NATIONAL DATA GOVERNANCE FRAMEWORK

July 2025

National Statistics Bureau
Royal Government of Bhutan

NATIONAL DATA GOVERNANCE FRAMEWORK

July 2025

Printed in Bhutan.
ISBN 978-99980-61-09-5

NDGF Technical Team:
1. Birkha Gurung, NSB;
2. Thinley Dorji, NSB;
3. Chimi Dem, NSB;
4. Yangchen Choden, NSB;
5. Yamuna Powdel, NSB;
6. Gyeltshen, OCASC;
7. Tandin Zangmo, OCASC;
8. Tshering, GovTech;
9. Dechen Dema, GovTech;
10. Radhika Orari, GovTech;
11. Tenzin Deki, GovTech;
12. Tenzin Selden, OAG; and
13. Kinley Pelzang, BICMA.

National Statistics Bureau
Royal Government of Bhutan
PO Box No 338
Thimphu, Bhutan
Tel: +975 2 333296, +975 2 335848
Fax: +975 2 323069
www.nsb.gov.bt

CONTENTS

FOREWORD

I am pleased to present the National Data Governance Framework (NDGF) of Bhutan, which was officially approved and came into effect on 11th July 2025. This landmark document represents a critical reform in the way data is governed, reinforcing our commitment for evidenced-based planning and policy formulation.

The NDGF addresses challenges identified through the National Data Governance Baseline Report 2024, including fragmented legal structures, inconsistent data practices, lack of clear institutional roles, and inadequate safeguards for data privacy and protection. It introduces a unified and structured approach to ensure that data is treated as a strategic national asset, governed by robust policies, ethical standards, and strong institutional accountability.

Anchored on five foundational pillars - Data Classifications and Standards, Data Sharing and Exchange, Data Security and Protection, Data Privacy and Ethics, and Data Infrastructure - the Framework provides comprehensive guidance to all entities engaged in data collection, processing, usage, and dissemination. It establishes mechanisms to ensure data standards, classification based on risk and impact, protection of personal data, and the ethical use of data in line with global best practices and Bhutanese values.

The establishment of the National Data Governance Committee (NDGC) will provide high-level oversight to ensure consistency, compliance, and continuous improvement in data governance. The National Statistics Bureau (NSB), as the lead implementing agency, is entrusted with coordinating implementation, building capacity, conducting sensitization, and engaging all stakeholders in this national effort.

In an era where data drives innovation, governance, and service delivery, the NDGF will serve as an enabling instrument for evidence-based decision-making, efficient public administration, and the responsible use of data for the collective benefit of the Bhutanese people.

I commend the collaborative efforts of the National Statistics Bureau, GovTech Agency, and all stakeholders who contributed to the development of this Framework. I urge all entities to embrace its principles and provisions, ensuring that data is used securely, ethically, and effectively in the service of national progress.

(Kesang Deki)
Cabinet Secretary

MESSAGE

The development and approval of the National Data Governance Framework (NDGF) marks a significant milestone in Bhutan's journey toward a well-coordinated, ethical, and secure data ecosystem. In an era defined by digital transformation, data is the core asset for planning, policymaking, innovation, and public service delivery.

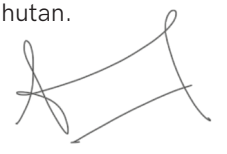
The NDGF, approved on 11th July 2025, is a timely response to systemic challenges identified through the National Data Governance Baseline Report 2024, including fragmented data management practices, lack of institutional clarity, and weak data privacy and protection mechanisms. The Framework establishes a coherent and inclusive national approach, anchored in shared principles and strategic pillars. Its implementation and monitoring will be carried out through a structured set of activities, categorized into short-, medium-, and long-term phases.

Anchored in five foundational pillars, the NDGF aims to strengthen data governance by promoting accountability, effectiveness, and inclusiveness. It focuses on streamlining data management systems, establishing national data standards, enhancing interoperability and data sharing, ensuring data security and privacy, upholding ethical data use, and improving data infrastructure.

The framework aims to establish a robust, accountable, and inclusive data governance ecosystem in Bhutan. Its key initiatives include operationalizing the framework, instituting a National Data Governance Committee, developing and revising data management guidelines, strengthening regulatory mechanisms for data protection and cybersecurity, and enhancing data infrastructure and interoperability. Implementation will be driven through coordinated efforts among key agencies, led by the NSB, GovTech, and the Office of the Prime Minister and Cabinet.

We remain fully committed to implementing the NDGF and fostering a data governance culture grounded in accountability, inclusiveness, and effectiveness to ensure secure, ethical, and reliable data use in support of Bhutan's vision of becoming a Developed Bhutan.

(Sonam Tenzin)
Director General, NSB



(Jigme Tenzing)
Secretary, GovTech Agency

ACKNOWLEDGEMENT

The development of the NDGF would not have been possible without the contributions of many individuals and institutions. We express our deep appreciation to the representatives from government ministries, agencies, non-governmental organizations, corporate and private sectors who actively participated in the stakeholder consultations. Your diverse perspectives and inputs were essential in shaping a framework that is both inclusive and implementable.

We also sincerely thank Mr. Sebastian Foo, World Bank Expert, for his unwavering technical support throughout the drafting and consultation process. His guidance has helped align the NDGF with global standards while reflecting Bhutan's unique national priorities.

We express our sincere gratitude to the United Nations Population Fund (UNFPA) Country Office for the financial support, which has been instrumental in both the development and implementation of the NDGF.

We are deeply grateful to the Hon'ble Cabinet Secretary, Office of the Prime Minister and Cabinet, for her unwavering oversight and invaluable professional support throughout the development and approval of the NDGF. We also extend our heartfelt thanks to the Director, Office of the Cabinet Affairs and Strategic Coordination, Office of the Prime Minister and Cabinet, for strategic guidance, and coordination in this process.

DEFINITIONS

- **Data** are facts, figures, or details collected for analysis, reference, or decision-making.
- **Data classification** is categorizing, and labelling data based on its impact**,** purpose, and access requirements.
- **Data classification impact assessment** is the level of confidentiality and protection required for data based on its potential impact if disclosed without authorization.
- **Data infrastructure** is the combination of physical systems, digital technologies, and institutional frameworks—including laws, policies, and standards—that enable the secure, efficient, and coordinated management of data across its entire lifecycle.
- **Data management** is the coordinated activities and policies that ensure the effective handling of data throughout its lifecycle, encompassing data collection, storage, sharing, and protection, to support informed decision-making and service delivery.
- **Data producer(s)** are organizations or individuals responsible for the data collection, compilation, and validation, ensuring consistency, accuracy, and compliance with relevant standards.
- **Data security by design and default** is an approach where cybersecurity threats to the data are considered at the initial design stage and throughout the data management lifecycle to ensure all PIIs and data are protected.
- **Data standards** are a set of structured rules and guidelines that ensure the consistency and accuracy of data and management of data across systems and organizations. These include elements such as naming conventions, standardized data formats, measurement units, and validation criteria.
- **Data subject(s)** is an individual(s) whose personal data is used.

- **Data at rest** refers to data stored on a storage medium such as a hard disk drive, solidstate drive, optical disc, or backup media, and is not actively moving through networks or being processed.
- **Data in transit** refers to data that is actively moving from one location to another, such as across the internet or through a private network.
- **Data in use** refers to data that is being processed by applications, endpoints, or systems, for example, data in system memory or CPU registers.
- **Entity(ies)** includes government, corporate, private agencies, and individuals who are engaged in managing data.
- **Government purposes** are any activities for evidenced-based decision-making, including the formulation of policies, plans, any sectoral strategies, initiatives or dissemination of official statistics while strictly ensuring that individuals cannot be identified.
- **Internet of Things (IoTs)** are a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data.
- **Interoperability** is the ability of diverse systems, databases, or organizations to integrate, exchange and utilize data seamlessly and effectively.
- **Metadata** is the descriptive information about data that describes statistical data and statistical processes in a standardized way by providing information on data sources, methods, definitions, classifications, and data quality.
- The **National Statistical System** is the ensemble of institutions and stakeholders that are responsible for the collection, analysis, dissemination, and coordination of official statistics in a country.
- **Official statistics** are data and information systematically collected, processed, and disseminated by national statistics offices and other authorized organizations to support decision-making, policymaking, and public understanding based on the principle of official statistics.

- **Personal data or Personally Identifiable Information (PII),** as defined under the Information, Communications, and Media Act (ICM) 2018, is any data or information which relates to a person who can be identified from that data or other information, which is in the possession of, or is likely to come into the possession of, an ICT service provider or ICT facility provider, and includes any expression of opinion about that person and any indication of the intentions of the ICT service provider or ICT facility provider or any other person in respect of that person.
- **The Fundamental Principles of Official Statistics** refers to the set of principles adopted by the United Nations General Assembly under Resolution 68/261 on 29 January 2014.
- **Pseudonymization** refers to a data protection technique where PIIs are replaced with a unique identifier that allows for the re-identification of the original data if necessary.
- **Public Use File (PUF)** refers to a dataset prepared and disseminated by entity(ies) in which all PIIs have been removed or anonymized to ensure privacy protection, allowing the data to be accessed and used freely by researchers, policymakers, and the public for statistical, academic, and policy analysis purposes.
- **Quantum threats** refers to the risks that future quantum computers could break today's data security methods, making sensitive and restricted data vulnerable to being accessed, stolen, or distorted with.
- **Sector Level** refers to ministries, departments, and agencies.
- **Sectoral regulatory body** refers to a governmental or independent authority vested with the mandate to implement and enforce responsibilities as prescribed by relevant laws/regulations/ statutory provisions within its sector.
- **Vendors** are an external organization or individual hired to provide services or products, which may involve access to **restricted data,** and is required to follow data protection and security rules.

ACRONYMS

AI	Artificial Intelligence
ARC	Advance Release Calendar
BSDS	Bhutan Statistical Database System
BSQAF	Bhutan Statistics Quality Assurance Framework
BtCIRT	Bhutan Cyber Incident Response Team
DGC	Data Governance Committee
DIN	Data Inventory
DMG	Data Management Guide
FYP	Five-Year Plan
GDC	Government Data Centre
GDDS	General Data Dissemination System
GovTech	Government Technology
ICM	Information, Communication and Media
ICT	Information and Communication Technology
IMF	International Monetary Fund
IoT	Internet of Things
MIS	Management Information Systems
NDGF	National Data Governance Framework
NSB	National Statistics Bureau
NSDS	National Strategy for the Development of Statistics
NSS	National Statistical System
PII	Personally Identifiable Information
PUF	Public Use File
RGoB	Royal Government of Bhutan
RMA	Royal Monetary Authority of Bhutan
SDG	Sustainable Development Goals
SDMX	Statistical Data and Metadata Exchange
UNDESA	United Nations Department of Economic and Social Affairs
UNESCAP	United Nations Economic and Social Council for Asia and Pacific

BACKGROUND

The development of the National Data Governance Framework stems from the absence of a clearly defined institutional mandate on data governance in Bhutan. During the formulation of the 13th Five-Year Plan (FYP), the Office of the Prime Minister and Cabinet directed the National Statistics Bureau (NSB) and the GovTech Agency to engage in consultations to clarify their respective roles and responsibilities in this area. Following a series of discussions, a mutual agreement was reached between NSB and GovTech to delineate roles and establish a coordinated approach to data governance.

As Bhutan undergoes a significant digital transformation, data serves as a vital asset for national progress. In this context, the establishment of the National Data Governance Framework (NDGF) represents a timely initiative aimed at addressing critical gaps in the country's data ecosystem. The Bhutan National Data Governance Baseline Report 2024 hasunderscored a range of systemic challenges, including fragmented legal and policy frameworks, inconsistent data management practices, unclear institutional roles, and inadequate technical infrastructure.

Moreover, the report highlights persistent gaps in key areas such as data security and privacy, data sharing mechanisms, digital identity management, the establishment of specialized data units, standardized operational processes, and the availability of skilled personnel across government agencies. These challenges significantly constrain Bhutan's ability to fully leverage data for sustainable development, improve public service delivery, and support evidence-based policymaking.

In the absence of a cohesive and enforceable data governance structure, the effective utilization and protection of data remain at risk. The NDGF offers a foundational step toward ensuring that data is managed securely, ethically, and responsibly across entities. To build on this positive momentum, the introduction of a comprehensive National Data Policy is imperative. By establishing a robust and integrated data governance ecosystem underpinned by legal and regulatory support, Bhutan will be better positioned to unlock the full potential of data as a strategic resource for national progress.

RATIONALE

This NDGF will address these critical gaps by providing a clear and unified approach to data governance. It will establish consistent policies, standards, and procedures for data quality, interoperability, data privacy and data protection, while ensuring transparency and accountability across all sectors. The framework will promote effective coordination among entities, enhance institutional capacity, and improve data literacy in the country. It will ensure that data governance systems are resilient, inclusive, and adaptable to emerging challenges. The successful implementation of this framework will maximize the value of its data assets and foster innovation.

1. PRELIMINARY

This framework shall support the implementation of, but not limited to, the Executive Order of 2006 to NSB, the Information, Communications and Media (ICM) Act of Bhutan 2018 and National Digital Identity Act of Bhutan 2023.

1.1 TITLE, COMMENCEMENT, AND APPLICATION

This framework shall be called the National Data Governance Framework of Bhutan 2025, hereinafter referred to as the NDGF 2025.

This framework shall be applicable to all data producers, custodians, users, and any other entity(ies) engaged in the collection, storage, sharing, and usage of data.

This framework shall come into effect from 11th July 2025.

1.2 OBJECTIVES

The core objectives of the NDGF are based on the principles of data accountability, effectiveness and inclusiveness to:

a. Streamline policies, institutions, processes, and people related to overall data management in the NSS;
b. Establish national data standards and classification to ensure consistency and comparability of data;
c. Enhance data sharing and interoperability to facilitate secure and seamless data exchange across entities;
d. Ensure data security and protection to strengthen safeguards against unauthorized access and misuse;
e. Promote data privacy and ethics to uphold ethical use of data; and
f. Strengthen data infrastructure to support efficient storage, processing and accessibility.

2. PILLARS

The NDGF is adopted based on the broad five pillars of the UNDESA's Data Governance Framework.

2.1 PILLAR ONE: DATA CLASSIFICATIONS AND STANDARDS

2.1.1 Data producers shall identify and categorize data based on impact assessments as provided in **Table I**. All data shall be classified as follows:

a. **Public data** are those data that are open and can be disclosed to the public without any restrictions. This type of data requires no/minimal security controls when used or stored;

b. **Internal data** are those data that are meant only for internal use within the organization. Access to internal data may have associated approvals and/or costs depending upon a formalized arrangement between data producers and users; and

c. **Restricted data** are those data that can be shared only among authorised agencies. The authorized agencies shall be determined by the data producing agencies.

Table I: Categories and levels of data classification impact assessment[1]

Impact category			Impact levels		
Impact main category	Impact subcategory	Considerations	High impact = Restricted data	Low impact following removal pseudonymization/ anonymization of sensitive information = Internal data	No impact = Public data
National interest	National security	Would the disclosure of this data threaten the country's security or facilitate the commission of serious crime?	High impact on the country's security.	No impact on the country's security after filtering the sensitive information.	No impact on the country's security.
	Diplomatic relations	Would the disclosure of this data harm the country's diplomatic relationships?	High impact on the country's diplomatic relationships.	No impact on the country's diplomatic relationships after filtering the sensitive information.	No impact on the country's diplomatic relationships.
	National economy	Would the disclosure of this data cause economic losses at the national level?	Long-term impact on the country's economy.	No impact on the country's economy after filtering the sensitive information.	No impact on the country's economy
Entity(ies) activities	Profits of corporate and private entities	Would the disclosure of this data lead to financial loss of corporate and private entities?	Adverse impact on the profits of corporate and private entities.	Low impact on the profits of corporate and private entities after filtering the sensitive information.	No impact on the corporate and private entities' profits
Individuals	Individuals' health/safety	Would the disclosure of this data hamper the health and safety of individuals?	High impact on the health and safety of the individuals.	Low impact on the health and safety of individuals after filtering the sensitive information.	No impact on the individuals' health and safety.
	Privacy	Would the disclosure of this data violate the individuals' privacy?	Disclosure of PIIs.	Low impact on the individuals' privacy after filtering the sensitive information.	No impact on the individuals' privacy.

1 Based on the Standard Operating Procedure for Geographic Information Categorization & Identification of Single Source of Truth (SSOT)

2.1.2 Data producers shall develop, maintain, and update comprehensive metadata that includes detailed descriptions of variables and/or indicators, data structure, format, representation, source, and update frequency.

2.1.3 Entity(ies) shall adhere to national data standards, including but not limited to the Standard Industrial Classification, Standard Occupational Classification, Standard Geographic Codes, and any other sectoral or cross-cutting standards.

2.1.4 All data standards shall be regularly reviewed and updated to align with the evolving requirements as determined by NSB.

2.1.5 Entity(ies) shall ensure that data collected, processed, and disseminated is fit for its intended purpose, contextually relevant, and sufficiently comprehensive to meet the data needs of intended users.

2.2 PILLAR TWO: DATA SHARING AND EXCHANGE

2.2.1 Data producers shall classify and share data with other agencies or individuals based on the data impact classification (clause 2.1.1).

2.2.2 Data producers shall follow Bhutan Statistical Quality Assurance Framework (BSQAF), which may be updated from time to time.

2.2.3 Entity(ies) shall share data (excluding data classified as 'public') to authorised/ approved entities for the sole purpose of their work /on the named project/research and shall not be shared with any third party wholly or partially.

2.2.4 Entity(ies) shall not disclose PIIs, unless required by law or as specified otherwise.

2.2.5 Entity(ies) shall ensure data is shared through a formalized data sharing arrangement (or as approved by an authorized person). The arrangement shall include the following:

a. Information on the data producers;
b. Information on the data users;
c. Data sharing objectives, mechanisms and timeframe;
d. Metadata details;
e. Basis for sharing PIIs, if applicable;
f. Non-disclosure of any PIIs through NDAs, if applicable;
g. Emphasize proper management; and
h. Any other obligations resulting from enabling legislation of either party.

2.2.6 Entity(ies) shall provide data truthfully without intentional misinterpretation within a specified timeframe.

2.3 PILLAR THREE: DATA SECURITY AND PROTECTION

2.3.1 The NSB shall lead the development of data privacy and protection regulation in collaboration with GovTech Agency and relevant stakeholders.

2.3.2 In absence of a national regulations for data privacy and protection, entities shall implement the following minimum requirement:

a. Maintain a Personal Data Inventory documenting all personal data processed for service delivery;
b. Ensure the security of data throughout its lifecycle to prevent unauthorized access, misuse, or loss, particularly for personal and restricted data;
c. Encrypt sensitive data at rest, in transit, and in use;
d. Specify strategies for data retention, audit trails, and deletion;
e. Enforce multiple factor authentication for all systems storing user data with stringent access control and auditing;
f. Develop protocols for breach detection, reporting, and response;
g. Shall notify the Sectoral Regulatory Body within 72 hours of becoming aware of a data breach;
h. Refrain from unapproved or illegal use of restricted data, including PIIs;
i. Conduct regular risk assessment;
j. Evaluate and enforce data security standards for third-party vendors and partners, with contractual obligations for compliance;
k. Ensure AI systems align with legal and user safety standards in their data usage;
l. Prepare for emerging disruptive technologies and threats; and
m. Develop and ensure data security in software development lifecycle and network infrastructure by design and default.

2.4 PILLAR FOUR: DATA PRIVACY AND ETHICS

2.4.1 Entity(ies) shall ensure PIIs and other restricted data are managed ethically, and in compliance with the ICM Act of Bhutan 2018, the Fundamental Principles of Official Statistics, and/or other relevant acts/policies/rules and regulations.

2.4.2 Entity(ies) shall ensure archival or deletion of data, including PIIs, when it is no longer necessary or lawful.

2.4.3 Entity(ies) shall avoid collecting PIIs if it is not required.

2.4.4 Entity(ies) shall provide access to PIIs to only those authorised personnel, adhering to strict security controls throughout its lifecycle.

2.4.5 Entity(ies) shall obtain voluntary and informed consent from data subjects for data collection, processing, and sharing.

2.4.6 In instances of crises or emergencies, data collection, processing, and sharing may proceed without explicit consent, provided that:

a. The data usage aligns with applicable laws and emergency provisions;
b. The data processing is strictly limited to the scope required for crisis management and does not extend beyond the emergency situation;
c. Data is only accessible to authorized personnel with strict controls and NDA to prevent misuse; and
d. Once the emergency subsides, affected individuals should be notified, and data should either be anonymized or returned under normal governance protocols.

2.4.7 Entity(ies) shall either pseudonymize or anonymize PIIs as required for data sharing, processing and usage.

2.4.8 Entity(ies) shall include data ethics review mechanisms into their data security and protection protocols (in line with 2.3.2).

2.4.9 Entity(ies) shall ensure professional ethics on the methods and procedures throughout the data management lifecycle.

2.4.10 Entity(ies) shall ensure that the data produced is inclusive and unbiased.

2.5 PILLAR FIVE: DATA INFRASTRUCTURE

2.5.1 Entity(ies) shall ensure a robust ICT infrastructure to provide secure, reliable and scalable data.

2.5.2 The RGoB shall ensure all its ICT infrastructure standards as prescribed under the GEAF.

2.5.3 All government data exchange shall be routed through the National Data Exchange Platform of the RGoB.

2.5.4 Entity(ies) outside of the RGoB shall develop and adopt standardized Application Programming Interface (APIs) to enable seamless data exchange, system interoperability, and integration across platforms.

2.5.5 The RGoB shall ensure all critical information infrastructure is managed as per the Critical Information Infrastructure Protection Regulations.

2.5.6 Entity(ies) shall ensure the protection of all data sources, including but not limited to IoT devices, analytics software, and AI.

2.5.7 The GovTech Agency shall develop and implement National Cloud Strategy to support the NDGF.

2.5.8 For development, production, and use of official statistics, it shall be guided by the National Strategy for the Development of Statistics (NSDS).

3. GOVERNANCE STRUCTURE

3.1 There shall be a National Data Governance Committee (NDGC) as the apex body responsible for overseeing the implementation of the National Data Governance Framework (NDGF).

3.2 The NDGC shall comprise of the following members:

a. The Cabinet Secretary, Chairperson;
b. The Secretary, Government Technology Agency, Member;
c. The Director/Director General, National Statistics Bureau, Member Secretary; and
d. Any other relevant representatives as required.

3.3 The NDGC shall be responsible for defining, reviewing and approving national data standards, classifications, protection and privacy measures, ethical guidelines, infrastructure and/or any other key aspects of the NDGF.

4. ANNEXURE I: IMPLEMENTATION, MONITORING AND EVALUATION

Sl.#	Activity	Timeline	Lead Agency(ies)	Collaborating Agencies	Itemised cost activities	Budget (M. Nu.)
1	Develop and implement the NDGF.	Short term (Immediate next step)	NSB	Cabinet Secretariat, GovTech Agency, BICMA & other relevant entities	• Advocacy workshops • Layout and design	1.00
2	Institute the National Data Governance Committee.		NSB & Cabinet Secretariat (national level)	GovTech and relevant agencies	• Conduct meetings	0.25
3	Develop and implement Critical Information Infrastructure Protection Regulation/ Guideline		GovTech	GovTech and relevant stakeholders	• Stakeholder consultations • Consultancy services	1.10
4	Review the Data Management Guide 2023.		1. NSB. 2. Sectors-Specific based on the Data Management Guideline	GovTech Agency	• Stakeholder consultations • Layout and design	0.50
5	Conduct Data Maturity Assessment for priority sectors (MoAL, DoTR, MoESD)		NSB	GovTech and relevant agencies	• Meetings and consultations • Assessment of the maturity level • Providing recommendation	1.50
6	Capacity building	Short term and medium term	NSB & GovTech Agency	Relevant entities	• Workshops and trainings	2.50
7	Develop Data Privacy and Protection Regulation/Guideline	Medium term	NSB	1. GovTech 2. BICMA 3. RBP 4. OAG 5. MoHA	• Stakeholder consultations • Consultant hire • Layout and design	2.50
8	Develop, review and update relevant national data standards.		1. NSB-Statistics 2. GovTech-Systems & Cyber Security 3. Sector - Sector specific (RMA for finance, MoH for health etc.,)	All relevant entities	• Stakeholder consultations • Layout and design	1.50
9	Review and update the National Data Classification.		1. NSB & Cabinet Secretariat (national level) 2. Sector- Sector specific based on National Data Classification	GovTech Agency, BICMA, OAG & other relevant entities	• Stakeholder consultations • Layout and design	1.50
10	Develop and Implement the Government Enterprise Architecture		GovTech Agency	NSB, BICMA and other relevant entities	• Stakeholder consultations	0.80

Sl.#	Activity	Timeline	Lead Agency(ies)	Collaborating Agencies	Itemised cost activities	Budget (M. Nu.)
11	Develop and implement National Cyber Security Standards and guidelines.	Medium term	GovTech Agency	BICMA and other relevant entities	• Stakeholder consultations • Consultancy services	5.00
12	Enhance Bhutan Statistical Database System Strengthen Data Sharing Platforms	Medium term	NSB GovTech Agency	Relevant entities	• Hire private firm to develop • Rollout the BSDS • Rollout data sharing platforms	3.50
13	Develop and propose for National Data Governance Policy	Long-term	Cabinet Secretariat, NSB & GovTech Agency	BICMA, RMA, OAG, RBP, Ministries, private, corporate sectors and relevant entities.	• Stakeholder consultations • Consultancy services	2.50
14	Monitoring and evaluation	Periodic	1. OPMC (National level) 2. NSB (National level) 3. GovTech Agency (National Level) Sectoral regulators (Sector level)	Relevant entities	Conduct periodic M&E workshops	0.50
					Total	24.65

* Timeline - Short term: 1-2 years; Medium term: 3-5 years; Long term: 6-10 years

5. ANNEXURE II: RISK ASSESSMENT

Risk type	Potential issue	Mitigation	Response
Data security	Unauthorized access, cyberattacks, and data breaches.	Implement encryption, access controls, and multi-factor authentication.	Conduct regular security audits, risk assessments, and breach response plans.
Data privacy, ethics & compliance	Violations of data protection laws, unethical data usage.	Align strategies/ guidelines/rules/ regulations policies with national and global privacy frameworks.	Establish real-time compliance tracking and reporting mechanisms.
Operational effectiveness	Data inconsistencies, integration failures, and governance misalignment.	Standardize data collection and dissemination formats, develop and enforce metadata format.	Conduct routine data audits, issue resolution mechanisms.
Technical capacity	Infrastructure downtimes, interoperability failures, and emerging threats.	Enhance system resilience, adopt future-proof security strategies	Develop early-warning mechanisms and disaster recovery protocols.
ICM Act 2018	Conflicting personal information provisions for sharing and storage	Relevant provisions in the NDGF	To seek consent from the data subjects.
NDI Act 2023	Conflicting personal information provisions for sharing and storage	Relevant provisions in the NDGF	Provide disclaimer on the consent form.

6. REFERENCES

1. **Atlan, n.d.** *Data Governance Framework: Examples, Template & How to Create*. [online] Available at: https://atlan.com/data-governanceframework/? ref=/know/data-governance/for-ai/#the-three-pillars-of-any-datagovernance-framework [Accessed 5 Jan. 2025].

2. **Atlan, n.d.** *Data Governance Standards*. [online] Available at: https://atlan.com/data-governancestandards/#:~:text=Data%20governance%20standards%20are%20guidelines,security %20of%20its%20data%20assets [Accessed 10 Mar. 2025].

3. **Data Policy and Information Management Assessment Platform (DPIMAP), n.d.** *Data Exchange Framework*. [online] Available at: https://dpimap.org/methodology/data-exchange-framework [Accessed 17 Apr. 2025].

4. **IT Governance EU, n.d.** *The GDPR: What is Sensitive Personal Data?* [online] Available at: https://www.itgovernance.eu/blog/en/the-gd-pr-what-is-sensitivepersonal-data [Accessed 25 May. 2025].

5. **OECD, n.d.** *Good Practice Principles for Data Ethics in the Public Sector*. [online] Available at: https://www.oecd.org/gov/digital-government/good-practiceprinciples-for-data-ethics-in-the-public-sector.htm [Accessed 5 Jun. 2025].

6. **Patel, A. and Patel, H., 2020.** *Towards Data Privacy and Security Framework in Big Data Governance*. [online] ResearchGate. Available at:https://www.researchgate.net/publication/346049042_TOWARDS_DATA_PRIVACY_AND_SECURITY_FRAMEWORK_IN_BIG_DATA_GOVERNANCE [Accessed 31 Dec.2024].

7. **Right to Education Initiative, n.d.** *Glossary: Disaggregated Data*. [online] Available at: https://www.right-to-education.org/monitoring/content/glossary-disaggregateddata [Accessed 30 May. 2025].

8. **UK Government, 2020.** *Data Ethics Framework*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/data-ethics-framework/data-ethicsframework-2020#overarching-principles [Accessed 30 Apr. 2025].

9. **United Nations Development Group (UNDG), 2017.** *Big Data for Sustainable Development: A Discussion Guide*. [online] Available at: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf [Accessed 20 Dec. 2024].

10. **United Nations ESCAP, 2023.** *Singapore Regional Statistics Governance Peer Exchange Series (SGRPES)*. [online] Available at: https://www.unescap.org/sites/default/d8files/eventdocuments/Singapore_RSG_SGRPES_31Oct-2Nov2023.pdf [Accessed 28 Feb. 2025].

11. **World Bank, n.d.** *Data Protection and Privacy Laws*. [online] Identification for Development (ID4D). Available at: https://id4d.worldbank.org/guide/dataprotection- and-privacy-laws [Accessed 15 May. 2025].

9 789998 061095

National Statistics Bureau
P O # : 338
Thimphu : Bhutan

Telphone # : +975 2 333296
+975 2 335848
Fax # : +975 2 323069

www.nsb.gov.bt