximize the use of data across sectors such as research and development, health, national security, finance and technology. Advocating for the value and importance of data will drive data-driven innovations and create new organizations capable of generating valuable insights from both local and international data, ensuring global competitiveness and fostering Mauritius growth in the digital economy. Advancing national AI capabilities by prioritizing the creation and stewardship of high-quality, diverse and well-annotated datasets, while ensuring equitable access to scalable compute infrastructure is crucial. These foundational pillars will enable the development, training and deployment of sophisticated AI solutions, driving innovation across key economic and public service domains.

Public and private institutions shall reuse and share information and data that are already stored subject to data privacy requirements. In adherence to principles of user-centricity, data shall be submitted by users only once. They are required to establish mechanisms for retrieving and sharing this data strictly in compliance with prevailing data protection regulations.

3.8 PILLAR 8: PRESERVATION OF INFORMATION

The principle of Preservation of Information is a foundational pillar to ensure the long-term legibility, reliability and integrity of electronic records and information held. Such preservation is critical for safeguarding documentation of procedures and decisions while maintaining accessibility, security and privacy over time. A data retention policy has been elaborated to manage the storage, retention and disposal of personal data. This policy aims to ensure the proper handling of sensitive information while safeguarding the privacy rights of individuals.

3.9 PILLAR 9: AI POWERED TOOLS, CYBERSECURITY AND CENTRALIZED SERVICES

The Data Protection Office in collaboration with MITCI has issued a Generative Artificial Intelligence (GAI) Policy for public officers. The purpose of the policy is to ensure the responsible, secure and lawful use of GAI tools in government operations. It applies to all public officers and contractors and third parties dealing with public authorities.

An AI Guide is currently in preparation to provide practical insights and regulatory frameworks for AI implementation. This initiative underscores DPO's commitment to advancing AI governance while safeguarding data protection and individual rights in the evolving digital landscape.

In line with the Government Programme 2025-2029, a National Artificial Intelligence (AI) Strategy will be formulated. The core objective is to leverage the potential of AI to significantly propel economic growth and enhance efficiency across various sectors of the economy and the society.

To accelerate the transition to a digitally advanced economy, an AI Unit will be established under the aegis of the Ministry of IT. This dedicated unit will act as a cross-cutting enabler, integrating AI across all national digital projects and ensuring AI technologies are responsibly and effectively harnessed to improve public services, economic productivity and social well-being.

A new entity, the National Cyber Resilience and Cybersecurity Agency (NCRCSA), will be created to ensure the timely deployment of effective cybersecurity measures at the national level. Furthermore, new entities/units will be set up to manage digital identity, including the ID Card, Mobile ID, Digital Service Authentication and Trust services for Digital Signature Identity Management. These services will be recognized by this new entity, providing legal sanctity to electronic identity management services such as Digital Service Authentication, as well as other digital identity registration and verification services in the private sector.

With the Unified Government Portal and the upcoming Government Super App, all services will be available under one roof. With just one login, using Digital ID or Mobile ID, citizens will be empowered to consume services online. Government is moving from being in line to being online to provide fast services, at the comfort of citizens. DIVA, Digital Interactive Virtual Assistant, is a key component of this digital transformation, evolving into a comprehensive AI-powered digital platform leveraging Agentic AI, Multi-Modal Large Language Models (LLMs) and Retrieval-Augmented Generation (RAG) for broad public service delivery. This move aims to transition from informative to transactional services across various ministries, ensuring responsive, proactive and transparent citizen engagement.

To ensure that every digital service is simple, secure and designed around citizens' real needs, a National Digital Services Framework will be adopted. This framework will make it mandatory for all public services to follow key principles: digital-by-default, once-only data collection, life-event-based journeys and mobile-first access. It will set clear standards for service quality, data reuse and inclusion, ensuring that services comply with availability standards. Blockchain technology to strengthen data integrity and secure identity management, while leveraging Internet of Things (IoT) data to accelerate smart innovation initiatives is to be implemented.

A clear lifecycle and risk-based AI governance framework will ensure that:

- AI systems follow a defined lifecycle from design through deployment and monitoring.
- Accountability for AI-supported decisions is well understood.
- Public confidence in digital government is maintained.
- A proportionate, risk-based approach is applied to classifying public-sector AI systems based on impact, data sensitivity and degree of automation.

These measures will align with international good practices including ISO/IEC 23894:2023.

3.10 PILLAR 10: Legal and regulatory reform on data protection and privacy

Government will undertake a comprehensive update of its data protection and privacy laws to strengthen trust in the digital environment. This includes:

(i) Modernisation of the Data Protection Act to be realigned with the European Union General Data Protection Regulation (GDPR)

(ii) Enactment of regulations relating to data protection officers and e-privacy to cater for the protection of data processed through electronic communications networks

(iii) Enactment of Freedom of Information Act to cater for access to public information.

(iv) Revision of the constitutional right to privacy to cater for data protection and freedom of information.

4.0 NDS Enablers and Drivers

4.0 NDS ENABLERS AND DRIVERS

4.1 NDS Enablers

The successful outcomes of the National Data Strategy (NDS) in Mauritius will rely on several key enablers:

Leadership: Strong leadership is crucial for the effective implementation of the NDS across both public and private sectors in Mauritius. Senior management in government and private organizations must recognize that data is a valuable resource that can drive the digital economy. Leaders must ensure the necessary capabilities, supportive environment and effective governance structures to allow the NDS to meet its goals. Full support and commitment from leadership at all levels are essential for the NDS's successful implementation.

Enabling Environment: An effective enabling environment, including appropriate laws, policies, regulations, guidelines, processes and measures, is necessary to ensure full compliance with and implementation of the NDS.

Governance: Strong governance is needed to ensure clear responsibilities, accountability and sound decision-making throughout the implementation of the NDS. A governance framework must be established to guide the full implementation of the strategy.

4.2 Drivers of the NDS

The NDS is driven by several key factors:

Analytics: The digitization and digitalization of various economic sectors in Mauritius will generate vast amounts of data, which will require advanced analytics capabilities. The more data is digitized, the greater the need for analytics to support informed decision-making, thereby creating value. Technologies such as machine learning (ML), deep learning (DL) and artificial intelligence (AI) will be essential to unlocking this potential. Effective data analytics will be a core driver of the NDS's goals and contribute to the growth of the digital economy, ultimately benefiting the broader economy.

Innovation: As Mauritius seeks to develop its economy and society, innovation driven by data will play a pivotal role. Data-driven innovation is a key source of growth in the digital age, as confirmed by international organizations such as the OECD. By leveraging big data, Mauritius can foster new industries, processes and products, creating a competitive advantage on the global stage. The country's pursuit of innovation will help shift its economy from one that is consumption-based to one that is more production-driven, enhancing its global competitiveness.

Digital Services: The implementation of digital services brings numerous benefits, including increased convenience, reduced operational costs and expanded access to public service delivery. These advantages will drive inclusive growth and sustainable development. At the heart of digital service delivery are high-quality data and digital intelligence. The push for seamless, end-to-end digital services will propel the NDS forward, contributing to the growth of the digital economy in Mauritius.

4.3 Data Management Unit/Data Management Office (DMU/DMO)

A Data Management Unit (DMU) will be established to lead the National Data Strategy, ensuring data is shared securely, used ethically, and creates value. The DMU will develop policies, ensure compliance with data protection laws and promote responsible data sharing and innovation. It will enhance data literacy across sectors and address challenges such as privacy, infrastructure and coordination. Through these efforts, the DMU will strengthen governance, boost economic growth and position Mauritius as a regional leader in data management and innovation. The DMU will evolve into a Data Management Office (DMO) to drive robust governance, privacy, security and interoperability.

4.4 Key roles and responsibilities of the DMU/ DMO

4.4.1 Institutional Structure for Data Governance

The DMU/DMO will frame the National Data Governance Framework (DGF) and provide essential central guidance and hold powers relating to oversight, enforcement and rule-making.

4.4.2 Enforcement Mechanisms to Incentivize Data Sharing

Both the DMU/DMO and governmental agencies are tasked with compliance and enforcement powers. Experiences from other jurisdictions highlight the importance of compliance mechanisms due to the importance of granular aspects of data governance (such as data classification and data quality standards) as well as carrot-and-stick incentive structures to boost data sharing in decentralized models.

The DMU/DMO may consider enforcement powers and grievance redressal mechanisms to encourage compliance. The DMU/DMO could have powers to enforce compliance, by either retaining the power to impose fines on government agencies that do not regularly share data that meets data quality standards, or by instituting a central grievance redressal officer so that users can get recourse at a central level for issues faced with sectoral datasets. Singapore's Public Sector Governance Act, 2018 and EU's Data Governance Act can be referred to for rules which set out a multi-level enforcement mechanism for data sharing (Box 2).

Box 2:

Compliance Frameworks in Singapore's Public Sector Governance Act, 2018 and EU's Data Governance Act, 2022

Singapore has established a robust framework for enforcing data sharing across government agencies through the Public Sector (Governance) Act 2018 (PSGA). The PSGA empowers the Minister to issue data sharing directions to public sector agencies for specific purposes, including, for data sharing. When a data sharing direction is given, agencies and their officers are legally authorized to share information under their control with agencies, overriding common law confidentiality obligations (though legal privilege and contractual obligations remain protected). The PSGA enforces compliance through strict fines (up to USD 5000), criminal penalties (imprisonment up to 2 years) for unauthorized disclosure or improper use of data.

The **European Union's Data Governance Act** (DGA), which entered into force on June 23, 2022, establishes a comprehensive framework to enhance trust in data sharing and strengthen mechanisms for increased data availability across the EU. The DGA focuses on facilitating the re-use of protected data held by public sector bodies, creating a notification and supervisory framework for trustworthy data intermediation services, and establishing voluntary registration for entities collecting data for altruistic purposes. Each EU Member State must appoint competent authorities to monitor compliance with the DGA, with powers to suspend non-compliant data sharing services, remove organizations from public registers, and impose financial penalties for violations. Additionally, individuals have the right to lodge a complaint when a competent authority or registered entity fails to fulfill its obligations under the DGA.

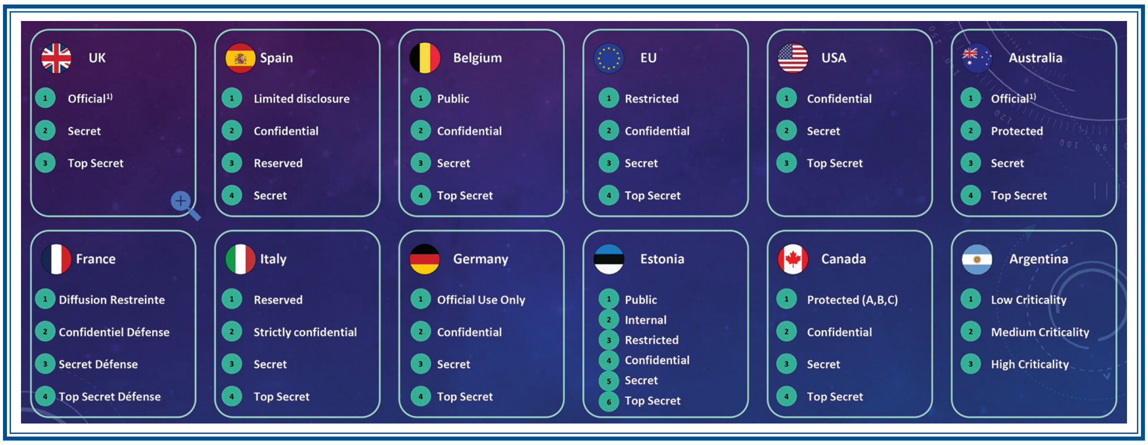
Source: *Singapore's Public Sector (Governance) Act, 2018 and the (EU) 2022/868 of the European Parliament and of the Council of 30 May*

Alternatively, incentives such as awards and additional budget may encourage compliance. Countries all over the world have adopted a range of approaches to encourage governmental agencies to share data. The DMU/DMO can consider adopting a "carrot and stick" approach, such as rewarding better data sharing, quality and classification with additional budget for IT infrastructure or training of officers. The NDS and DGF must also define budgetary allocations. For instance, countries like Denmark and Singapore, house their 'digitalization missions' within their Ministry of Finance, which enables these entities to financially incentivize digital reforms, such as data governance. These budgets can be utilized to reward good data governance practices, by, for example, prescribing a phased approach to policy adoption within a governmental agency leading to increase in infrastructural spending. Alternatively, Mauritius can replicate its existing 'Public Service Excellence Awards' to award officers who have pioneered data sharing efforts in different ministries.

4.4.3 Rules on Data Classification

The effectiveness of the DGF and NDS could be strengthened by objective and enforceable rules on data classification. Data governance frameworks have benefited from a principle-based approach, for example, by requiring governmental bodies to only impose non-discriminatory, transparent, proportionate and objectively justified conditions on sharing data. Data governance frameworks have mostly adopted 3-4 categories of data based on the severity of impact of unauthorized disclosure (Figure 6.0).

Data Classification policies have usually been adopted and enforced by central authorities, like the DMU/DMO. The DMU/DMO should collaborate with different governmental agencies while drafting the data classification regime, to ensure early alignment and to familiarize the DMU/DMO with sensitivity in different agencies relating to different types of data. Further, the data classification framework should be accompanied by an implementation guide which defines the different classification levels, the criteria for data to be classified, examples, and rationale of classification. Lastly, classification frameworks for data sharing should be harmonized with other classification frameworks for government cloud or data localization policies.



	1	2	3	4	5	6
UK	Official[1]	Secret	Top Secret			
Spain	Limited disclosure	Confidential	Reserved	Secret		
Belgium	Public	Confidential	Secret	Top Secret		
EU	Restricted	Confidential	Secret	Top Secret		
USA	Confidential	Secret	Top Secret			
Australia	Official[1]	Protected	Secret	Top Secret		
France	Diffusion Restreinte	Confidentiel Défense	Secret Défense	Top Secret Défense		
Italy	Reserved	Strictly confidential	Secret	Top Secret		
Germany	Official Use Only	Confidential	Secret	Top Secret		
Estonia	Public	Internal	Restricted	Confidential	Secret	Top Secret
Canada	Protected (A,B,C)	Confidential	Secret	Top Secret		
Argentina	Low Criticality	Medium Criticality	High Criticality			

Source: *Cloud Business Line, Workshop on Implementation of Lebanon's Digital Strategy, World Bank*

Figure 6.0: Overview of Data Classification frameworks adopted around the world

4.4.4 Strategic Leadership and Governance

In shaping the nation's digital future, efforts include setting comprehensive data policies and strategies, which involve defining national-level frameworks and best practices aligned with strategic goals such as economic development and digital transformation. This encompasses establishing clear standards for data ownership, stewardship, classification and access rights across all sectors. Furthermore, a central coordinating role across various ministries ensures a consistent and harmonized approach to data management throughout the government.

4.4.5 Technology and Innovation Enablement

Complementing these efforts, the work extends to providing guidance on national data infrastructure, encompassing cloud services, platforms and analytics tools. This also involves enabling the responsible use of data for advanced analytics, machine learning and artificial intelligence across government, while actively promoting innovation through collaboration with the private sector to create data-driven solutions.

4.4.6 Capacity Building and Culture

Furthermore, this involves leading initiatives for skills development to promote data literacy, governance and analytics. The objective is to foster a robust culture of data-driven decision-making within government agencies.

4.4.7 Technical Specifications for Data Quality and Interoperability

The DMU/DMO and the Ministry of Information Technology, Communication and Innovation may need to focus on the following aspects:

- Legal interoperability: Conduct "interoperability checks" for sectoral or geographical restrictions in the use and storage of data or restrictive data licensing conditions.[1] Further, rules pursuant to the DGF must ensure consistent data formats, data quality standards and mandate the use of a single intermediary (such as an API gateway, or 'Service Bus)[2] which enables transfer of data from individual ministries for consolidation and integration.
- Semantic interoperability refers to the ability of different information technology systems and software applications to automatically interpret the information exchanged meaningfully and accurately to produce useful results.[3] Semantic interoperability in the open data context relies on metadata standards and common vocabularies so that all agencies have a common understanding of data and its classification.
- Technical interoperability involves setting up infrastructure that allows machine-to-machine communication and uniform technology standards for software, physical hardware components, and systems and platforms.[4] Notable examples include the X-road data exchange layer deployed in over 20 countries.[5]
- Quality in the context of data sharing spans six dimensions: relevance, accuracy and reliability, timeliness and punctuality, accessibility and clarity, comparability, and coherence.[6] Ensuring interoperability and data quality go hand in hand, and the DMU/DMO could mandate a level of quality that all agencies must adhere to. Certain legislations require annual data quality audits, and the verification of completeness, accuracy and provenance of data held by agencies.[7] Therefore, ensuring data quality also involves continuous monitoring and evaluation to inculcate good practices in all agencies.

[1] Interoperability Frameworks, Practitioner's Guide, ID4D, https://id4d.worldbank.org/guide/interoperability-frameworks

[2] Interoperability: Towards a Data-Driven Public Sector, World Bank Group, (2022) 53, https://documents1.worldbank.org/curated/en/099550101092318102/pdf/P1694820242a9c041083900346bab0910eb.pdf (WB Interoperability Guide).

[3] WB Interoperability Guide, page 12.

[4] WB Interoperability Guide, page 17.

[5] https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/x-road-data-exchange-layer

[6] Supply and Quality of Data, Open Data Toolkit, World Bank Group, https://opendatatoolkit.worldbank.org/en/data/opendatatoolkit/supply

[7] The US Open Government Data Act, 2018, https://www.cio.gov/handbook/it-laws/ogda/

4.4.8 Creation of Data Warehouse

The DMU/DMO will strategically leverage a suite of advanced AI tools to enhance the utility of the national data warehouse operated by the GOC. These tools will be instrumental in performing sophisticated data manipulation tasks, including automated data cleaning and transformation, identification of complex patterns and correlations and the generation of predictive analytics. By applying AI-powered techniques, the DMU/DMO aims to unlock deeper, more actionable insights from the vast data resources within the warehouse, ultimately supporting evidence-based policymaking and improved public services.

The data warehouse will: -

- Store historical data, allowing AI tools to analyze trends over time and build more robust predictive models.
- Provide a framework for implementing strong data security measures and enforcing data governance policies, ensuring responsible and ethical use of national data, which is paramount for public trust and compliance with regulations.
- Be designed to be scalable and provide the performance needed to handle large volumes of data required for effective AI applications.

The relationship between AI tools and the warehouse is symbiotic:

- The warehouse provides the fuel (data) necessary for AI tools to learn, analyze, and generate insights. A well-structured and comprehensive data warehouse will propel an ethical use of AI applications. AI tools will provide the engine to extract value from the data stored in the warehouse. They will enable sophisticated analysis and the generation of actionable intelligence that would be impossible with traditional analytical methods alone.

5.0 NDS Governance and Ecosystem

5.0 NDS GOVERNANCE AND ECOSYSTEM

5.1 NDS Governance Structure

Governance of the NDS aims to provide effective leadership and coordination to ensure accountability and responsibility for its successful implementation. The NDS data ecosystem includes various stakeholders, systems and an enabling environment that empowers individuals, businesses and the public sector to safely and securely use data to pursue social and economic opportunities, in line with applicable standards, guidelines, regulations and laws.

5.1.1 NDS Governance Structure

Each organisation will have its own governance structure, which will provide sector-specific leadership, coordination and accountability. Every sector is expected to develop its own data strategy based on the national data governance model outlined in the NDS. The governance structure will include a Data Steering Committee (DSC) or Data Governance Committee (DGC) and data users, all working together to enforce standards, policies, principles and processes for effective data management and use. A data governance reporting mechanism will be implemented to support the effective execution of the NDS at the organizational level.

While ownership is distributed in each organisation who is responsible for its own data, the DMU/DMO as the central governance body ensures consistency in standards, compliance and metadata.

5.1.2 Lessons from International Experience

India's experience with its National Data Sharing and Accessibility Policy ('NDSAP'), 2012 demonstrates the pitfalls of excessive decentralization. Open data platforms and sharing of non-personal data in India is governed by the National Data Sharing and Accessibility Policy ('NDSAP'), 2012. The NDSAP empowered individual ministries and agencies to declare which datasets were 'non-shareable'. In the absence of uniform, harmonized procedures for collecting, curating and sharing data, datasets available on the open data platform were found to exhibit shortcomings, including non-machine-readable formats, inconsistent terminology, and incomplete datasets. In addition to these issues, the Indian Ministry of Electronics and Information Technology ('MEITY') also identified lack of enforcement mechanisms for monitoring data sharing efforts, standard classification for identification of high value datasets, capacity building strategy for officers, as crucial gaps.

MEITY released the Draft National Data Governance Framework Policy ('NDGFP') in May 2022 to address these shortcomings which provided for an India Data Management Office ('IDMO') to standardize data management, enforce guidelines, and oversee compliance. India's evolution toward more centralized governance underscores the importance of centralized rulemaking for effective data governance. Similarly, experts have noted that data sharing in the US's federated approach could have also been strengthened with more central guidance and oversight (Box 1).

Box 1:

United States: The Need of Central Oversight in a Federated Model

Launched in 2018, the Federal Data Strategy put forward a transparent and clear ten-year vision and action plan for the U.S. government on public data management and called for the release of annual action plans for agencies to identify "practice-related" milestones towards its implementation. Action plans were developed in close collaboration with an interagency and interdisciplinary working groups and a Chief Data Officer Executive Committee (CDO Council). The CDO Council was established alongside the FDS in 2018 with the ambition of establishing "government-wide practices for the management, use, protection, dissemination and generation of data." Chief Data Officers (CDOs) serve across agencies and are positioned to regularly engage with agency leadership. CDOs were required to be nonpolitical appointee employees within the agency. As of March 2022, membership of the CDO Council included more than 90 federal agencies.

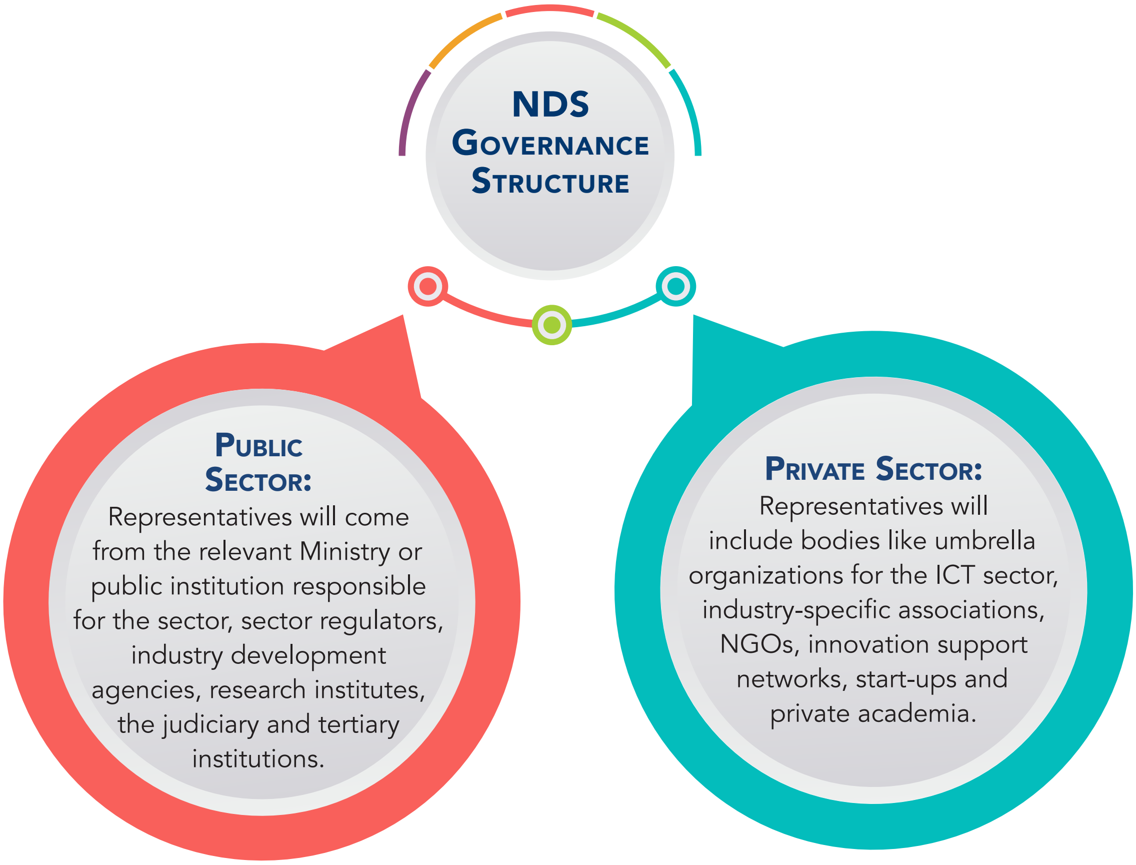
An independent non-profit review revealed that the FDS action plans were too generic and high-level for agency use, leaving CDOs without clear guidance and support in implementing the strategy. Plans were also not linked to executive-level policy priorities, including emergency health response or immigration, or agency-level mission outcomes. Further, no federal entity had been designated as an oversight and governance body for the FDS, when bodies existed that could have been repurposed towards such a task (e.g. OMB's Federal Data Policy Committee).

Source: *Unlocking the Value of Public Data: Foundations for Effective Data Governance in Egypt, Egypt Digitalization Programmatic TA, World Bank (Draft for Discussion)*

The NDS and DGF could provide more powers to the DMU/DMO relating to oversight, enforcement and rulemaking. This mandate should be strengthened by adding monitoring and enforcement provisions and the power to make rules on classification of datasets, data quality, interoperability, high value datasets. This centralized governance approach must also account for Mauritius unique administrative context. Unlike larger, more populous nations such as the United States or India—where decentralized implementation is often necessary—Mauritius compact governance structure may allow for greater delegation of operational responsibilities to individual ministries while maintaining cohesive central oversight.

5.1.3 Composition of the NDS Governance Structure

The governance structure of each sector will comprise representatives from both the public and private sectors. The composition will be as follows:



NDS Governance Structure

Public Sector: Representatives will come from the relevant Ministry or public institution responsible for the sector, sector regulators, industry development agencies, research institutes, the judiciary and tertiary institutions.

Private Sector: Representatives will include bodies like umbrella organizations for the ICT sector, industry-specific associations, NGOs, innovation support networks, start-ups and private academia.

5.1.4 Functions of the NDS Governance Structure

The functions of the governance structure in each sector will include:

1. Providing strategic direction and coordinating sector-specific operational activities.
2. Facilitating the development of an integrated data platform for the sector.
3. Creating business models and implementation plans for data access and use.
4. Promoting and ensuring adequate investments in digital infrastructure.
5. Coordinating the development of data policies, frameworks and standards.
6. Performing any other functions as assigned by relevant bodies.

A review mechanism to maintain the National Data Strategy as a dynamic, living framework will be implemented to ensure sustained relevance, responsiveness and adaptability to evolving data ecosystems.

5.2 NDS Ecosystem

To promote dialogue and feedback among stakeholders, the NDS proposes a multi-stakeholder ecosystem in Mauritius, including:

1. Data owners or subjects.
2. Data users (individuals using data-driven services).
3. Data controllers and processors.
4. Data-driven service providers and start-ups.
5. Policymakers, planners and practitioners in data.
6. International organizations, development partners and foreign data users.
7. Industry players and academia involved in data-driven economic development.
8. Members of the NDS governance structure.

Each sector will have its own NDS ecosystem, with leadership responsible for coordinating activities. There will also be an overarching NDS ecosystem for Mauritius.

5.2.1 Responsibilities of the Sector NDS Ecosystem

The sector-specific NDS ecosystem will:

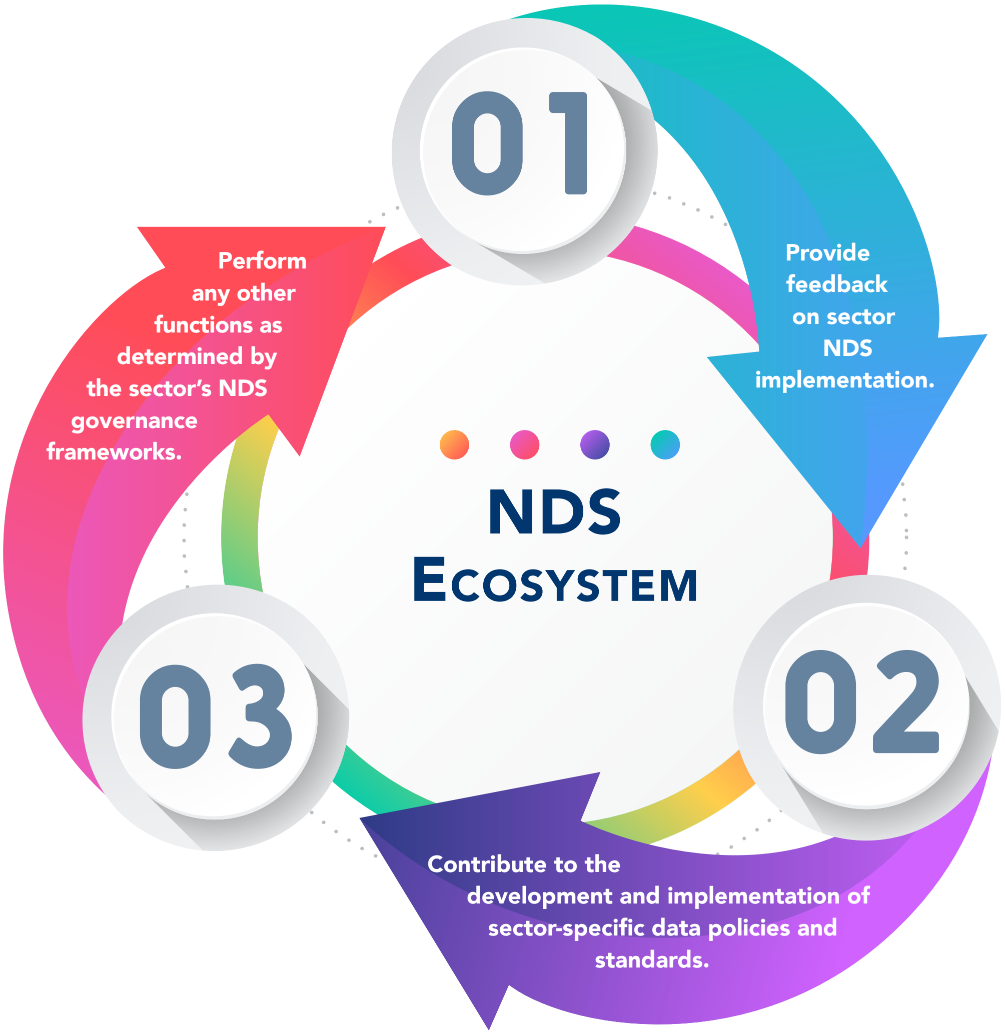
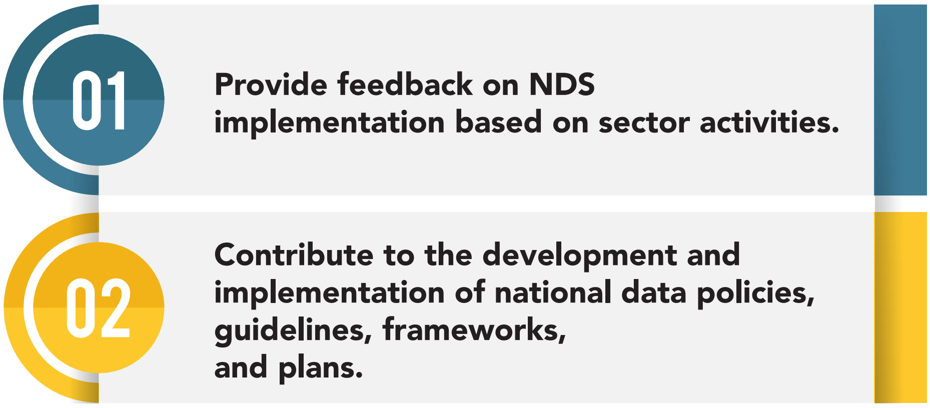

01
Provide feedback on sector NDS implementation.
02
Contribute to the development and implementation of sector-specific data policies and standards.
03
Perform any other functions as determined by the sector's NDS governance frameworks.
NDS
Ecosystem

Figure 7.0: NDS Ecosystem

5.2.2 Responsibilities of the Overall NDS Ecosystem

The overall NDS ecosystem will:



Provide feedback on NDS implementation based on sector activities.

Contribute to the development and implementation of national data policies, guidelines, frameworks, and plans.

Figure 8.0: Responsibilities of the Overall NDS Ecosystem

5.3 Ministry of Information Technology, Communication and Innovation (MITCI)

The Ministry of Information Technology, Communication and Innovation (MITCI) plays a vital role in promoting the national data strategy by developing policies, fostering digital infrastructure and ensuring data governance. MITCI works to establish data standards, enhance privacy and security and encourage the use of data in decision-making across public and private sectors. It supports the creation of open data platforms, encourages public-private partnerships and promotes digital literacy through training programs. MITCI also facilitates innovation by collaborating with businesses and academic institutions, as well as aligning Mauritius strategy with international best practices. MITCI's efforts contribute to a data-driven economy, improved public services and better governance, ultimately positioning Mauritius as a leader in digital transformation. This strategy is aligned with the blueprint of MITCI.

6.0 References

https://www.google.mu/search?q=national+data+strategy+template&client=safari&sca_esv=3ec8625b255dccb3&channel=iphone_bm&ei=4LPJZ9uGCbL97_UP1564gAg&oq=national+data+strategy+tem&gs_p=EhNtb2JpbGUtZ3dzLXdpei1zZXJwIhpuYXRpb25hbCwBkYXRhIHN0cmF0ZWd5IHRlbSoCCAAyBxAhGKABGAoyBxAhGKABGAoyBRAhGJ8FMgUQIRifBUjxO1CXClikMXAFeAGQAQCYAbwCoAGHD6oBBTItNi4xuAEByAEA-AEBmAIMoALyD8ICChAAGLADGNYEGEfCAgUQABiABMICBhAAGBYYHsICBRAhGKABwgILEAAYgAQYhgMYigWYAwCIBgGQBgiSBwc1LjAuNi4xoAfjHA&sclient=mobile-gws-wiz-serp

https://www.npc.qa/en/nationaldataprogram/Documents/EnNationalDataPolicy.pdf

https://nitda.gov.ng/wp-content/uploads/2022/11/Final-Draft-National-Data-Strategy.pdf

Annex 1: Model Data Governance Framework

Annex 2: Data Sharing Policy Template

Annex 3: Data Sharing Protocol Template

Annex 4: Data Retention Policy

Designed and printed by The Government Printing Department - 2026