DEPARTMENT OF INFORMATION & COMMUNICATIONS TECHNOLOGY

DATA GOVERNANCE & DATA PROTECTION POLICY 2023

V5.0

Contents

FOREWORD BY MINISTER

I am delighted to present the Data Governance and Data Protection policy, a transformative initiative that marks a significant milestone in our journey towards digital excellence in the Pacific. This policy stands as a testament to our commitment to becoming a leader in digital transformation, with a focus on securing our citizens' trust in the digital government services we provide.

As we embark on this digital transformation journey, this policy serves as a crucial foundation for implementing our Digital Government Agenda. It lays the legal groundwork for all digital government services across the nation, providing the necessary trust and security to foster a secure digital environment that encourages innovation and growth. Additionally, it will underpin all our efforts in digital government, e-commerce, and e-trade, positioning PNG as a leading force in the digital landscape.

In our modern world, data plays an ever-increasing role, transforming how government agencies fulfill their missions and serve our nation. The Data Governance and Data Protection Policy sets a vision to create a secure digital environment that promotes innovation, growth, and development. By providing a clear framework for effective data management in the digital economy, it establishes fundamental data protection and governance principles, objectives, and goals, with well-defined strategies for implementation, monitoring, and evaluation.

Through the Department of ICT, my Ministry has been empowered by the Digital Government Act 2022 to lead and coordinate digital transformation within the government. This paves the way for critical digital government services, including Government Cloud Services, a Federated Secure Data Exchange Platform, a National eGovernment Portal using the Technology Stack, and an electronic window for e-commerce and e-trade. These initiatives will showcase PNG as a beacon of e-commerce, innovation, and trade, inspiring other nations in the process.

I extend my heartfelt gratitude to the Marape-Rosso Government for their unwavering support to my Ministry and the entire sector as we embark on this transformative journey. Together, we are committed to creating a world-class digital government that prioritizes our people, enhances efficiency, transparency, and accountability, and positions PNG as a welcoming hub for innovation and entrepreneurship.

Hon. Timothy Masiu, MP
Minister for Information and Communications Technology

PREAMBLE BY SECRETARY

I am delighted to introduce the Data Governance and Data Protection Policy, a milestone initiative that sets a clear framework for responsible, transparent, and accountable data management in our country. This policy paves the way for creating a secure digital environment that fosters innovation, growth, and development, making it an integral part of our Digital Government Agenda.

Our vision is to establish sound institutional governance and congruence with international standards while respecting the rights and freedoms of our citizens. This policy focuses on essential aspects, such as responsible data management, the Once Only Principle (OOP), artificial intelligence, open data, and data sharing, aligning with global best practices.

With the launch of the GovPNG Technology stack and the roll-out of digital government services, safeguarding data becomes of utmost importance. This policy ensures that all data collected, processed, stored, or transmitted is protected against unauthorised access, use, or disclosure. The policy outlines basic principles, objectives, goals, and implementation strategies that align with international standards and best practices The providing a robust foundation for effective data protection and governance.

As we advance towards our digital transformation journey, the principles of privacy and trust become crucial in all digital transactions. Confidentiality, integrity, and accessibility of data underpin mutual trust between the government and citizens, fostering a working e-government model. Technologies for trust serve as the technical building blocks for establishing and maintaining trusted networks, applications, and services, forming the bedrock of a trusted digital government infrastructure.

This policy plays a pivotal role in the successful implementation of our Digital Government Agenda, providing a legal basis for all digital government services. It instils confidence in consumers, industries, and other users, creating a secure digital environment that encourages innovation and growth.

I commend all those who have contributed to shaping this comprehensive policy, which sets PNG on a path of digital excellence, protecting the interests of our citizens and ensuring a prosperous digital future.

Steven Matainaho
Secretary

EXECUTIVE SUMMARY

In an era characterized by the prolific generation and utilisation of data, Papua New Guinea (PNG) recognizes the paramount importance of safeguarding the integrity and privacy of this invaluable resource. The need for a comprehensive and robust data governance and protection policy is evident as PNG steers into a digital future that thrives on secure, data-driven decision-making and innovation.

This policy establishes the foundational framework for enhancing data governance and data protection in PNG. At its core is the creation of the Data Protection Authority, a central body tasked with coordinating, regulating, and ensuring the secure management of data across the nation. The Data Protection Authority role as the vanguard of data protection and governance signifies PNG's commitment to this critical endeavor.

As data custodians, government agencies and businesses in PNG are entrusted with a vast array of data, encompassing personal, business, and sensitive information. Their role in data stewardship, from collection to disposal, is pivotal in ensuring the responsible and secure handling of data. Striking a delicate balance between safeguarding data privacy and enabling data-driven decision-making is at the heart of this policy.

A harmonious ecosystem for data governance and protection hinges on the synergy of government agencies, private sector entities, civil society, and academia. Together, they bear the collective responsibility of adhering to the guidelines outlined in this policy. Such cooperation fosters trust, transparency, and, in turn, efficient data-driven decision-making that fuels economic growth.

The Data Protection Authority, once established, will play a multifaceted role in upholding data protection in PNG. From policy development and enforcement to fostering collaboration and ensuring compliance, the DG Act's influence reverberates throughout the data landscape.

The policy strikes a harmonious balance. On one side, it ensures the secure protection of data, particularly sensitive information and data related to children. On the other, it empowers data utilisation, driving innovation and economic progress. This equilibrium respects the rights of individuals and organisations, cultivating a synergy that defines PNG's data ecosystem as resilient, trustworthy, and forward-looking.

This comprehensive data governance and protection policy heralds PNG's entry into the digital age, where the security and integrity of data coexist with the power of data-driven possibilities. It is a testament to the nation's commitment to protecting its digital future while fostering growth and prosperity.

SECTION ONE: BACKGROUND

1. Introduction

Developments in ICT combined with the growth in connectivity and Internet-enabled services have led to more intensive and automated collection and use of data, including personal data, in greater volumes by the private and public sectors. While these developments are accelerating economic and social developmentopportunities and benefits, they are also generating new risks for individuals and society as a whole, requiring national policies and strategies.

The Government of PNG recognizes the increasingly important role data plays in the development of the economy and society at large and wishes to adopt measures to help protect data and associated fundamental rights and freedoms, including the right to privacy, to ensure public trust in the use of data.

Data is a driver of digital transformation. Many digital technologies, rely on, and, generate massive amounts of data. The use of data can spur innovation and productivity, meaning firms may have a greater interest in collecting and storing data, including information about consumers. Governments are also collecting and using data to make better decisions, deliver improved public services, including in applications like health and education, and build more reliable national statistical systems. Elsewhere, data use has positively impact individual well-being, for example, by enhancing development cooperation to help developing countries use data more effectively to improve welfare and fight poverty.

In the current era, massive amounts of data including personal information are collected, transferred, processed, and stored within, between and among business and government entities businesses and jurisdictions. Accordingly, it is imperative that national policy, legal and regulatory frameworks are adequately designed and equipped to address the ever-evolving precepts and tenets governing these and attendant data sharing arrangements.

Data plays an increasingly important role in our modern world and new approaches to gathering, analysing, and using data are transforming the way federal agencies fulfil their missions and serve the nation. Maintaining trust in Government data is also pivotal to a democratic process. This expansion in data use also poses challenges for how agencies execute data-related activities as each agency faces a different set of infrastructure challenges, abides by different legal mandates, and maintains a unique culture. In this evolving environment, working with data and data management have become disciplines key to organisational success.

As data proliferates and analytical techniques advance the ability to link what once was non-personal data to an individual, concerns about potential privacy violations have risen. Personal data is increasingly collected without people's explicit awareness or being used in ways not anticipated at the time of collection. With the growth in use and value of data, personal data breaches have become more common.[1]

In a globalized world, cross-border data flows are a critical enabler of economic and social activity. Today's trade and production activities are heavily dependent on moving, storing, and using digital information (data), increasingly across borders. Data enables the co-ordination of international production processes through global value chains, helps small firms reach global markets, can be an asset that can be traded, or a conduit for delivering services, and is a key component for automation in trade facilitation. By some estimates, cross-border data flows

[1] OECD (2017), OECD Digital Economy Outlook 2017, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264276284-en.

contribute around USD 2.8 trillion to global economic activity, or 3.5% of global GDP[2].

Cross-border data flows raise questions about how to achieve important public policy objectives, such as the protection of privacy, security, sovereignty, and intellectual property rights, in the new digital landscape.[3] Reaping the benefits of digital transformation requires multi-stakeholder dialogue on regulatory approaches that ensure the interoperability of differing regulatory regimes, particularly for transversal issues such as cross-border data flows.

1.1 Importance of this Policy in Digital Economy

In the digital era, data has become an invaluable resource, profoundly impacting our economy, government services, and everyday activities. However, this increased reliance on data has introduced significant risks, especially concerning privacy and security. To address these challenges and build a secure, trusted, and well-regulated data ecosystem, the development of the Data Governance and Data Protection Policy in PNG is of paramount importance.

This policy serves as the cornerstone of our commitment to safeguarding the rights and interests of both individuals and businesses in our nation. With a robust legislative and regulatory framework, it empowers us to address the multifaceted issues surrounding data governance and protection. As we embark on this journey, we acknowledge the critical importance of responsible data management, promoting the ethical and lawful use of data.

The need for this policy is underscored by various challenges, including data protection, governance, infrastructure, quality, and security. Our aim is to strengthen data privacy and security measures, improve data management and governance, facilitate data-driven innovation, protect individual rights and dignity, and establish a trustworthy data ecosystem. By doing so, we enhance public trust, encourage investments, and promote a culture of responsible data use, which is essential for our national development and growth.

This policy is not just a set of rules but a commitment to the well-being and prosperity of our citizens and the nation. It aligns us with international best practices, promotes transparency, accountability, and data-driven innovation, and safeguards our cultural values and ethical principles. With a robust legislative framework, we strive to ensure that data is not just a tool but a guardian of our national interests and individual rights.

1.2 Current Data Governance and Data Protection Landscape in PNG

PNG's competitiveness in the digital economy relies on harnessing data's value. With data volumes exponentially increasing, the potential for value creation is immense. Publishing, linking, and sharing data can unlock opportunities not yet foreseen by government or businesses. Anonymized government data stimulates innovation and drives economic outcomes.

The data held by the PNG Government is a strategic national resource with significant potential for growing the economy, improving service delivery, and shaping policy outcomes. The policy commits to optimizing the use and reuse of public data, defaulting to open access for non-sensitive data. Collaboration with private and research sectors will further extend the value of data for the benefit of PNG citizens. Public data encompasses all government- collected data, while non-

[2] MGI (McKinsey Global Institute) (2016), "Digital Globalization: The new era of global flows", McKinsey & Company, March, www.mckinsey.com/business-functions/mckinseydigital/our-insights/digital-globalization- the-new-era-of-global-flows.

[3] OECD (2019), "Data in the digital age", OECD Going Digital Policy Note, OECD, Paris, www.oecd.org/going-digital/data-in-the-digital-age.pdf.

sensitive data is anonymized and compliant with privacy and security requirements as defined in the Digital Government Act (*Paragraph 36*).

In an era marked by digital transformation and data-driven decision-making, PNG recognizes both the potential and the risks associated with the collection, storage, and utilisation of both public and private data. These challenges underscore the need for a comprehensive Data Governance and Data Protection policy framework that addresses the unique attributes of PNG's diverse and dynamic society.

Key challenges in PNG's data landscape include:

i) **Data Protection:** Safeguarding data against threats and preserving its confidentiality, privacy, integrity, and availability is pivotal. This requires establishing robust data protection regulations and frameworks to deter and mitigate unauthorised access, breaches, or misuse.

ii) **Lack of Data Management:** While data is a valuable asset, an effective governance framework is required to manage it responsibly. PNG currently lacks comprehensive policies, regulations, standards, and guidelines governing data management, sharing, and protection.

iii) **Limited Infrastructure and Connectivity:** The geographical diversity of PNG poses challenges to establishing a robust data infrastructure and connectivity. Reliable internet and data communication services are lacking in many areas, hindering data collection, storage, and dissemination.

iv) **Data Accessibility:** Poor data management practices, the lack of centralized repositories, and data silos hinder accessibility to data across government agencies, businesses, researchers, and the general public. Streamlining data management practices is imperative to improve data accessibility.

v) **Data Quality and Integrity:** Data quality is hindered by inadequate collection methods, a lack of data standards, and limited data verification and validation capabilities. Enhancing data quality is crucial for informed decision-making.

vi) **Privacy and Security:** With the digital age raising concerns about data privacy and security, PNG requires robust data protection mechanisms to safeguard sensitive information from unauthorised access, breaches, or misuse.

vii) **Data Literacy and Capacity:** Enhancing data literacy and analytical skills among policymakers, public officials, and the general population is essential for harnessing the benefits of data.

viii) **Cultural and Ethical Considerations:** PNG's cultural diversity presents unique challenges for sensitive data handling, especially concerning indigenous knowledge and practices. Respecting cultural values and ethical principles is a priority.

ix) **Coordination and Collaboration:** Effective data governance necessitates collaboration among government agencies, the private sector, and civil society organisations. Improved coordination and data-sharing mechanisms are essential.

x) **Data Integration:** Siloed and duplicated data across various agencies need to be shared. Developing data standards is crucial for enabling data sharing and avoiding duplication.

xi) **Funding and Resources**: Allocating more resources to data-related initiatives is essential to meet emerging data demands.

xii) **Data for Decision-making:** Integrating data-driven decision-making practices into sectors like healthcare, education, and economic planning remains a challenge. Prioritizing investments in data infrastructure, promoting data literacy, establishing robust data protection regulations, and fostering stakeholder collaboration are vital steps to facilitate data-driven decision-making.

1.3 Data Governance and Data Protection Landscape Globally

Data plays an increasingly important role in our modern world and new approaches to gathering, analyzing, and using data are transforming the way government agencies fulfil their missions and serve the nation. Different countries have different approaches to regulating data privacy, data protection and data governance. *Annex B* contains an overview on how other countries have dealt with these issues. The European Union's General Data Protection Regulation is considered to be one of the main standards that others base their legislation on. Other countries such as Australia, New Zealand and the UK have various approaches..

Maintaining trust in Government data is also pivotal to a democratic process. This expansion in data use also challenges how agencies execute data- related activities. Each agency faces a different set of infrastructure challenges, abides by different legal parameters, and maintains a unique culture. In this evolving environment, working with data and data management have become disciplines key to success.

1.4 Intention of the Policy

The policy has several key intentions that are pivotal to Papua New Guinea's digital development and data governance:

i) **Protection of Privacy:** This policy is committed to safeguarding the privacy rights of individuals by establishing clear guidelines and standards for how personal data is collected, processed, stored, and shared. It ensures that personal data is handled fairly, transparently, and within the bounds of the law, granting individuals control over their data and protection against unauthorised access or misuse.

ii) **Governance and Accountability:** The policy seeks to establish a robust governance framework that enforces accountability in the management of data. This means defining roles, responsibilities, and obligations for data controllers and processors, whether they belong to the public or private sectors. The aim is to encourage transparency and responsibility in data handling.

iii) **Supporting Digital Transformation:** Recognizing that data is at the heart of digital transformation and economic progress, this policy promotes responsible data sharing and use.

By doing so, it aims to boost innovation, foster business growth, and enhance the delivery of public services. This not only benefits the economy but also empowers the government to serve the public more effectively.

iv) **Alignment with International Best Practices:** It is the policy's objective to bring PNG's data protection and governance framework in line with international best practices and

standards. This alignment is crucial to ensure that PNG remains up to date with global data protection trends and developments, especially concerning cross-border data flow.

1.5 Outcomes

The implementation of the Policy is expected to yield several positive outcomes for PNG, with each aspect contributing to the development of a secure and data-driven digital landscape:

a) **Enhanced Data Privacy and Security:** The policy, coupled with data protection legislation, will fortify data privacy and security measures. It will ensure that personal, confidential, and sensitive business data remains protected from unauthorised access and misuse. Moreover, this framework will facilitate secure data sharing and necessitate consequential amendments to existing legislation, instilling trust and confidence in data handling practices.

b) **Data Protection**: This policy followed by data protection legislation, is essential for safeguarding data from potential threats. It encompasses crucial measures such as encryption, access controls, firewalls, and other security technologies to shield data from unauthorised disclosure, alteration, or destruction.

c) **Improved Data Management and Governance:** By investing in capacity building and institutional strengthening, the policy will enhance skills and understanding of data management. This will foster a coordinated approach to data governance across government agencies, private sector organisations, and stakeholders. Compliance with relevant standards, laws and regulations will be ensured, promoting ethical and lawful data usage.

d) **Facilitation of Data-Driven Innovation:** The policy places an emphasis on data portability, interoperability, and secure data sharing. This approach will nurture a data-driven culture that fuels innovation and economic growth. Businesses, particularly SMEs, will benefit from improved access to their data, enabling them to make informed decisions and enhance efficiency and decision-making.

e) **Protection of Individual Rights and Dignity:** Recognizing data privacy as a fundamental human right, the policy empowers individuals to exercise control over their personal data. This includes granting individuals' access, correction, and deletion rights. By upholding privacy principles, the policy safeguards individuals from unwarranted intrusion, preserving their rights and dignity.

f) **Establishment of a Trustworthy Data Ecosystem:** The policy underscores transparency and accountability to build a trustworthy data ecosystem.

This commitment inspires public trust in data processors and services, creating an environment conducive to investments and collaborations. These advancements contribute significantly to the country's digital transformation journey.

1.6 Policy Development Process

The development of the Policy was a comprehensive and collaborative process, ensuring that the policy is well-informed, inclusive, and aligned with the needs and expectations of stakeholders in PNG. The policy development journey comprised several key activities, which are detailed below:

a) Stakeholder Consultation Workshop (26th May, 2022)

A Stakeholder Consultation Workshop was held at Hilton on the 26th of May 2022. This workshop brought together representatives from government agencies, private companies, NGOs, academia, and civil society organisations. The objective was to gather valuable insights, perspectives, and feedback from stakeholders regarding data governance and data protection requirements.

b) Internal Workshop (22nd- 23 February, 2023)

An Internal Workshop took place at Gaire, in Central Province, PNG on the 22nd and 23rd of February, 2023. This workshop involved internal subject matter experts, data governance managers, legal advisors, consultants, and relevant stakeholders. The primary focus was to review and discuss the content of the policy in-depth, ensuring it addresses issues at hand and alignment with organisational goals and values.

c) Lockdown for Policy Discussion (16th April, 2023)

To ensure rigorous scrutiny and refinement of the draft policy, an internal lockdown session was conducted on the 16th of April 2023. Internal key stakeholders, senior management, legal experts, and external consultants participated in this session. The objective was to firm up the draft policy, address potential gaps, and ensure cohesiveness before proceeding to the public consultation phase.

d) Policy Out for Public Consultation (21st April, 2023)

The draft Policy was published for public consultation on the 21st of April 2023. The policy document was made accessible to the public through the organisation's website: www.ict.gov.pg, social media channels, and other communication platforms.

During this period, feedback, suggestions, and recommendations were actively sought from the broader public (*feedback matrix).*

e) FM 100 Talk Back Show (2nd August, 2023)

As part of the public consultation process, an FM 100 Talk Back Show was organized on the 2nd of August.

The radio show provided a platform for citizens, taxpayers, and interested parties to voice their opinions, concerns, suggestions, and questions related to the Policy. This interactive session enriched the consultation process more transparent and allowed for direct engagement with the public.

f) Incorporating Public Feedback and Finalization

Feedback received during the public consultation period, including inputs from the FM 100 Talk Back Show, was carefully reviewed and analysed. Relevant suggestions were incorporated into the final version of the Policy. The policy development team worked collaboratively to ensure that the policy addressed the concerns and aspirations of all stakeholders.

g) Consultation & Validation Workshop (8th August, 2023)

Upon completion of the review and finalization process, the Policy was presented to the stakeholders during the consultation and validation workshop. The feedback received, was finalised and incorporated into the policy.

h) Incorporating Feedback from Consultation & Validation Workshop

DICT took all the valuable feedback from the validation workshop both on site and from the feedback forms handed in from the meeting and integrated it into a new version of the Policy that was put on the DICT website. As stated in the Workshop we have kept the process open for more than the 3 weeks mentioned and have created a new version of this policy we will submit to the NEC for approval (*feedback matrix, attached 2)*.

i) Prepare NEC Submission

On the 22 of November 2023, NEC Submission was drafted and submitted for NEC deliberation and approval

SECTION TWO: DATA GOVERNANCE AND PROTECTION POLICY STATEMENT

2.1 Mission

The mission of the Data Governance and Data Protection Policy is to govern and protect data throughout its life cycle from collection, storage and processing, utilizing and dissemination, archiving and disposal. This is to implement a shared, integrated government data hub in a centrally coordinated manner to improve public service delivery to all citizens and stakeholders effectively.

2.2 Goals

Goals of the Data Governance and Data Protection policy:

Goal 1: Develop and implement comprehensive data privacy, protection, and governance laws to safeguard all types of data, including personal, public, and business data, from unauthorised access, disclosure, or misuse.

Goal 2: Educate and raise awareness among government entities, citizens, and businesses on best practices for managing and protecting all types of data, including sensitive information.

Goal 3: Establish and enforce data sharing policies and mechanisms that protect the privacy and security of all citizens and businesses, especially when sharing sensitive information.

Goal 4: Create a data protection authority to oversee and enforce data management, protection, and privacy regulations, investigate complaints and breaches, and ensure compliance with applicable laws and regulations.

Goal 5: Foster international collaboration to exchange best practices and lessons learned on data governance and protection and stay aligned with global standards.

2.3 Objectives

Data Governance is needed in PNG and to ensure we achieve this, following are the objectives to achieve that;

a) To ensure that there is a centralised coordination of government data for a digital and sustainable economy,

b) To develop appropriate legislative and regulatory frameworks to support the availability, accessibility, and sharing of data while protecting data privacy.

c) To ensure that data standards, principles, and best practices of data management are in place to comply with so that government agencies can maintain data quality throughout the data-value lifecycle.

d) Ensure effective and secure data management by identifying and mitigating privacy risks associated with data collection, retention, use, disclosure, and disposal.

e) Establish a framework for data sharing, management, and governance across the public sector and with stakeholders, promoting responsible and legitimate data use.

f) Promote the use of data to support government decision-making and improve the delivery of government services.

2.4 Outcome

Outcomes include;

- Increasing consistency and confidence in decision-making
- Maximizing the revenue potential of data
- Improving data security or transparency of data lineage
- Enabling the availability and accessibility of data is a securely manner
- Making sure you're complying with data privacy rules
- Enable Data Sharing

2.6 Policy Alignment

The National Data Governance and Data Protection Policy represents a significant stride toward addressing PNG National development objectives of PNG, elevating the importance of data security and citizens' privacy protection. The National Data Governance and Data Protection Policy aligns with several significant national policies, strategies, and legislation encompassing the:

- Medium Term Development Plan (MTDP) IV 2023-2027
- Digital Government Plan (2023 - 2027)
- Digital Government (DG) Act 2022
- PNG Open Government Partnership National Action Plan (2022 - 2024)
- National Cyber Security Policy (2021)
- PNG Digital Transformation Policy (2020)
- 2018 ICT Sector Roadmap
- PNG Strategy for the Development of Statistics (2018 - 2027)
- PNG National Planning and Monitoring Act 2016
- Civil Registration (Amendment) Act 2014
- National and Local-level Government Electoral Regulation 1997
- Statistical Services Act 1980
- National Identity Act 1971

Within the MTDP IV, Strategic Priority Area (SPA) 6 underscores the critical role of National Security, particularly in Cybersecurity, while SPA 8 focuses on Digital Government, National Statistics, and Public Service Governance. These foundational policies and strategies emphasize the imperative need for robust data governance, data protection, and data privacy regulations. These priorities are integral to PNG's strategic growth plan. This alignment emphasizes the policy's role in advancing the country's development objectives and safeguarding citizens' data security and privacy.

SECTION THREE: POLICY SCOPE:

3.1 Audience

The Data Governance and Data Protection Policy is intended for a diverse audience, encompassing various stakeholders across PNG. Government agencies, especially large data stakeholders including those in public service, health, education, law enforcement, and statistics, stakeholders doing business with the government are vital recipients of this policy, as it provides essential guidelines and requirements for data management and protection within their sectors.

Equally important, the private sector organisations that collect, process, or store data, government data particularly personal data, are a significant audience for the policy. It outlines their responsibilities and obligations pertaining to data protection and governance of Government data, promoting responsible data practices within the business landscape. Additionally, data controllers and processors, who determine the purposes and means of processing personal data, must be aware of their roles and responsibilities as outlined in the policy and data standards.

The policy extends its scope to encompass data subjects, individuals whose personal data is being processed, by outlining their rights and the measures in place to safeguard their privacy and data. Civil society groups and advocacy organisations focused on data protection and privacy are also relevant stakeholders, contributing to the policy development process. Legal professionals, external regulatory bodies, and data protection authorities involved in enforcing data protection laws and regulations form a key stakeholder, ensuring effective implementation and coordination.

3.2 Policy Response

This Policy Response presents a comprehensive strategy designed to effectively address the challenges related to data governance and data protection in PNG. The primary objective is to ensure that data is managed securely and responsibly throughout its entire life cycle, from the moment of collection to the final dissemination and archival. It underscores the critical importance of data quality, consistency, and responsible utilisation while adhering to international data governance and protection standards.

- **Legislative Framework:** Key strategy involves strengthening the legislative framework by aligning national data protection, sharing, management, and governance laws with international best practices and standards. This approach establishes a robust legal foundation in PNG to safeguard all forms of data, including personal, confidential, and sensitive business data. By establishing clear and comprehensive data protection laws, individual privacy rights are fortified, engendering a trustworthy environment for data sharing and processing.

- **Data Quality Enhancement:** A fundamental pillar of this strategy is to elevate data quality and standardization. We emphasize the use of standardise data collection methods and practices, which significantly enhance data accuracy, completeness, and overall reliability. This strategy also includes data validation and verification processes to ensure the accuracy and consistency of the collected data.

- **Data Integration Practices:** The policy highlights the importance of data integration practices. It underscores the need to harmonize data from various sources, effectively preventing data duplication and ensuring the accuracy of the integrated data. Furthermore, there is an explicit focus on establishing a data governance framework that defines data quality standards and guidelines. This framework also assigns specific roles and responsibilities related to data collection and management.

- **Facilitating Data Sharing:** Facilitating data sharing is a pivotal aspect of this policy. It promotes the development of data sharing protocols and agreements to enable data exchange among government entities, businesses, and stakeholders. The government is entrusted with a significant role in promoting secure data sharing, particularly through the establishment of a Secure Data Exchange Platform, as outlined in the DG ACT.

- **Data Audits and Quality Assessments:** Regular data audits and quality assessments are highlighted as essential components of the policy. These systematic processes are crucial for identifying and rectifying errors and inconsistencies in data. The policy ensures that data continually adheres to the defined standards and requirements, thus maintaining data integrity.

- **Training and Capacity Building:** Capacity building and institutional strengthening are paramount for successful policy implementation. Robust training and awareness programs will enhance the skills and understanding of government agencies, private sector entities, and stakeholders handling data, ensuring compliance with data protection principles. Strengthening institutional governance will foster coherence and coordination across diverse sectors and entities in managing, sharing, and protecting data.

SECTION FOUR: DEFINITIONS

The first three sections set the scene for Data Governance and Data Protection landscape and also provided everyone with the Intent of the Policy. This section provides some key definitions of the terms we will be using in this policy.

Data Governance and Data Protection have never been the same thing, and the line between the two disciplines used to be very clear, but lately, the line between the two has blurred somewhat so that the two terms complement each other instead of being very distinct. Data governance is the key driver for outcomes, such as efficiency, accurate reporting, compliance support, reputation and customer experience improvements.

Below you will find some key definitions on Data, Data Governance and Data Management, Data protection. Additional definitions related to data governance and data protection can be found in *Annex A*

4.1 What is Data?

a) Data

Data refers to a collection of facts, statistics, information, or any pieces of knowledge that are recorded, stored, and can be processed or analyzed. Data can take various forms, including numbers, text, images, audio, video, and more. It is a fundamental component of information and knowledge.

Data can be raw and unprocessed, such as a list of numbers, or it can be processed and organized into meaningful information. In the context of computing and technology, data often refers to digital information stored in electronic devices or systems. Data is the foundation for making informed decisions, conducting research, and performing various tasks in fields ranging from science and business to everyday life. It serves as the building blocks for knowledge and insights.

b) Electronic Data

Electronic data refers to any data or information that is stored or transmitted electronically, using computers, networks, or other electronic devices. This includes a wide range of digital information, such as text documents, spreadsheets, images, videos, audio files, databases, and software applications. Electronic data can be created, collected, processed, and transmitted in various forms, such as emails, instant messages, social media posts, cloud storage, and online transactions. This makes electronic data an integral part of modern communication, business, and everyday life.

c) Personal Data

Personal data refers to any information that can identify an individual, directly or indirectly. This can include a person's name, address, email address, phone number, identification number, online identifiers, or any other data that could be used to identify the person. It also includes sensitive personal data such as health information, racial or ethnic origin, political opinions, religious beliefs, or sexual orientation.

Personal data can be collected, processed, and used by individuals, organisations, or governments for various purposes, such as marketing, research, employment, and law enforcement. The collection and processing of personal data are subject to data protection laws and regulations, which aim to ensure that personal data is processed fairly, lawfully, and transparently, and that

individuals' privacy rights are protected.

d) Pseudonymous Data

Pseudonymization is a data protection technique that involves processing personal data in such a way that it cannot be attributed to a specific individual without additional information that is kept separate and secure. This technique can help protect individuals' privacy while still allowing data to be used for research, analytics, and other purposes. An example of pseudonymous data is coded data sets used in clinical trials, where identifying information is replaced with a code to prevent the disclosure of personal information. This presents new challenges for data protection, as the use of personal data must be balanced with the need to protect individuals' privacy. Therefore, it is important to establish rules and regulations to ensure that personal data is used in a way that respects individuals' fundamental rights while promoting technological progress and electronic commerce.

4.2 What is Data Governance, Data Protection, Data Privacy and Data Sharing Life Cycle

a) Data Governance

Data governance is a comprehensive framework and set of practices aimed at ensuring the effective management of data within an organisation or at a national level. It encompasses the process of establishing and maintaining control over the collection, storage and processing, utilizing and disseminate, and archive and disposal within an organisation. The primary objectives of data governance are to maintain the quality, availability, security, and integrity of data assets.

At its core, data governance is designed to enable organisations and countries to leverage data effectively for informed decision-making. It cultivates a culture where data is valued as a strategic asset, encouraging transparency and accountability in data-related activities. This approach enhances the efficiency of data management, fosters a data-driven culture, and contributes to better decision-making across various sectors and industries.

Data Governance involves creating policies and procedures to ensure that all data is accurate, secure, and compliant with regulations. Data Governance also involves monitoring the use of data to ensure that it is being used responsibly and ethically.

b) Data Protection

Data protection encompasses a set of practices and measures aimed at safeguarding data from unauthorised access, alteration, disclosure, destruction, or misuse. It revolves around ensuring the security, privacy, and integrity of data, particularly sensitive or personal information. This comprehensive approach serves to prevent the inappropriate handling or processing of data, whether by individuals or organisations. The core principle of data protection is rooted in the right to privacy, ensuring that personal information is not exploited by entities responsible for data processing.

In the modern digital age, data protection assumes immense significance, as data plays a central role in various aspects of personal, business, and governmental activities. Its primary objectives are to establish trust between data controllers (those responsible for collecting and processing data) and data subjects, to ensure the responsible and ethical management of data. By preserving data, data protection fosters a secure and dependable digital environment that respects individual privacy and encourages the ethical utilisation of data.

Data protection affords individuals and organiations greater control over how they share their data with data processors, whether governmental entities or individuals. It defines the responsibilities of data processors, including obtaining informed and voluntary consent before processing data, implementing measures to guarantee data integrity and confidentiality, and ensuring that third parties adhere to the same level of data protection when sharing information. In cases of data processor breaches, individuals have the right to object and request corrections or deletions of their personal data.

c) Data Management

Data management refers to the process of acquiring, storing, organizing, processing, and maintaining data in a systematic and secure manner throughout its lifecycle. It involves various activities and strategies to ensure data is accurate, reliable, accessible, and usable for the intended purposes.

Data management is crucial for organisations to leverage data effectively for business operations, strategic planning, and innovation. Proper data management practices enhance data reliability, reduce data redundancy, and enable seamless data sharing and collaboration across teams and departments.

It also ensures compliance with data protection and privacy regulations, building trust with customers and stakeholders regarding data handling practices.

d) Data Collection

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

Data collection methods can vary widely and may include techniques such as surveys, interviews, observations, experiments, sensor data, and data mining, among others.

Data collection is a fundamental step in generating insights, making informed decisions, and conducting research in diverse fields, including business, healthcare, social sciences, and more. It is crucial to ensure that the collected data is accurate, reliable, and relevant to the objectives of the study or analysis. Proper data collection processes and tools are essential for obtaining high-quality data that can be used effectively for various applications.

e) Data Storage

Data storage refers to the process of preserving digital information, typically in electronic or magnetic form, for future access and use. It encompasses the mechanisms, devices, and technologies used to store data, including documents, files, databases, images, videos, and more. Data storage systems can be physical, such as hard drives, solid-state drives (SSDs), optical discs, and magnetic tapes, or cloud-based, where data is stored and managed on remote servers accessible through the internet.

Effective data storage solutions ensure that data is accessible, secure, and reliable when needed. Data storage systems should provide mechanisms for data retrieval, protection from unauthorised access, backup and recovery options to guard against data loss, scalability to accommodate increasing data volumes, and cost-efficiency in managing storage resources.

Data storage plays a vital role in various domains, including business operations, information technology, research, and personal data management.

f) Data Processing

Data processing is a term used to describe the collection, manipulation, storage, and retrieval of data. It refers to any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means. Examples of data processing include organizing data into databases, searching and retrieving data from those databases, analyzing and manipulating data, and transmitting data to other systems.

Data processing can be categorized into two types: manual and automated. Manual data processing involves the use of human effort to input and process data, while automated data processing involves the use of computers or other electronic devices to perform data processing tasks. Automated data processing is often faster, more accurate, and less prone to errors than manual data processing.

g) Data Utilisation

Data utilisation refers to the process of extracting meaningful insights, information, or value from stored data for various purposes. It involves accessing, analysing, and applying data to make informed decisions, solve problems, or support specific objectives. Data utilisation encompasses the transformation of raw data into actionable knowledge, typically through data analysis, interpretation, and visualization.

Effective data utilisation involves several key components, including data retrieval, data analysis techniques (such as data mining, statistical analysis, and machine learning), and the application of findings to inform decision-making or enhance processes. Data utilisation is crucial across various sectors, including business, healthcare, education, research, and government, as it helps organisations and individuals leverage their data assets to gain insights, improve efficiency, and drive innovation.

h) Data Portability

Data portability is a data management concept that empowers individuals and businesses, particularly small and medium-sized enterprises (SMEs), with the right to access and use their data for various purposes. It involves the ability to transfer and utilize data in a structured and machine-readable format, either by the data subject (individual) or a third party chosen by the data subject. This facilitates the exchange of data between different sectors and entities, promoting data usability and empowering data owners.

Data portability respects the privacy and confidentiality of certain data. It acknowledges that not all data can be openly shared with the public due to legitimate concerns related to privacy, intellectual property, organisational interests, or national security. Therefore, data portability in PNG may involve restricted data-sharing arrangements to balance data accessibility and the need to protect sensitive information.

i) Data Sharing

Data sharing is the controlled and authorise process of providing access to data to individuals, organisations, or entities, with the intention of supporting data-driven decision-making, research, collaboration, or service delivery. It involves making data available through direct sharing or data exchange mechanisms while ensuring that access to the data is regulated.

This practice can occur within an organisation or extend to partnerships between different entities, including government agencies, private enterprises, research institutions, and non-governmental organisations. Data sharing serves as a catalyst for collaboration, transparency, and innovation in various domains.

Data sharing has a significant impact on fields like healthcare, research, public administration, and business analytics. By enabling the exchange of data, it facilitates cooperation, knowledge dissemination, and the formulation of decisions based on data-driven insights. Nonetheless, data sharing should be conducted responsibly, emphasizing the protection of individual privacy and maintaining the security and confidentiality of the shared data.

j) Secured Data Exchange

Secured Data Exchange (SDE) is a platform established under Section 31 of the Digital Government Act (2022), designed to facilitate the secure and encrypted exchange of sensitive data and information between government entities and businesses. This platform offers a protected means of transmitting and receiving data, ensuring that the information is shielded from unauthorised access, interception, or tampering.

SDE platforms serve as government-authorised secure digital channels for the sharing of sensitive data, which can encompass various types of confidential information, including financial records, medical data, or personal details. To ensure data security, these platforms employ cutting-edge encryption technologies that safeguard the data both during transmission and while at rest.

In addition to encryption, SDE platforms are equipped with features such as access controls, audit trails, and user authentication. These elements work together to guarantee that only authorise individuals or entities have the requisite access to the shared data, fortifying data protection and confidentiality.

k) Data Dissemination

Data dissemination is the controlled sharing of data with specific individuals, organisations, or the public, often for the purpose of sharing information, research findings, or statistics. It involves distributing data to a targeted audience in a responsible and transparent manner. Data dissemination ensures that data is used for its intended purpose while adhering to privacy and security considerations.

l) Central Electronic Data Repository

The Central Electronic Data Repository, as per the definition outlined in the DG Act under Section 28, serves as an official storage server with the primary purpose of securely backing up electronic data generated and utilized by public bodies. It functions as a safeguard against unforeseen events or incidents that could potentially lead to data loss within public bodies. In essence, it acts as a protective repository for vital electronic data, ensuring its preservation and availability, even in the face of unexpected disruptions or data-related challenges.

m) Data Achieving

Data archiving is the systematic and policy-driven process of retaining data that, while not actively needed for current operations, possesses enduring value and may be utilized or stored for future reference or legal compliance. This practice, aligned with the guidelines established by the PNG Library and Archives Law, ensures the preservation of valuable information that could be relevant or essential in the future.

The archived data is securely stored, allowing for efficient retrieval when necessary, and contributes to optimizing storage resources and complying with regulatory requirements.

n) Data Disposal

Data disposal typically involves the permanent removal or destruction of data that is no longer needed, outdated, or no longer serves a purpose. The main goal of data disposal is to ensure that sensitive or confidential information does not fall into the wrong hands, especially when it is no longer relevant. Common methods of data disposal include shredding physical documents, wiping or securely erasing digital files, and physically destroying storage media like hard drives

o) Data Security

Data security refers to the set of measures and practices implemented to protect digital data from unauthorised access, use, disclosure, destruction, alteration, or any form of unauthorised manipulation. It is a critical aspect of information security that aims to safeguard data from potential threats and breaches, ensuring its confidentiality, integrity, and availability.

Data security is crucial in today's digital age, as organisations and individuals rely heavily on digital data for various purposes, and breaches can have severe consequences, including financial loss, reputational damage, and privacy violations. Effective data security measures help safeguard sensitive information and ensure data privacy and confidentiality are maintained.

Data security involves a combination of technical, administrative, and physical controls to mitigate risks and protect sensitive information. Some common data security measures include:

i) **Encryption:** Converting data into a coded form that can only be deciphered with a specific encryption key, making it unreadable to unauthorised individuals.

ii) **Access Controls:** Implementing authentication mechanisms, such as passwords, biometrics, or multi-factor authentication, to restrict access to data only to authorise users.

iii) **Firewalls:** Setting up network security devices that monitor and control incoming and outgoing traffic to prevent unauthorised access and potential attacks.

iv) **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** Tools that detect and block suspicious activities or potential threats in real-time.

v) **Data Backup and Recovery:** Regularly backing up data and having contingency plans in place to restore data in case of data loss or system failure.

vi) **Security Awareness Training:** Educating employees and users about data security best practices to minimize human-related vulnerabilities, such as phishing attacks.

vii) **Secure Data Transmission:** Using secure communication protocols (e.g., SSL/TLS) to protect data during transmission over networks.

Data security is essential for protecting sensitive and confidential information in an increasingly digital and interconnected world. It helps organisations and individuals maintain the privacy, integrity, and availability of their data while mitigating the risks associated with data breaches and cyber threats.

p) Data Breach

A Data Breach refers to a security incident that involves the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to a wide range of sensitive data, including personal data, government records, and business data. This breach can affect data that is being transmitted, stored, or processed. It encompasses any situation where sensitive information, whether related to individuals, government operations, or business activities, is compromised due to unauthorised or unintended actions. Such incidents can lead to significant privacy breaches, financial loss, damage to reputations, and potential misuse of the data. Data breaches are a serious concern, necessitating immediate attention and action to mitigate their consequences and prevent further unauthorised access or disclosure.

q) Data Privacy

Data Privacy is a comprehensive concept that entails the safeguarding and management of personal information across various contexts. It pertains to the protection, control, and responsible handling of individuals' sensitive data. Data privacy ensures that people have the authority to dictate how their personal information is collected, processed, used, and shared.

Data privacy encompasses a broad spectrum of practices, including securing personal data against unauthorised access, ensuring transparency in data collection practices, obtaining informed consent from individuals, and respecting their right to access, correct, or delete their data. It plays a vital role in safeguarding sensitive information, preventing data breaches, and fostering trust between data controllers and data subjects.

Data privacy extends beyond the protection of personal data and encompasses the secure and responsible handling of all types of data, including personal, business, and government information. It involves safeguarding data from unauthorised access, use, disclosure, alteration, or misuse, respecting an individual's or organisation's right to maintain data confidentiality and integrity.

Data privacy in a broader context includes:

i) **Business Data Privacy:** Ensuring the confidentiality and security of sensitive business data, such as financial records, intellectual property, trade secrets, and proprietary information. Protecting this data is essential for a company's competitiveness, innovation, and overall success.

ii) **Government Data Privacy:** Governments collect and manage vast amounts of data, including citizen records, financial data, and sensitive national security information. Data privacy in the public sector is vital to protect individual rights, maintain national security, and prevent data breaches.

iii) **Healthcare Data Privacy:** Medical records and patient information are highly sensitive and require stringent data privacy measures. Protecting healthcare data is crucial to ensure patient trust, comply with healthcare regulations, and advance medical research.

iv) **Research Data Privacy:** Research institutions collect and analyze vast datasets, some of which may contain sensitive or confidential information. Data privacy safeguards are necessary to protect research subjects, maintain research integrity, and adhere to ethical standards.

v) **Intellectual Property Data Privacy:** Protecting intellectual property, including patents, trademarks, copyrights, and trade secrets, is essential for fostering innovation and maintaining a competitive edge in various industries.

vi) **Government and Public Records Privacy:** Government agencies hold various public records, which may contain personal and sensitive information. Maintaining the privacy of these records is important for both transparency and individual rights.

vii) **Financial Data Privacy:** Financial institutions and organisations handle financial data, which includes account information, transaction history, and credit reports. Data privacy is crucial to protect individuals from identity theft and financial fraud.

viii) **Educational Data Privacy:** Educational institutions collect student data, including academic records and personal information. Protecting this data is necessary to comply with privacy laws and maintain trust with students and parents.

Data privacy measures may include encryption, access controls, regular audits, security policies, and compliance with relevant laws and regulations. Data privacy is fundamental in maintaining trust, ensuring compliance, and preventing the potentially devastating consequences of data breaches and misuse.

r) Data Classification

Data Classification is a systematic categorization and labeling process used to differentiate electronic data based on its level of sensitivity, access permissions, and security requirements. This classification process is guided by the provisions of the DG Act. Data is categorized into various tiers or classifications, with each tier representing a specific level of sensitivity:

i) **Top Secret Data:** This classification includes the most sensitive information that demands the highest level of security and confidentiality. Access to top-secret data is highly restricted and typically reserved for authorise personnel with a legitimate need to know. It may include critical government, security, or confidential business information. It is discouraged for sharing, and those seeking access must adhere to established procedures. Unauthorised disclosure, alteration, or destruction of top-secret data may result in significant harm to national security and endanger sources of vital information and state.

ii) **Confidential Data:** Confidential data represents information that is sensitive and requires a significant level of protection. Access to confidential data is limited to individuals or entities with specific authorisation, and it may include proprietary business data, personal information, or sensitive government records. Confidential data comes in two distinct categories, each with its own set of safeguards:

1. **Office Use Only Data/Sensitive Data:** This category includes data generated, collected, and stored within organisations for their operational needs. It may contain sensitive information vital for the government's internal processes. Such data can be shared between government entities (national, regional, and international) and government-to-business for facilitating business operations. It should be shared through secure government or business-approved digital platforms. Proper security measures, including access controls, must be implemented to prevent unauthorised access or disclosure. Unauthorised access to this data may result in reputational damage, financial loss, legal actions, or the compromise of national interests.

2. **Restricted or Highly Sensitive Data:** Some data are so confidential that open sharing is not feasible due to privacy, intellectual property, or national security concerns. Such data must be shared through government-approved secure digital platforms. Unauthorised access to highly sensitive data may lead to severe consequences, such as significant reputational damage, serious financial loss, legal actions, or the compromise of national interests.

iii) **Open/Public Data:** Open data, in contrast to the previous two classifications, is information that is intended for public access and sharing. Open data is not considered sensitive and does not require stringent access controls. This category, as articulated under the DG Act, encompasses data intended for open disclosure. Any data approved for public consumption is considered public. This may include press releases, annual statements, reports, and other publicly available information. Such data must be made accessible through official websites and shared with the public in an easily understandable format. It includes data that can be openly and freely disseminated, promoting transparency and accessibility.

The standards and guidelines for data classification will be developed in accordance with the provisions outlined in Section 64 of the DG Act. These standards will specify the criteria for classifying data into one of the categories mentioned above, as well as the security measures, access controls, and data handling procedures associated with each classification. Data classification ensures that data is handled in a manner that aligns with its sensitivity, safeguarding sensitive information while enabling responsible data sharing and access.

SECTION FIVE: PRINCIPLES

The first few sections set the scene for Data Governance and Data Protection landscape, provided everyone with the Intent of the Policy, and the relevant definitions of words that will be used in this policy. This section provides some key principles of data that will guide the policy narrations and statements of this Policy.

5.1 Principles of Data

Principles of Data Governance, Data Protection, Data Management, Data Security, Data Sharing, Data Ownership, Data Minimization and Single Source of Truth, Data Classification, Data Sovereignty & Data Localisation, and Artificial Intelligence.

5.1.1 Principles of Data Governance

i) **Privacy and Security:** Ensure the protection of individuals' and organisations' privacy by implementing measures like secure data transmission, access controls, and consent requirements. Prioritise data security to safeguard information from unauthorised access and breaches.

ii) **Integrity**: Maintain data integrity by following standards for secure data usage and management.

iii) **Transparency:** Promote the responsible use of data and outline roles and responsibilities of stakeholders in data governance.

iv) **Accessibility:** Ensure easy access to the policy online, following W3C accessibility standards for reliability and availability of data and information.

v) **Accountability:** Establish clear ownership and responsibilities for data throughout the organisation. Implement checks and balances between different teams and define accountabilities for data stewards.

vi) **Quality:** Provide a framework for sustainable data governance practices and outline principles and goals, including data security, privacy, integrity, accuracy, and accessibility

vii) **Confidence:** Maintain strict confidentiality measures for collected data and establish procedures to protect data access and integrity.

viii) **Compliance:** Ensure auditable data governance processes with documentation to support compliance-based and operational auditing requirements. Comply with international standards and best practices for data governance.

5.1.2 Principles of Data Protection

i) **Sound Institutional Governance:** Effective institutional management and governance shall be pursued, maintained, and practices of transparency, accountability, non-discrimination, and good governance shall be infused into their operations and management. Moreover, the national governance frameworks must promote fairness and not encourage, facilitate, or ignore the abuse of power regarding data use, processing, management, or transfers.

ii) **Congruence with International Standards and Best Practices:** International standards and best practices shall be pursued and implemented in the national data protection and sharing architecture to preserve and protect the rights of persons as data subjects and govern the actions of data custodians.

iii) **Respect for Rights and Freedoms:** The rights and freedoms of persons shall be respected in accordance with the national legal framework and commitments of the Government of PNG under relevant regional and international agreements.

iv) **Once Only Principle (OOP):** The "Once Only" Principle is a digital government principle that is premised on the use, reuse and/or sharing of data, information or documents already previously supplied within the public administration system, in a manner which is transparent. This principle pursues enhanced efficiency, a reduction in administrative burden and the protection of personal information, given that it is grounded on the need to submit information only once within any system or network of systems. This principle is therefore closely linked with the concept of interoperability.

5.1.3 Principles of Data Management

Responsible data management is a key principle of data governance, and it involves;

- ensuring that data is managed responsibly and ethically.
- ensuring that data is collected, stored, processed, and used in compliance with relevant laws and regulations and ethical and moral standards.
- ensuring that data is accurate, complete, and up- to-date and that appropriate measures are in place to protect the data from unauthorised access, disclosure, or misuse.
- implementing appropriate security measures, such as access controls, encryption, and firewalls, and ensuring that data is only accessed by authorise personnel who have a legitimate need for it.
- Responsible data management requires that data is used for legitimate purposes and that individuals are informed about how their data will be used and who will have access to it.
- obtaining informed consent from individuals before collecting their data and providing them with the opportunity to opt-out of certain uses of their data.

5.1.4 Principles of Data Security

i) **Confidentiality:** Ensure that data is accessible only to authorise individuals or entities and is protected from unauthorised access.

ii) **Integrity:** Maintain the accuracy and consistency of data throughout its lifecycle, preventing unauthorised alteration or tampering.

iii) **Availability:** Ensure that data is available and accessible to authorise users when needed, without interruptions or downtime.

iv) **Authentication:** Implement mechanisms to verify the identity of users and ensure that only legitimate users can access data.

v) **Authorisation:** Control access to data based on the principle of least privilege, granting access only to those who need it for their specific roles or tasks.

vi) **Encryption:** Utilize encryption to protect data both at rest and in transit, ensuring that sensitive information remains confidential even if intercepted.

vii) **Auditing and Monitoring:** Implement monitoring and auditing mechanisms to track data access and detect any suspicious or unauthorised activities.

viii) **Data Backup and Recovery:** Regularly back up data and establish reliable data recovery processes to prevent data loss in case of incidents or disasters.

ix) **Secure Data Sharing:** Implement secure data sharing protocols to ensure that data is exchanged safely and only with authorise parties.

x) **Continuous Improvement:** Regularly review and update data security measures to stay ahead of evolving threats and maintain a robust security posture.

5.1.5 Principles of Data Sharing

i) **Open Data and Data Sharing:** Data sharing and open data are crucial in the digital era, facilitating electronic transactions, e-commerce, and e-government services. Within PNG, these concepts are exemplified through initiatives like the electronic Single Window and e-Government Portal established through the *Digital Government Act (DG ACT) 2022* under *Section 35*. This policy recognizes the significance of open data as defined in **Section 36** of DG ACT and provides relevant guidelines. Open Data involves making data freely accessible via the internet, enabling download, and distribution without legal or financial constraints. It is a vital aspect of data sharing, requiring clear policy direction and decision-making.

ii) **Interoperability:** Interoperability plays a crucial role in the effective implementation of data governance and protection frameworks in PNG. It refers to the ability of different systems, organisations, and stakeholders to exchange, access, and utilize data in a standardise and seamless manner.

The following principles are to be complied with when dealing with interoperability and integration of systems.

a. **Standardisation:** Encourage the adoption of international and industry-recognized data standards, formats, and protocols to ensure compatibility and interoperability across systems. Establish a national framework aligned with global best practices to facilitate seamless data exchange and collaboration.

b. **Metadata Management:** Emphasis the importance of comprehensive and consistent metadata management. Develop guidelines for creating, maintaining, and sharing metadata to facilitate data discovery and understanding across different entities.

c. **Data Sharing Agreements:** Establish clear guidelines and legal frameworks for data sharing agreements between organisations. Encourage the use of standardise templates, specifying terms, conditions, and responsibilities to ensure secure and lawful data exchanges.

d. **Data Integration:** Promote the use of interoperable data integration techniques and technologies, such as APIs, to enable seamless data flow and integration between systems. Advocate for open data standards and APIs to facilitate interoperability among different data sources.

e. **Data Security:** Prioritise robust data security and privacy measures in interoperability efforts. Implement strong encryption, authentication, and access controls to safeguard data during exchange and integration while complying with relevant privacy laws.

f. **Data Quality Assurance:** Establish mechanisms to assess and maintain data quality during interoperability processes. Develop guidelines for data validation, cleansing, and transformation to ensure accuracy, completeness, and consistency**.**

g. **Collaboration and Coordination:** Encourage collaboration between government agencies, private sector organisations, and civil society to develop shared standards, guidelines, and frameworks for interoperability. Establish a national body or committee to coordinate interoperability initiatives and facilitate stakeholder engagement.

h. **Regular Assessment & Review:** Conduct periodic assessments and reviews of interoperability practices to identify areas for improvement. Ensure compliance with evolving technological advancements, standards, and legal requirements while maintaining an iterative approach to data governance and protection.

5.1.6 Principle of Data Ownership

The principle of Data Ownership embodies the accountability and responsibility associated with managing and safeguarding data throughout its lifecycle. This principle ensures that individuals and organisations are vested with clear roles and obligations, emphasizing the importance of ethical and lawful data stewardship.

i) **Accountability:** Individuals and entities collecting, processing, or managing data are held accountable for their actions. Accountability extends to adherence to data protection laws, organisational policies, and ethical standards. This principle reinforces the commitment to transparent and responsible data practices.

ii) **Responsibility:** Responsibility in data ownership encompasses the obligation to protect, use, and share data in a manner that aligns with legal and ethical standards. Data custodians are responsible for the accuracy, integrity, and security of the data under their purview. This principle emphasizes proactive measures to ensure data protection.

iii) **Clear Ownership Structure:** Establishing a clear ownership structure is paramount. Organisations and entities should designate specific individuals or teams as data owners with defined roles and responsibilities. This ensures that accountability and responsibility are clearly demarcated, fostering efficient data governance.

iv) **Ethical Data Handling:** Data owners are tasked with upholding ethical considerations in data handling. This includes avoiding unauthorised access, ensuring privacy protections, and abstaining from any form of data misuse. Ethical data practices are fundamental to maintaining trust and integrity in data ownership.

v) **Compliance with Data Protection Laws:** Compliance with data protection laws is non-negotiable. Data owners must stay abreast of relevant regulations, ensuring that data processing activities align with legal requirements. Regular audits will be conducted to verify compliance, with non-compliance incurring appropriate consequences.

vi) **Informed Data Decision-Making:** Data owners play a pivotal role in decision-making processes. Informed decisions are grounded in quality data. This principle underscores the responsibility of data owners to provide accurate, timely, and relevant data to support organisational decision-making across various domains.

vii) **Data Lifecycle Management:** Data ownership extends across the entire data lifecycle, from collection and processing to storage and disposal. Clear guidelines will be established for each phase, ensuring responsible data management practices. Data owners will implement secure disposal mechanisms for data that is no longer needed.

viii) **Transparency and Communication:** Transparent communication regarding data ownership is essential. Individuals whose data is collected should be informed about the purposes, processes, and entities involved in data management. Transparency builds trust and aligns with the principles of responsible data ownership.

ix) **Continuous Training and Awareness:** Recognizing the evolving nature of data management, data owners will undergo continuous training to stay informed about emerging trends, technologies, and best practices. This ensures that they remain equipped to fulfill their accountability and responsibility in an ever-changing landscape.

x) **Collaboration for Responsible Data Ownership:** Collaborative efforts will be encouraged among data owners, organisations, and stakeholders. Sharing best practices, insights, and challenges will contribute to a collective commitment to responsible data ownership. Collaboration reinforces a shared responsibility for the stewardship of data.

5.1.7 Data Minimization and Single Source of Truth

a) Once Only Principle

The Once Only Principle emphasizes the collection and maintenance of data at its source only once, eliminating duplication across multiple systems and databases. Under this principle, data shall be captured and recorded at the point of origin and subsequently referenced and shared as needed with stakeholders, reducing redundancy and enhancing data accuracy and integrity.

b) Guidelines

- **National Electronic Data Bank (Single-Source-of-Truth):** To uphold the Once Only Principle, a National Electronic Data Bank or Data Repository shall be established as per Section 27 of the DG Act 2022 which will be commonly referred to as the Single Source of Truth (SSoT). This repository will serve as the primary and definitive data source for specific information, ensuring consistency and accuracy across the public sector.

- **Data Referencing:** Data users and systems shall reference and access data from the SSoT rather than creating separate copies or silos of data. This practice ensures data integrity and minimizes the risk of inconsistencies arising from duplicate records.

- **Data Update and Validation:** Updates and modifications to data stored in the SSoT shall be made by the data owners to ensure data accuracy and currency. Proper validation processes shall be established to maintain the reliability of the data stored in the SSoT.

- **Data Sharing and Integration:** organisations shall prioritise data sharing and integration with the SSoT to foster a unified and standardise approach to data management.

- **Data Governance Oversight:** The Data Governance team shall oversee the adherence to the Once Only Principle, ensuring compliance across all sectors and resolving any instances of data duplication or discrepancies.

- **Data Security and Access Controls:** Access to the SSoT shall be restricted to authorise personnel, ensuring that data integrity and confidentiality are maintained. The team will ensure to collect only relevant and necessary data needed for that particular project or assignment is collected to ensure data privacy and security.

5.1.8 Principles of Data Classification

By adhering to these principles, organisations can create a robust data classification framework that aligns with their operational needs, regulatory obligations, and the overarching goal of safeguarding sensitive information.

- **Data Sensitivity:** Classify data based on its sensitivity, considering factors such as confidentiality, integrity, and availability. Recognise information critical to the organisation's operations, strategic plans, or sensitive stakeholder data.

- **Data Ownership:** Assign ownership to specific individuals or departments responsible for the creation, maintenance, and protection of classified data. Clearly define stewardship responsibilities, outlining who is accountable for the data at each stage of its lifecycle.

- **Legal and Regulatory Requirements:** Classify data in alignment with legal and regulatory requirements applicable to the organisation. Regularly update classifications to ensure ongoing compliance with evolving laws and regulations.

- **Data Lifecycle Considerations:** Consider data classification at each phase of its lifecycle, including creation, processing, storage, transmission, and eventual disposal and achieving. Recognise that the sensitivity of data may change over time, requiring dynamic reclassification.

- **Access Controls:** Apply the principle of least privilege, ensuring that access to classified data is granted only to individuals or systems with a legitimate need. Implement robust authentication and authorisation mechanisms to control access at different levels of classification.

- **Encryption and Masking:** Classify data to determine the appropriate level of encryption or masking required for storage, transmission, and processing. Ensure that encryption and masking align with the sensitivity of the data to protect against unauthorised exposure.

- **User Awareness and Training:** Conduct regular training sessions to educate users on data classification principles and the importance of handling classified information responsibly. Foster a culture where employees understand their role in maintaining the confidentiality and integrity of classified data.

- **Audit and Monitoring**: Implement audit trails and monitoring systems to track access, modifications, and transfers of classified data. Conduct regular audits to assess compliance with data classification policies and identify potential vulnerabilities.

- **Data Labeling and Marking:** Clearly label and mark data according to its classification to provide visual cues to users about the sensitivity of the information. Explore automated solutions for consistent and efficient data labeling, reducing the risk of human error.

- **Incident Response Planning:** Integrate data classification into incident response planning, specifying procedures for handling incidents involving different classifications of data. Establish protocols for reporting and responding to security incidents related to classified data promptly.

5.1.9 Principles of Data Sovereignty & Data Localisation

The principles of data sovereignty and data localization ensure that organisations protect individuals' rights and privacy, retain control over data, and comply with relevant laws and regulations in PNG while taking advantage of the safeguards and safe harbor provided by the APEC Cross-Border Privacy Guidelines.

i) **Data Transfer Mechanisms:** Implement a secure and authorise data transfer mechanisms when transferring data to or from cloud services located outside of PNG.

ii) **Cloud Service Provider Evaluation:** Carefully evaluate and select cloud service providers that demonstrate strong commitments to data protection, security, and compliance with international standards. Assess their data handling practices, security controls, certifications, and adherence to relevant data privacy regulations to ensure data is treated in accordance with the principles of data sovereignty.

iii) **Legal and Regulatory Compliance:** Always maintain a thorough understanding of the legal and regulatory requirements in PNG concerning data protection, privacy, and security. Our data governance practices align with local laws, regulations, and industry-specific requirements to protect the rights and privacy of individuals and ensure the secure handling of data.

iv) **Data Residency and Jurisdiction:** While our data may reside in data centers located outside of PNG, this policy and the forthcoming legislation provide for all data in the cloud to be governed by this policy and the forthcoming law and is fully aligned with the APEC Cross-Border Privacy and Enforcement Mechanism.

v) **Data Breach & incident Response:** Maintain robust incident response procedures to promptly address and mitigate any data breaches or security incidents. Collaborate with cloud service providers for coordinated efforts in managing and reporting incidents while complying with local regulatory obligation.

5.1.10 Artificial Intelligence

The Organisation for Economic Co-operation and Development (OECD) has outlined a set of principles related to Artificial Intelligence (AI) and Ethical AI. These principles provide a framework for the responsible development and use of AI, emphasizing ethical considerations, human rights, transparency, and accountability. These principles will be updated subject to changes, in line with latest OECD publications on most recent recommended principles.

OECD Principles on AI:

vi) **AI Should Benefit People and the Planet:** AI systems should contribute to inclusive social and economic development, environmental sustainability, and the well-being of individuals.

vii) **AI Should Respect Human Rights:** AI should be designed, developed, and used in a manner that respects human rights and ensures their protection.

viii) **Transparency:** There should be transparency in AI systems. This includes providing clear, understandable, and accessible information about the capabilities and limitations of AI systems.

ix) **Robustness, Security, and Safety:** AI systems should be robust, secure, and safe throughout their entire lifecycle. Measures should be in place to prevent accidents and avoid unintended harm.

x) **Accountability:** There should be accountability for AI systems. This includes ensuring that those responsible for AI systems are identifiable and answerable for their proper functioning.

xi) **Fairness:** AI systems should be designed and implemented to be fair, avoiding unfair bias and discrimination.

xii) **Inclusiveness:** All individuals and communities should have access to, benefit from, and influence AI technologies. There should be efforts to reduce digital divides and ensure inclusiveness.

xiii) **AI Should Be Transparently Discussed and Governed**: There should be public and private cooperation in the governance of AI. This involves creating a transparent environment for discussion and decision-making on AI.

xiv) **International Cooperation:** There should be international cooperation on AI. This includes facilitating the exchange of information and experience to create a global understanding of AI opportunities and challenges.

SECTION SIX: POLICIES

This section will delve into specific policies derived from the key principles outlined in Section Five. It will articulate detailed guidelines, regulations, and approaches to be adhered to in the realms of Data Governance and Data Protection. This section will translate the overarching principles into actionable and practical directives, covering aspects such as data collection, sharing, security, privacy, and compliance. Essentially, this section will serve as the operational core of the policy, offering a comprehensive framework for the effective implementation of Data Governance and Data Protection practices.

6.1 Data Governance

Data Governance in this policy refers to the comprehensive management of data throughout its entire lifecycle, starting from the point of data collection, moving through stages like storage, processing, utilisation, sharing, and concluding with responsible data dissemination. This meticulous approach ensures that each phase of the data's journey is carefully planned, regulated, and executed. The primary objective is to maximize the value of data while safeguarding privacy, maintaining data integrity, and upholding transparency.

6.2 Data Protection

Data protection is a fundamental aspect of this policy, ensuring the secure management and safeguarding of data throughout its entire lifecycle. This policy addresses data protection from the moment data is collected, all the way through its storage, processing, utilisation, sharing, and dissemination phases. The primary goal is to mitigate the risks associated with unauthorised data access, data breaches, and data misuse throughout the data life cycle.

6.2.1 Data Protection

To bolster data protection efforts, this policy prioritises the establishment of robust data access controls, safeguard public access data transparency, and ensure the privacy of personal access data. Additionally, a regime of regular audits and monitoring activities will be implemented to fortify data security, ensure strict compliance with data standards and regulations, and uphold the security and integrity of data assets.

POLICY STATEMENT:

a) **Data Access Controls:** Through this policy and in compliance with the DG ACT, organisations will be required to implement authentication, authorisation, and encryption measures to ensure that data is accessed only by authorise personnel based on their roles and responsibilities.

b) **Public Access Data Protection:** Specific standards and guidelines to be developed in line with DG ACT to ensure security and responsible sharing of public access data, including public/open data. Organisations will be required to ensure that publicly available datasets do not contain sensitive or personally identifiable information that could compromise individual privacy.

c) **Personal Access Data Protection:** Strict adherence and enforcement of set standards and guidelines on protecting personal access data, such as customer information, patient records, and financial records, to ensure access is only by authorise personnel and used for specific purposes or tasks.

d) **Data Access Audit and Monitoring:** Organisations to conduct periodic audits and monitoring of data access to detect and prevent unauthorised access or misuse. Any suspicious activities or data breaches to be promptly investigated and reported.

e) **Data Protection Standards:** A data protection standards and guidelines to be developed by the Department of ICT. These data standards will cover personal data, data access controls, encryption, data privacy measures, and incident response procedures.

6.2.1 Data Collection

Quality data collection is the cornerstone of effective data management, serving as the foundation for informed decision-making, innovation, and economic development. Avoiding data duplication is equally critical as it not only optimises resources but also ensures that data is consistently reliable. The policy framework places a strong emphasis on enhancing data collection processes to support the ease of doing business and data sharing in PNG.

POLICY STATEMENT:

To ensure quality data collection and avoid duplication while enabling data sharing for ease of doing business, organisations are encouraged to implement the following:

a) **Clearly Defined Objectives:** Clearly define the objectives of your data collection efforts. Understand what specific data you need and why you need it. This clarity will help in collecting only relevant data.

b) **Standardised Data Collection:** Develop standardise data collection forms, templates, or digital tools to ensure consistency in data entry. Clear instructions should be provided to data collectors.

c) **Data Validation:** Implement data validation rules during data entry to check for errors, inconsistencies, and missing values. This helps maintain data quality at the source.

d) **Data Dictionary:** Create a data dictionary that documents the definitions, formats, and allowable values for each data element. This document serves as a reference for data collectors.

e) **Unique Identifiers:** Assign unique identifiers to entities or records to avoid duplication. This is particularly important when collecting data about individuals, businesses, or entities.

f) **Training and Oversight:** Train data collectors to ensure they understand the importance of accurate data entry and are aware of the validation rules. Regular refresher training is encouraged.

g) **Supervision and Oversight:** Implement supervision and oversight of data collection activities. Supervisors can review collected data for quality and completeness.

h) **Digital Data Collection Tools:** In compliance to Section 48 of the DG Act, digital data collection tools are encouraged that include real-time data validation and checks to prevent data entry errors.

i) **Data Ownership:** Clarify data ownership within the organisation. Establish roles and responsibilities for data custodians and data stewards who are responsible for data quality.

j) **Quality Assurance:** Set up a quality assurance process to review data periodically. This can include data audits, spot checks, and data quality assessments.

k) **Data Cleaning and Validation:** Regularly perform data cleaning and validation processes to identify and correct errors or inconsistencies in the data. This can be done using data cleaning software.

l) **Data Integration:** If data comes from multiple sources, implement data integration practices to merge and reconcile data accurately. This can help avoid data duplication and inconsistencies.

m) **Data governance framework:** Establish a data governance framework that includes data quality standards and guidelines. This framework should define roles and responsibilities related to data collection.

n) **Data Sharing Protocols:** If data collected is required or needed by other organisations or agencies for their business process, to share such data, establish data sharing protocols and agreements to ensure data consistency. Such data can be shared on a government established Secure Data Exchange Platform established under Section 31 of DG ACT.

o) **Feedback Mechanism:** Encourage data collectors to provide feedback about data collection processes and the data quality. This can help identify issues and improve data collection methods.

p) **Documentation:** Maintain comprehensive documentation about data collection processes, including who collected the data, when, and under what circumstances. Documentation is critical for auditing and accountability.

q) **Data Audits:** Conduct periodic data audits to assess data quality, identify issues, and take corrective actions. Audits help maintain data integrity.

r) **Data De-Duplication:** If dealing with large datasets, consider using data de-duplication tools that can identify and eliminate duplicate records.

In accordance with Section 48 of DG ACT, standards will be developed guided by the above policy statements to regulate the data collection to ensure data collected is reusable, can be shared.

6.2.2 Data Storage and Processing

PNG acknowledges the critical importance of data storage and processing for both government operations and business interactions. While the establishment of the Central Electronic Data Repository established under Section 28 of DG ACT is underway, ongoing negotiations with cloud and data center providers have presented the need for a comprehensive Policy that ensures business continuity and upholds data sovereignty.

This policy seeks to address the storage and processing of data, striking a balance between safety, accessibility, and data sovereignty. It ensures a comprehensive approach to managing data in PNG, addressing storage and processing concerns while maintaining data sovereignty. The policy upholds the principles of data security, accessibility, and ethical data management in alignment with PNG's digital transformation journey.

POLICY STATEMENT:

a) **Data Classification and Storage Standards**
   - **Data Classification:** Data shall be classified into different categories, such as public, confidential, and top-Secret in accordance with Section 45 of DG Act. These categories will determine the appropriate storage and security measures.

   - **Storage Standards:** Organisations, including government bodies and businesses, shall adhere to predefined storage and security standards. These standards include data encryption, access controls, backup protocols, and data retention policies.

b) **Data Sovereignty**
   - **Data within Jurisdiction**: Top Secret and Sensitive government data, in particular, must be stored and processed within PNG's jurisdiction whenever feasible. The use of local data centers and cloud providers that comply with PNG regulations is encouraged.

   - **Vendor Selection Criteria:** Criteria for selecting cloud and data center providers shall be established in accordance with DG ACT and Government Cloud Policy 2023. These criteria shall encompass data security standards, compliance with PNG data protection laws, uptime guarantees, disaster recovery capabilities, and adherence to data sovereignty principles.

c) **Data Backup and Recovery:** Organisations are mandated to implement regular data backup and recovery procedures. Backup copies of data shall be stored securely in multiple locations to ensure data resilience and business continuity prior to the Central Electronic Data Repository

d) **Data Sharing Protocols:** Data sharing protocols and agreements governing data exchange between government entities, businesses, and cloud providers shall be developed. These protocols shall address issues like data access, data portability, and data sharing for authorise purposes.

e) **International Data Transfers:** Safeguards for international data transfers shall be established. Such transfers must comply with PNG data protection laws and respect data sovereignty.

f) **Education and Training:** Education and training programs shall be provided for government employees, businesses, and stakeholders. These programs include data security awareness training and guidance on data handling compliance.

g) **Collaboration with Stakeholders:** Key stakeholders, including government agencies, businesses, and cloud providers, shall be actively involved in the policy development and implementation process. Collaboration ensures that all parties participate in the policy's effectiveness.

h) **Transparency and Public Awareness:** Promote transparency in data handling practices. Public communication and awareness initiatives shall provide information about how data is stored and secured, thereby building trust and encouraging public engagement.

i) **Compliance and Audits:** Routine compliance checks and audits shall be conducted to verify adherence to data storage and security guidelines. Non-compliance shall be subject to appropriate consequences.

j) **Periodic Policy Review:** The policy commits to regular reviews to adapt to the changing digital landscape and advancements in data storage and security technologies. Flexibility is essential to accommodate changes and improvements.

6.2.3 Data Utilisation and Dissemination

The effective utilisation, sharing, and dissemination of data are essential for informed decision-making, economic development, and enhancing the ease of doing business in PNG. Historically, data utilisation has been limited, leading to ad hoc government decisions not backed up by proper data. This policy aims to ensure the collection, storage, processing, utilisation, sharing, and dissemination of high-quality data to ensure decisions are backed by quality data. This policy sets out the guidelines for harnessing data effectively to facilitate well-informed decision-making while promoting a conducive environment for businesses.

The Data Utilisation and Dissemination are integral to PNG's data-driven decision-making and economic development. This policy promotes data quality, accessibility, and utilisation, fostering transparency and collaboration while adhering to data privacy and security measures. It sets the stage for an improved business environment and public governance by utilizing data effectively to make informed decisions and drive economic growth.

POLICY STATEMENT:

a) **Data Quality Assurance:** Establish standardise data collection methods and practices to ensure data accuracy, completeness, and reliability. Data collected within PNG shall meet defined quality standards. Implement validation and verification processes to confirm the accuracy of data, with a focus on public, confidential, and top-secret data.

b) **Data Utilisation for Decision-Making**
- **Data-Driven Decision-Making:** Encourage government entities to embrace data-driven decision-making practices. Data shall be considered a valuable resource for policy formulation, planning, and implementation across sectors, including healthcare, education, and economic planning.

- **Decision Support Systems**: Develop and implement decision support systems that rely on data analytics, modeling, and forecasting. These systems shall guide government decisions and policies with data-backed insights.

c) **Data Sharing and Accessibility**
- **Data Sharing Framework:** Formulate data sharing protocols that facilitate the exchange of data between government entities, businesses, and stakeholders. Data sharing agreements shall address data access, data portability, and data sharing for authorise purposes.

- **Open Data Initiatives:** Encourage government entities to publish non-confidential and non-sensitive data sets as open data. This fosters transparency, innovation, and public engagement.

d) Data Privacy and Security

- **Data Privacy Protection:** Ensure that shared data is devoid of personal and confidential information. Data shall be anonymised or stripped of identifiers to protect privacy and data security.

- **Secure Data Sharing:** Implement secure data sharing mechanisms and encryption techniques to safeguard data during transit and at rest.

e) **Interoperability and Standardisation:** Establish data format and metadata standards to ensure interoperability. Data from various sources should be compatible and readily integrated for analysis and decision-making.

f) **Data Dissemination:** Promote the accessibility of government data for the public through user-friendly portals and platforms. Data dissemination should align with transparency practices, enhancing public awareness and participation.

g) **Public Awareness and Education:** Launch public awareness campaigns and educational programs to enhance data literacy and promote data usage within the community. These initiatives should empower individuals with knowledge on utilizing and interpreting data for various applications.

h) **Collaboration with Stakeholders:** Encourage the active participation of government agencies, businesses, and stakeholders in the data utilisation, sharing, and dissemination process. Collaborative efforts enhance the effectiveness of data utilisation.

i) **Compliance and Audits:** Regular audits shall verify compliance with data utilisation and sharing guidelines. Non-compliance shall be subject to appropriate consequences.

j) **Periodic Data Review and Improvement:** Conduct regular data quality assessments and reviews to identify areas for improvement. Ensure data continually meets the defined standards and requirements.

6.2.4 Data Sharing

This policy section focuses on establishing a framework for secure data sharing, promoting collaboration while safeguarding data integrity, privacy, and compliance with regulatory standards.

POLICY STATEMENT:

a) **Data Sharing Framework:** Clear protocols and guidelines will be formulated to facilitate secure data sharing among government entities, businesses, and stakeholders. Data sharing agreements will explicitly define authorise purposes, ensuring that shared data is used responsibly and ethically.

b) **Open Data Initiatives**: Government entities will be encouraged to publish non-confidential and non-sensitive data sets as open data, fostering transparency, innovation, and public engagement. Open data initiatives will adhere to established standards to ensure data quality, accessibility, and interoperability.

c) **Data Access and Portability:** User-friendly portals and platforms will be established to enhance the accessibility of government data for the public, promoting awareness and participation. Protocols for data access and portability will be developed, allowing individuals and businesses to easily retrieve and transfer their data.

d) **Secure Data Sharing Mechanisms:** Secure data sharing mechanisms, including encryption, will be implemented to safeguard data during transit and at rest. Stringent access controls will be enforced to ensure that only authorise individuals or entities have access to shared data.

e) **Interoperability and Standardization:** Standardise data formats and metadata will be established to ensure interoperability, facilitating the integration of data from various sources for analysis. Compliance with data format and metadata standards will be mandatory to promote seamless data sharing.

f) **Public Awareness and Education:** Public awareness campaigns and educational programs will be launched to enhance data literacy within the community. These Initiatives will empower individuals with the knowledge to utilize and interpret data for various applications, fostering a data-literate society.

g) **Collaboration with Stakeholders:** Government agencies, businesses, and stakeholders will be actively encouraged to participate in the data sharing process. Collaborative efforts will enhance the effectiveness of data utilisation, sharing insights, and improving decision-making.

h) **Compliance and Audits:** Routine audits will verify compliance with data sharing guidelines, with non-compliance subject to appropriate consequences. Audits will identify areas for improvement, ensuring that data sharing practices continually meet defined standards.

i) **Periodic Data Review and Improvement:** Regular data quality assessments and reviews will be conducted to identify areas for improvement. The policy will be adaptable to technological changes and evolving security standards, ensuring continuous improvement in data sharing practices.

6.2.5 Data Disposal and Archive

To ensure responsible data management, this policy outlines specific actions for secure data disposal and efficient archiving. The goal is to uphold data integrity, privacy, and compliance with regulatory standards.

POLICY STATEMENT:

i) **Data Disposal Practices:** Establish clear and secure methods for disposing of data that is no longer needed, ensuring that sensitive information becomes irreversibly inaccessible. Regular checks will be conducted to verify that data disposal practices align with established procedures and legal requirements.

ii) **Data Archiving Protocols:** Criteria will be set to identify data with long-term value for archiving, preserving valuable information. Define standards for secure data archiving, including encryption and access controls, to safeguard archived information.

Regular reviews of archived data will be conducted to assess its ongoing relevance, optimizing storage resources.

iii) **Legal and Regulatory Compliance:** Policies will be developed to align with legal and regulatory requirements for data retention, specifying retention duration and disposal conditions. Comprehensive documentation of data disposal and archiving processes will be maintained to demonstrate compliance with laws and regulations.

iv) **Responsibility and Accountability:** Clear roles and responsibilities will be assigned for data disposal and archiving, ensuring accountability for adherence to established procedures. Training and awareness programs will be provided to educate personnel on the significance of secure data disposal and archiving.

v) **Audit and Monitoring:** Routine audits of data disposal and archiving activities will be conducted to assess compliance, identify improvement areas, and promptly address any non-compliance. Mechanisms will be implemented to monitor access to archived data, enhancing security and ensuring that only authorise personnel retrieve information.

vi) **Data Restoration Protocols:** Clear procedures will be defined for the retrieval of archived data, ensuring a streamlined process for accessing valuable information. Integrity checks will be conducted during data restoration to verify that retrieved data remains accurate and unaltered.

vii) **Continuous Improvement:** A feedback mechanism will be established to gather insights from personnel involved in data disposal and archiving, facilitating continuous improvement. Regular assessments and updates of data disposal and archiving protocols will be conducted to adapt to technological changes and emerging security standards.

6.2.6 Data Security

PNG recognizes the pressing need to fortify its data security measures to safeguard against unauthorised data access, disclosure, alteration, or destruction. Inadequate data security not only leaves the nation vulnerable to data breaches and cyberattacks but also poses potential harm to individuals, organisations, and the country's overall interests.

This policy establishes a robust framework for data protection and security across the entire data lifecycle, ensuring the secure management and safeguarding of data throughout its journey from collection to utilisation, sharing, and dissemination. It promotes data governance practices aligned with local laws and international standards, safeguarding data privacy and sovereignty while facilitating secure data sharing for the benefit of PNG.

POLICY STATEMENT:

a) **Data Security Framework:** Develop data security standards, guidelines, and best practices in compliance with DG ACT, international standards and industry-recognised frameworks.

a) **Access Controls and Authentication**: Organisations will be required to adopt access controls based on the principle of least privilege, ensuring that users only have access to data necessary for their roles. Strong authentication mechanisms, such as multi-factor authentication, will be enforced to enhance user identity verification.

b) **Encryption and Data Protection:** Organisations to encrypt data, both in transit and at rest, to protect it from unauthorised access. Specific encryption standards and protocols will be defined to ensure data confidentiality.

c) **Incident Response and Cybersecurity Preparedness:** Organisations will be required to develop and regularly test incident response plans to effectively respond to data breaches or cybersecurity incidents. They will collaborate with the National Cyber Security Centre (NCSC) to enhance cybersecurity preparedness.

d) **Data Security Awareness and Training:** Conduct data security awareness programs and training for government employees, contractors, and other data handlers regularly. The training will cover data protection best practices, cybersecurity measures, and reporting procedures for suspected security incidents.

e) **Regular Security Audits and Assessments:** Organisations will be required to conduct periodic security audits and assessments to identify vulnerabilities and areas for improvement.

f) **Collaboration and Information Sharing:** Government agencies, private sector organisations, and international partners will share threat intelligence and best practices to collectively enhance data security.

6.2.7 Data Privacy

Data privacy is an overarching principle that requires a comprehensive framework encompassing personal, business, and government data. This policy approach underscores the importance of safeguarding and managing data across various sectors, ensuring that sensitive information is securely handled, and individuals' rights are respected.

This comprehensive data privacy framework is underpinned by principles such as encryption, access controls, regular audits, and adherence to relevant laws and regulations. By fostering a culture of data privacy across these diverse sectors, this approach aims to maintain trust, ensure compliance, and prevent the severe repercussions of data breaches and misuse.

POLICY STATEMENT:

a) **Business Data Privacy:** It is imperative to establish stringent data privacy standards for businesses. This includes securing financial records, intellectual property, trade secrets, and proprietary information. Robust business data privacy measures are not just a regulatory requirement but also critical for ensuring competitiveness, innovation, and overall success. Businesses should implement encryption, access controls, and regular audits to protect sensitive information.

b) **Government Data Privacy**: Governments collect and manage extensive data, ranging from citizen records to national security information. Data privacy within the public sector is paramount to safeguard individual rights, maintain national security, and prevent data breaches. Governments must adopt clear policies, encryption mechanisms, and access controls to secure this valuable information.

c) **Healthcare Data Privacy:** The healthcare sector deals with highly sensitive medical records and patient information. To build and maintain trust with patients, comply with healthcare regulations, and advance medical research, healthcare data privacy must be a top priority. Stringent safeguards, such as encryption and data access controls, are essential in this context.

d) **Research Data Privacy:** Research institutions frequently handle vast datasets, some of which contain sensitive or confidential information. Protecting research subjects, ensuring research integrity, and adhering to ethical standards necessitate robust data privacy safeguards. Encryption and strict access controls should be integral to research data management.

e) **Intellectual Property Data Privacy:** Safeguarding intellectual property, including patents, trademarks, copyrights, and trade secrets, is paramount for promoting innovation and maintaining a competitive edge in various industries. Data privacy practices should include mechanisms for securing intellectual property and monitoring unauthorised access.

f) **Government and Public Records Privacy:** Government agencies maintain numerous public records, some of which contain personal and sensitive information. Preserving the privacy of these records is essential for upholding transparency and respecting individual rights. Strong data privacy policies, including regular audits and access controls, are critical in this regard.

g) **Financial Data Privacy:** Financial institutions and organisations handle vast amounts of financial data, including account information and transaction history. Protecting individuals from identity theft and financial fraud is a fundamental goal. Data privacy in the financial sector should encompass robust encryption, access controls, and compliance with relevant financial regulations.

h) **Educational Data Privacy:** Educational institutions collect student data, including academic records and personal information. Complying with privacy laws, maintaining trust with students and parents, and ensuring responsible data handling are central to educational data privacy. Robust security measures, including encryption and strict access controls, should be established.

6.2.8 Data Classification

Data classification is a fundamental pillar of data governance and data protection. The absence of a standardise data classification system poses significant challenges to data management in PNG. To address this critical issue and ensure the highest standards of data protection and management, the government is committed to establishing a standardise data classification framework. This policy response outlines key actions aimed at enhancing data protection, reducing the risk of data breaches, and ensuring secure and appropriate data handling by authorise personnel.

By implementing a standardise data classification framework, PNG aims to fortify data protection, reduce vulnerabilities to data breaches, and ensure that sensitive information is handled with the utmost care. This policy response is a crucial step toward enhancing data management practices and maintaining the integrity and confidentiality of sensitive data.

POLICY STATEMENTS:

a) **Development of Standardise Data Classification Guidelines:** The government, in collaboration with relevant stakeholders, will develop clear and uniform data classification guidelines. These guidelines will categorize data based on its sensitivity, ensuring that sensitive information receives the highest level of protection. The classification will cover various types of data, including personal, business, and government information.

b) **Data Sensitivity Levels:** The data classification system will define sensitivity levels, such as "public," "confidential," and "top secret," to categorize data according to its level of sensitivity. This will help in clearly identifying which data requires the most stringent protection measures.

c) **Access Controls and Authorisation:** The framework will establish access controls and authorisation mechanisms for data based on its classification. It will outline who can access, modify, or transmit data at different sensitivity levels, ensuring that only authorise personnel can handle sensitive information.

d) **Data Handling Guidelines:** Clear guidelines will be developed for the appropriate handling of data based on its classification. This includes storage, transmission, and disposal procedures. These guidelines will help prevent mishandling and unauthorised access.

e) **Training and Awareness Programs:** To ensure the effective implementation of the data classification framework, training and awareness programs will be conducted for government agencies, businesses, and data handlers. These programs will emphasize the importance of data classification and the consequences of mishandling sensitive information.

f) **Monitoring and Compliance:** Mechanisms for monitoring and ensuring compliance with data classification policies will be established. Regular audits and assessments will be conducted to verify that data handlers are adhering to the defined data sensitivity levels and access controls.

g) **Integration with Data Governance and Data Protection Framework:** The data classification framework will be integrated into the broader data governance and data protection framework. This ensures that data sensitivity is a central consideration in data management practices and aligns with international best practices.

6.3 Data and Cybersecurity Governance

In recognition of the ever-increasing importance of data governance, data protection, and cybersecurity in a rapidly evolving digital landscape, PNG acknowledges the necessity of a well-structured and coordinated approach. This policy seeks to establish a harmonious synergy between the National Cyber Security Center (NCSC) and the DPA, recognizing their distinct yet complementary roles. Together, they safeguard the integrity of digital infrastructure, protect critical data, and ensure responsible data management, fostering innovation and economic growth while preserving privacy and security.

This policy acknowledges the vital roles of the NCSC and DPA in preserving the integrity and security of digital infrastructure and data. By working together and respecting each other's distinct yet complementary roles, they reinforce the protection of sensitive information, promote

innovation, and ensure that PNG's digital future thrives in a secure, data-driven environment.

6.3.1 Collaborative Framework

i) **Information Sharing and Coordination:** The NCSC and DPA shall establish a collaborative framework, facilitating the exchange of information and coordination of efforts where their roles intersect. Regular communication and mutual support will be encouraged.

ii) **Joint Incident Response:** In the event of a data breach with cybersecurity implications, the NCSC and DPA will collaborate in incident response, ensuring a comprehensive approach that addresses both data protection and cybersecurity concerns. They shall work together to contain the threat, minimize its impact, and conduct post-incident analysis.

6.3.2 Promoting Synergy

i) **Privacy and Security Alignment:** The NCSC and DPA shall work together to strike the necessary balance between safeguarding data privacy and ensuring cybersecurity. Privacy requirements and security measures shall be aligned to protect sensitive information while facilitating responsible data sharing.

ii) **Economic Growth and Innovation:** Recognizing that data is a valuable asset, the NCSC and DPA shall actively support initiatives that encourage data-driven decision-making and innovation. Collaboration with stakeholders from various sectors will be promoted to unlock the economic potential of data.

6.3.3 Review and Evaluation

i) **Periodic Assessment:** The NCSC and DPA shall periodically assess the effectiveness of their collaborative efforts, ensuring that the cybersecurity and data governance policies remain aligned with emerging threats and best practices.

ii) **Policy Enhancement:** If necessary, the policies governing the roles and responsibilities of the NCSC and DPA shall be enhanced to reflect changing cybersecurity and data governance landscape. Amendments will be made through a coordinated approach.

6.4 Data Ownership (Accountability and Responsibility)

This Policy underscores the essential principles of responsible and ethical data management, focusing on individuals and organisations as they receive and share data through various channels. It highlights the need for conscientious data consumption, utilisation, dissemination, and sharing, emphasizing compliance with legal and ethical standards, as well as the protection of data privacy and security.

POLICY STATEMENT:

a) **Responsible Data Handling and Sharing:** Those who receive data must handle it responsibly and ethically, using it only for authorise purposes. Misuse, unauthorised sharing, and actions compromising data integrity must be avoided. Data custodians are responsible for sharing data responsibly, complying with applicable laws and ethical standards, and ensuring data is shared exclusively for legitimate and authorise purposes.

b) **Data Privacy and Security:** Data recipients are entrusted with maintaining the privacy and security of received data. It is their duty to implement necessary measures to safeguard data against unauthorised access, breaches, and theft. This involves employing encryption, access controls, and secure storage methods. Data custodians share data securely and are equally responsible for preserving the privacy and security of shared data, with the implementation of encryption, access controls, and secure data transmission methods.

c) **Consent and Compliance:** Data recipients must obtain proper consent when required and ensure that data privacy is maintained throughout the data processing lifecycle. They are also responsible for complying with data protection laws, regulations, and organisational policies. Data custodians should similarly obtain proper consent when sharing data, maintain data privacy during the sharing process, and adhere to relevant legal and policy requirements.

d) **Ethical Data Sharing, Accuracy, and Integrity:** Data sharing must be approached responsibly, with data shared only with authorise parties for legitimate purposes. Data integrity and privacy must be maintained throughout the sharing process. Data custodians are accountable for the accuracy and integrity of shared data, implementing measures to prevent unauthorised modifications, data corruption, and inaccuracies.

e) **Data on Social Media and Freedom of Expression:** Data shared on social media platforms must be done with the consent of the data custodian or owner, respecting the principles of freedom of opinion and expression as enshrined in Section 51 of the PNG Constitution. This policy recognizes the importance of balancing data accountability with the fundamental right to freedom of expression.

f) **Data Accuracy and Integrity, and Ethical Data Management:** Data recipients must ensure the accuracy and integrity of received data. Unauthorised modifications, data corruption, and inaccuracies must be prevented when using, disseminating, or sharing data. Data custodians are expected to adhere to ethical data management practices, refraining from data misuse, unauthorised sharing, and any actions compromising data integrity.

g) **Legal and Ethical Compliance and Data Access Control:** Data recipients must comply with all relevant legal and ethical standards, respecting data subject rights, and ensuring data use aligns with legal requirements. They are also responsible for controlling access to data, permitting access only to authorise individuals or entities for intended purposes. Data custodians are accountable for granting access to shared data, ensuring that only authorise parties have access in alignment with the data's intended use.

h) **Reporting Data Misuse:** If data misuse or unethical practices concerning received data are observed, data recipients must report these incidents to the appropriate authorities or supervisors for corrective action. Data custodians should equally report any data misuse or unethical practices regarding shared data to facilitate corrective action.

i) **Data Retention and Disposal:** Data recipients are responsible for adhering to data retention and disposal policies. Data no longer needed should be securely disposed of, while data retention should align with legal, regulatory, and organisational requirements. Data custodians should ensure data retention and disposal policies are followed effectively.

j) **Transparency in Data Sharing:** When data recipients share data with third parties, they should do so transparently, providing information about the data's source, purpose, and any restrictions on data use. Data custodians should similarly share data transparently, offering insights into data's source, purpose, and any applicable use restrictions.

k) **Respecting Data Subject Rights:** Data recipients must respect data subject rights, including the right to access, correct, or request data deletion. Prompt responses to data subject inquiries, concerns, or requests are essential. Data custodians must equally respect data subject rights, ensuring timely responses to data subject inquiries and requests for data correction or deletion.

l) **Continuous Improvement:** Data accountability and responsibility are ongoing commitments. Data recipients should continuously strive to enhance data handling processes, uphold ethical standards, and adapt to evolving data protection requirements. Similarly, data custodians must commit to continuous improvement in data sharing processes, ethical standards, and compliance with evolving data protection requirements.

6.5 Stakeholders Roles and Responsibilities

In today's ever-evolving landscape of data governance and data protection, a comprehensive policy framework is not just desirable; it is essential. To ensure an all-encompassing approach, it is crucial to define the roles and responsibilities of stakeholders, all while maintaining a delicate balance between safeguarding sensitive information and facilitating data-driven decision-making. The roles and responsibilities outlined here are more than just building blocks; they are the very foundation upon which a robust data governance framework stands. These stakeholders are the guardians of data integrity, they are the enablers of data-driven decision-making, and they are the protectors of the interests of individuals and organisations.

POLICY STATEMENT:

a) **Data Custodians:** Every government agency and businesses, ranging from essential data stakeholders like the National Statistics Office (NSO) collecting population and demographic data to banks holding citizen's financial data, play a vital role in data management. They are entrusted with collecting, storing, processing, utilizing, sharing, and even disposing of various data types, including personal, business, and classified information. Their role as data stewards is fundamental to the success of this policy, fostering a culture of responsible data management throughout the data lifecycle.

b) **Coordinated Data Exchange:** The Secure Data Exchange (SDE) platform, established under Section 31 of the Digital Government Act, provides a central mechanism for sharing digitized data among stakeholders. However, it is incumbent upon entities to standardize their data to ensure seamless sharing through this platform. Standardization guarantees that data can flow freely and securely, promoting efficiency in data exchange.

c) **Collaboration and Responsibility:** Collaboration among stakeholders is a cornerstone of a well-regulated data ecosystem in Papua New Guinea. It involves government agencies, private sector organisations, civil society, and academia coming together to pool their efforts. Collectively, they are responsible for adhering to the guidelines set out in this policy. By doing so, they enable data-driven decision-making, thereby driving economic growth and societal development.

d) **Promoting Transparency:** Adherence to the policies and guidelines creates a transparent and efficient data ecosystem, which, in turn, fosters trust between citizens and agencies. As custodians of this information, government agencies and businesses must uphold the principles of data security and integrity. This commitment ensures that stakeholders have faith in the handling of their data.

e) **Balancing Act:** Maintaining a delicate equilibrium is paramount. On one side of the scale is the necessity to safeguard data privacy, particularly when it comes to sensitive information, and data that involves children. On the other side, facilitating data-driven decision-making fuels innovation and economic growth.

This policy skillfully strikes this balance, all the while respecting the rights of individuals and organisations, promoting data sharing to enable efficient business processes.

6.6 Training and Capacity Building

To build a data-literate workforce and create a conducive environment for responsible data governance and management, PNG is taking responsible actions. These actions empower individuals and institutions with the necessary technical expertise, knowledge of data protection, security, management, and sharing, as well as leadership skills to ensure responsible data governance. These coordinated actions aim to create a data-literate workforce, fostering a culture of responsibility, and ensuring data governance and management are carried out efficiently, securely, and in compliance with data protection and privacy regulations.

POLICY STATEMENT:

a) **Training and Skill Development:** Implement comprehensive training programs and workshops covering essential topics such as data protection laws, best practices in data security, data management techniques, and data sharing protocols. These initiatives will target government employees, private sector personnel, and other relevant stakeholders.

b) **Institutional Strengthening:** Develop relevant legislation, including standardise policies, procedures, and guidelines for data handling. Encourage the creation of specialized teams or data stewardship roles within organisations to ensure effective data management and adherence to data protection and privacy regulations.

c) **Collaboration and Knowledge Sharing:** Establish platforms and forums for sharing best practices, success stories, and lessons learned in data governance. These platforms will foster a culture of continuous learning and improvement in data-related fields.

d) **Technology and Infrastructure Enhancement:** Adopt secure data management systems and data analytics platforms, including emerging technologies. This will encourage the use of advanced technology to facilitate data-driven decision-making.

e) **Leadership and Management Development:** Support leadership and management development programs to ensure the effective implementation of data governance strategies and compliance with data protection regulations.

f) **Resource Mobilization:** Identify funding sources and expertise through partnerships with the public and private sectors, including international partners. These collaborations will support training programs, technology adoption, and other capacity building initiatives.

g) **Regular Evaluation and Monitoring:** Incorporate mechanisms for evaluating and monitoring the effectiveness of capacity building efforts. Regularly assess capacity issues and identify areas for improvement, ensuring that capacity building strategies remain relevant and up-to-date.

6.7 AI in Data Governance and Data Protection

The intersection of Artificial Intelligence (AI) and Data Governance presents unprecedented opportunities for innovation, efficiency, and informed decision-making. However, recognising the evolving nature of AI and the potential risks it introduces, this policy response aims to provide a flexible framework that harnesses the benefits of AI while ensuring robust Data Governance and Data Protection.

This policy response aims to strike a balance between leveraging the transformative power of AI and safeguarding against potential risks. It reflects a commitment to flexibility, ethical considerations, and continuous learning in the realm of AI within the context of Data Governance and Data Protection.

POLICY STATEMENT:

a) **Agile Governance:** The policy recognizes the dynamic nature of AI technologies and commits to an agile governance approach that adapts to emerging AI advancements. Regular reviews and updates will be conducted to align with evolving technological landscapes.

b) **Ethical AI Practices:** AI integration will adhere to ethical guidelines and principles. Decision-making algorithms will prioritise fairness, transparency, and accountability. Regular audits will be conducted to ensure alignment with evolving ethical standards.

c) **Data Privacy by Design:** AI systems will be developed with a "***Privacy by Design***" approach. All AI initiatives will undergo rigorous privacy impact assessments, ensuring compliance with data protection laws and evolving privacy standards.

d) **Continuous Learning and Adaptation:** Recognizing that AI is a field of continuous advancement, the policy encourages a culture of learning and adaptation. Mechanisms for ongoing training, research, and skill development will be established to keep pace with AI evolution.

e) **Robust Training and Awareness Programs:** Government entities and stakeholders involved in AI applications will undergo regular training on the latest developments in AI and their implications. Awareness programs will foster a culture of responsible AI use.

f) **Collaboration with AI Community:** The policy encourages collaboration with the AI research community, industry experts, and academia. Partnerships will facilitate the exchange of knowledge, best practices, and insights into emerging AI trends.

g) **Risk Assessment Mechanisms:** Prior to the deployment of AI applications, comprehensive risk assessments will be conducted. These assessments will include considerations of potential biases, privacy implications, and security risks associated with AI algorithms.

h) **Public Consultation on AI Governance:** Recognizing the societal impact of AI, the policy mandates public consultations on major AI initiatives. Input from citizens, civil society, and experts will be sought to ensure diverse perspectives in shaping AI governance.

i) **International Collaboration:** The policy encourages collaboration with international bodies and governments to stay informed about global AI governance practices. Participating in international forums will contribute to the development of consistent and globally aligned standards.

j) **Establishment of AI Oversight:** An AI Oversight mechanism will be established to monitor AI applications' adherence to the policy. These mechanisms will be responsible for assessing compliance, conducting audits, and recommending updates to the policy based on emerging AI trends.

SECTION SEVEN: LEGISLATIVE AND ORGANISATIONAL FRAMEWORK

7.1 Legislation and Regulatory Environment

The strengthening of data governance and protection regulations in PNG is a pivotal step toward advancing the nation's Digital Government and Digital Economy initiatives. Acknowledging the pivotal role of data as a valuable asset for progress, this policy harmonizes with our National Security and Digital Government priorities. It delineates the legal and policy frameworks necessary for the management and safeguarding of the Government of Papua New Guinea's data, thereby upholding national data sovereignty and addressing critical data-related challenges.

7.1.1 Legislative Framework

While PNG does not have a data protection law, the Cybercrime Code Act 2016[4] ('the Act') does contains certain provisions relevant to cybersecurity and aspects of data protection. It has been evidence through research[5] that there is no data governance law to protect data including personal data, hence there is significant need for the establishment of legal provisions concerning data governance and protection. The absence of such legislation leaves the privacy and security of data for all citizens at risk, particularly data collected by government agencies and businesses. This gap in the legal framework presents substantial challenges, rendering individuals and businesses vulnerable to potential data breaches and misuse.

This policy proposes for a development of a legal framework on Data Protection, Data Privacy, and Data Sharing. The enactment of this forthcoming legislation is essential for PNG, as it ensures data privacy, security, and responsible management. This legal framework will be developed in alignment with international standards, safeguarding the privacy and security of both citizens and businesses. Furthermore, it fosters a culture of data responsibility and transparency while supporting the country's Digital Government and Digital Economy objectives.

The legal framework will achieve the following objectives:

a) **Data Privacy and Protection:** The legislation will provide robust data privacy and protection for all citizens. It will ensure the integrity of data collected by government agencies and businesses, safeguarding sensitive information from unauthorised access and misuse.

b) **Protection of Vulnerable Groups:** Consequential amendments to related legislation will be introduced to extend protection to children's data and other vulnerable groups, recognizing the need to safeguard their privacy and security.

c) **Rights and Obligations:** The legislation will establish clear rights and obligations for data controllers and processors, ensuring that data processing is conducted in a lawful and ethical manner.

d) **Data Subject Empowerment:** Mechanisms will be established to enable data subjects to exercise their rights concerning their personal data, fostering transparency and control over their information.

[4] https://www.dataguidance.com/legal-research/cybercrime-code-act-2016
[5] https://www.dataguidance.com/jurisdiction/papua-new-guinea

e) **Data Breach Notification:** The legal framework will address data breach notification, ensuring that any data breaches are promptly reported and managed effectively.

f) **Data Sharing Protocols:** The legislation will establish clear guidelines for data sharing protocols, providing a structured framework for the secure exchange of data between stakeholders.

g) **Accountability and Deterrence:** Penalties for non-compliance will be introduced to promote accountability among data controllers and processors. These measures will serve as a deterrent against data misuse.

h) **Oversight Agency or Authority:** The law will establish or empower and existing agency or authority to be responsible for overseeing the implementation and enforcement of the legal provisions. The agency/authority will have the authority to investigate data breaches and non-compliance, impose penalties, and ensure adherence to the law.

i) **Emphasis on the "Once-only Principle":** The legislation will strengthen the "Once-only Principle" of data governance, encouraging efficient data management by collecting information only once and reusing it to prevent unnecessary duplication.

j) **Private Sector Participation:** The law will facilitate the participation of private sector organisations in the data exchange ecosystem. This involvement will support the implementation of the Secure Data Exchange (SDE) Platform in compliance with the DG ACT, ensuring the protection of personal data and sensitive information.

k) **National Data Governance Steering Committee (NDGSC):** The legislation will define the composition of this committee, bringing together major data stakeholders from government agencies, businesses, and civil society organisations involved in data governance and protection. This committee will promote coordination and collaboration, enhancing overall data governance efforts in PNG

7.1.2 Cybersecurity and Critical Infrastructure Law

This policy reinforces the importance of the *NEC Decision No. 348/2021*, which mandates the development of Cybersecurity and Critical Infrastructure legislations in PNG. These legislations are essential for safeguarding the nation's cyber space and critical infrastructure. The successful implementation of the Data Governance and Data Protection Policy and legislation depends on the simultaneous development of these two crucial laws. Together, they will establish a robust framework to address cyber threats and ensure the security of information systems, networks, and critical infrastructure.

The Cybersecurity and Critical Infrastructure legislations will provide clear guidelines for reporting and responding to cybersecurity incidents, as well as define appropriate penalties for cybercrimes. Additionally, these legislations will facilitate the establishment of a national cybersecurity authority tasked with overseeing and enforcing cybersecurity policies and regulations. By implementing these comprehensive legislations, PNG can significantly enhance its cybersecurity posture, ensuring the safety and security of its digital infrastructure.

The development of the National Cybersecurity and Critical Infrastructure Legislations is of utmost importance for the following reasons:

i) **Cyber Threat Mitigation:** The legislations will equip PNG with the necessary tools and protocols to effectively address cyber threats. By establishing guidelines for incident

reporting and response, the country can respond promptly to cyber incidents and prevent potential damage.

ii) **Protection of Critical Infrastructure**: Critical infrastructure, such as power grids, transportation systems, water, and communication networks, plays a vital role in the nation's functioning. The legislations will ensure that these infrastructures are adequately protected from cyber threats, minimizing the risk of disruptions and ensuring essential services continue uninterrupted.

iii) **Establishment of a National Cybersecurity Authority:** The legislations will pave the way for the creation of a dedicated national cybersecurity authority. This authority will have the expertise and resources to monitor, assess, and enforce cybersecurity policies across the country, fostering a safer digital environment.

iv) **Deterrence through Penalties:** By defining penalties for cybercrimes, the legislations will act as a deterrent, discouraging individuals and entities from engaging in malicious cyber activities. This will contribute to a safer online space for individuals and businesses alike.

v) **Improved Cyber Resilience:** Implementing the legislations will enhance PNG's overall cyber resilience. With clear protocols and regulations in place, the country will be better prepared to detect, respond to, and recover from cyber incidents.

vi) **Strengthening Data Governance and Data Protection:** Cybersecurity is intrinsically linked to data protection. A robust cybersecurity framework ensures that data is safeguarded from unauthorised access, breaches, and misuse, aligning with the objectives of the Data Governance and Data Protection Policy.

7.1.3 Consequential Amendments

To establish a unified and effective data protection framework in PNG, it is imperative to make consequential amendments to the existing legislation. These changes will align the regulatory landscape with the objectives of the National Data Governance and Data Protection policy, ensuring seamless data interoperability and robust security measures. Moreover, this alignment will enable various government agencies to share data more efficiently and integrate their systems within the PNG Government Technology Stack.

The DICT in consultation with relevant stakeholders, will undertake the following actions:

i) Facilitate the review of the DG ACT, NICT Act 2009, and Cyber Crime Code Act 2016 to ensure alignment and consistency between these legislations. This will ensure that the roles of the agency/authority established are aligned with the existing establishments.

ii) Facilitate the consequential amendments of existing legislations in Health, Education, Corporation laws, Customs, Finance, Tax, Land Registration, Payment Systems and a host of other Acts which will require updating to allow for data sharing and other Data Governance, Data Protection and Data Privacy to occur in PNG. This comprehensive review will redefine the roles and responsibilities of the government agencies, Businesses, and civil society organisations including, development partners, and other stakeholders and how they deal with Government data. The amendments will reflect the changing data governance and data protection landscape and technological advancements to allow for data sharing that is needed for digital government services delivery while upholding the

principles of Data Governance, Data Protection and Data Privacy.

7.2 Organisational Framework

In the ever-evolving landscape of data governance, data protection, and privacy, PNG recognizes the critical importance of a well-structured and organized approach to managing and safeguarding data. To this end, this policy proposes to establish a pivotal entity – The Data Protection Authority (DPA). This institution will serve as essential coordinator, entrusted with the task of ensuring that policies and practices related to data governance, data protection, and privacy are effectively implemented across all government agencies and businesses in PNG.

The roles and functions of the DPA and NDGSC are instrumental in forging a cohesive and comprehensive approach to data management. They play a significant role in aligning the efforts of diverse stakeholders in both the public and private sectors, promoting best practices, and ensuring a standardised approach to data governance and protection. This coordinated effort aims to bolster data security, safeguard privacy, and enhance data-driven decision-making while harmonizing with international standards and the unique values of PNG. The DPA and the NDGSC will drive the nation's data governance and protection strategy, fostering a resilient and prosperous digital environment for the benefit of all.

7.2.1 Data Protection Authority

This policy introduces a pivotal initiative - the creation of a DPA, which will serve as the central coordinating entity, ushering in an environment that empowers agencies and businesses to effectively harness the potential of their data. The DPA's overarching responsibility will be to oversee and regulate all dimensions of data management, sharing, privacy, and security.

Through the establishment of this dedicated and centralised authority, the government's vision is to cultivate a well-regulated and fortified data ecosystem. This ecosystem is envisioned to uphold data integrity, ensuring that data retains its value from the moment it's collected to when it's disseminated. Furthermore, the DPA's role is to support data-driven decision-making and stimulate economic growth by facilitating the effective utilisation of data resources.

Key Responsibilities of the DPA:

i) **Policy Development and Implementation:** The DPA will be responsible for developing comprehensive data protection policies, standards, and guidelines in consultation with DICT as the lead agency in developing Digital Data Standards. These standards will be industry wide. By implementing robust policies, the DPA will establish a clear framework for data management and data protection within PNG.

ii) **Data Governance Steering Committee.** DICT will be responsible in the early stages for coordinating data governance standards and regulations. In later years, DICT's goal is to transition this data governance responsibility and coordination to the DPA.

iii) **Collaboration and Coordination:** The DPA will work in collaboration with relevant government agencies, private sector organisations, and civil society to address data-related challenges collectively. It will also chair the Data Privacy Council which will lead the coordination efforts on Data Protection and Data Privacy in Government agencies, provincial, district and local levels and work directly with data privacy and information officers in all these agenices.

Through strategic partnerships and coordinated efforts, the DPA will foster a cooperative approach to managing and safeguarding data. It will also work collaboratively with the regional DPAs and global DPAs. This Authority will also offer insights and recommendations on legislative and administrative measures concerning the processing of personal and business data, as well as handle requests and complaints from data subjects.

iv) **Enforcement and Compliance:** The DPA will diligently ensure that both public and private sector organisations adhere to data protection policies, standards, and guidelines. The DPA legislation will enable and endow it with the ability to enforce compliance and take suitable actions against organisations found in violation of data protection regulations. This includes safeguarding personal and business data, overseeing proper data processing, monitoring compliance, and handling complaints related to data breaches. The DPA will maintain a registry of all data breaches and take necessary measures to secure compliance, provide remedies to affected individuals, and employ investigative and intervention powers to address non-compliance issues, which may lead to legal proceedings if required.

v) **Data Literacy and Awareness**: The DPA will actively promote data literacy and awareness among stakeholders. By conducting training and educational initiatives, it will enhance data literacy and disseminate knowledge about best practices in data protection and privacy.

The Authority will also provide advice and support to raise awareness about data protection, data privacy, and data governance by using social media and through capacity building activities surrounding the celebration the International Data Privacy Day set for 28 January each year. This day is “an international effort to create awareness about the importance of respecting privacy, safeguarding data and enabling trust."

Data Privacy Day's educational initiative focuses on raising awareness among businesses as well as users about the importance of protecting the privacy of their personal information online, particularly in the context of social networking. Data Privacy Day promotes events and activities that stimulate the development of technology tools that promote individual control over personally identifiable information; encourage compliance with privacy laws and regulations; and create dialogues among stakeholders interested in advancing data protection and privacy. This yearly celebration offers many opportunities for collaboration among government agencies, industry, academia, nonprofits, privacy professionals and educators.

vi) **Cultural and Ethical Considerations:** The DPA will take into account cultural and ethical considerations in data protection. It will ensure that data practices respect cultural norms and values while upholding international data protection standards.

vii) **Resource Management:** The DPA will advocate for funding and resources to support data protection initiatives. It will work towards resource mobilization to strengthen data infrastructure and data protection capabilities.

viii) **International Cooperation:** The DPA will be the key agency liaising with other relevant agencies in the Region and beyond. It will work closely with the GoPNG’s development partners in advancing its goals and ensures protection of citizens data.

7.2.2 Data Governance Steering Committee

The establishment of the Data Governance Steering Committee (DGSC) is a pivotal step in ensuring effective coordination and oversight of all matters related to national data governance, protection, and privacy in PNG. The DGSC will play a key role in setting the strategy, policy, standards, and guidelines for data governance and protection, ensuring that data-related initiatives align with the country's goals and international obligations.

By bringing together major data owners, relevant government agencies, private sector representatives, and civil society, the DGSC ensures that data governance and protection efforts are comprehensive, collaborative, and aligned with national and international goals. The committee's leadership and oversight will play a crucial role in fostering a data-driven and secure environment that promotes innovation, growth, and societal development while safeguarding data privacy and security.

Composition and Responsibilities of the DGSC:

i) **Chairmanship and Co-chairmanship:** The DGSC's leadership will consist of the Director of the DGSC as Chair, ensuring the DG's pivotal role in the decision-making process. The Secretary for DICT or his nominee will co-chair the committee, representing the department responsible for coordinating the Digital Government and Services for the whole-of-Government.

ii) **Representation of Major Data Owners:** The committee will incorporate major data owners from within the country, as well as relevant central government agencies. Their inclusion is imperative to ensure the active involvement of key stakeholders responsible for the management and ownership of critical data.

iii) **Involvement of Relevant Agencies and businesses:** Upon request, other government agency representatives will be invited to participate in the committee's sessions. This ensures a comprehensive representation of stakeholders, further enhancing the coordination of data governance and data protection efforts.

iv) **Private Sector and Civil Society Involvement:** The DGSC will include representatives from the private sector and civil society, recognizing the importance of incorporating perspectives and concerns from outside the government sector. This inclusive approach is vital for the collaborative enhancement of data governance.

v) **Strategy and Policy Development:** The committee will be responsible for providing strategic guidance on data management, sharing, privacy, and security practices.

vi) **Regular Meetings and Updates:** The DGSC will meet regularly to review and update the data governance policy, standards and guidelines as necessary. This ensures that the policies, standards and guidance remain relevant and up-to-date, considering evolving data-related challenges and opportunities.

vii) **Advice and Support:** The DGSC will provide advice and support to various stakeholders, assisting them in the effective implementation of the data governance and data protection policy and strategy.

7.3 Executive Sponsor and Lead Agency

Before the establishment of the Authority, the following interim arrangements will be set in place, designating DICT as the Executive Sponsor of this policy. DICT will work collaboratively with other relevant government agencies. DICT will assume a pivotal role in this capacity.

DICT, as the Lead Agency for this policy, will assume the responsibility for the development of policies and legislation pertaining to Data Governance and Data Protection Policy and any forthcoming legislative actions.

In this transitional phase, DICT, in close consultation with key stakeholders from government agencies, the private sector, civil society, the technical community, and academia, will actively coordinate the policy's implementation. This includes spearheading the development of the Data Protection Legislation, as well as any other legislative measures guided by this policy. This ensures a cohesive approach to data governance and protection in this interim period.

SECTION EIGHT: ENFORCEMENT AND MONITORING AND EVALUATION

8.1 Enforcement

Enforcement is a pivotal pillar of any comprehensive data protection and governance policy. It upholds the legal framework, ensures adherence to regulations, and safeguards individuals' privacy rights. The DPA is vested with the authority to enforce data protection laws and regulations. Its responsibilities encompass investigating and prosecuting those who violate data protection laws. Moreover, the DPA actively promotes compliance by offering guidance and support.

DPA will collaborate with law enforcement agencies, the judiciary, and relevant stakeholders further strengthens the legal and regulatory framework for data protection and governance. This collaboration fosters trust and confidence in the principles that underpin data protection and governance.

8.2 Monitoring and Evaluation

The process of monitoring and evaluation is fundamental for ensuring the effectiveness of data protection and data governance policies. These activities not only guarantee compliance but also build trust and confidence in the responsible management of personal and sensitive data.

Monitoring and Evaluation Responsibilities:

a) Prior to the establishment of the DPA, DICT assumes the role of monitoring and evaluating policy implementation.

b) Following the establishment of the DPA, DICT will collaborate closely with the Authority to address all monitoring and evaluation matters related to Data Governance and Data Protection.

c) The DPA will institute a robust system for monitoring and reporting on compliance with data protection and governance laws and regulations across the public and private sectors. This system will conduct regular assessments of data protection practices and procedures. Additionally, it will scrutinize data breaches and incidents to ensure swift and appropriate responses.

d) Periodic reviews of the policy will be conducted by the DPA to assess its effectiveness and identify areas that require improvement. These reviews will inform policy enhancements and adjustments.

The DPA is committed to transparency and public accountability. As part of this commitment, it will establish a system for public reporting on data protection and governance. This will involve the regular publication of reports detailing data breaches and incidents. Furthermore, these reports will shed light on trends and patterns in data protection practices and procedures, ensuring that both the public and stakeholders are well-informed.

ANNEXES

ANNEX A: ADDITIONAL DEFINITIONS

Data Governance Body

A Data Governance Body is an organization that has the authority and oversight over the management of agency data assets which are a key piece of data infrastructure. These bodies are commonly called by such names as Data Governance Boards, Data Councils, or Data Strategy Teams. The Data Governance Body establishes policy, procedures, and roles for developing, overseeing, and coordinating data management policy and helps prioritize data resource allocations to answer agency key questions and meet stakeholder needs.

An effective Data Governance Body is foundational to leveraging data as a strategic asset and a critical precursor to making conscious and realistic decisions about stewarding data assets and developing related data infrastructure. Agencies should establish a Data Governance Body as a top priority, thereby setting up the organizational structure to address data and related infrastructure needs.

The proposed Data Governance Body would identify the scope of the data that needs to be managed and prioritizes key data-related issues that need to be addressed. The Body would then identify appropriate policies, standards, and reporting structures to ensure that key information assets are formally and properly managed.

Most Data Governance Body uses maturity models to assess agency capabilities and seeks meaningful and broad agency and stakeholder input before recommending data investment priorities. They also set a process for monitoring compliance with policies, standards, and responsibilities throughout the information lifecycle. Regardless of how the Data Governance Body is constituted, it must be integrated into agency decision- making and operations to ensure that data are used effectively to address agency key questions and meet stakeholder needs.

Right to Privacy

The right to privacy is a fundamental human right that protects individuals from unwanted and unwarranted interference in their personal lives, including the collection, use, and disclosure of personal information. It covers all aspects of an individual's life and the processing of personal data by government and private organizations. In the digital age, this right has become increasingly important as more personal information is collected and processed, and individuals have the right to know what information is being collected, why it is being collected, and how it is being used.

Protecting the right to privacy is essential for maintaining individual autonomy, dignity, and freedom. It is critical for promoting trust and confidence in the digital economy, ensuring that individuals can fully participate in society without fear of discrimination or harm, and guaranteeing respect for personal dignity as a necessary part of the legal order. The Universal Declaration of Human Rights and the United Nations International Covenant on Civil and Political Rights define privacy as a right and everyone has the right to protection of the law against interference or attacks on their privacy, family, home, or correspondence.

Data privacy or information privacy

Data privacy, also known as information privacy, is a subcategory of data security that deals with protecting individuals' personal information. It encompasses the guidelines and regulations that ensure the appropriate collection, use, storage, and disclosure of personal information. Data privacy concerns arise when personal information is collected, processed, or shared without consent, notice, or regulatory obligations.

Although data security and data privacy are often used interchangeably, they have different objectives. Data security focuses on protecting data from unauthorized access, theft, or damage by external attackers or malicious insiders. On the other hand, data privacy aims to control the access, usage, and disclosure of personal information, thus ensuring that individuals' privacy rights are respected. While data security is essential in protecting personal data, it does not guarantee data privacy. Therefore, it is essential to implement both data privacy and data security measures to safeguard personal information.

Biometric data

Biometric data refers to unique physical, physiological, or behavioral characteristics of an individual that can be measured and analyzed for identification purposes. Biometric data can include a wide range of information, such as fingerprints, facial recognition, voiceprints, iris scans, and DNA. This data is processed using specialized technical procedures to confirm the identity of an individual or to grant them access to certain systems or locations.

Biometric data is considered highly sensitive personal information and requires special care and attention to ensure its security and protection. Due to the unique nature of biometric data, there are increased risks associated with its collection, processing, and storage. For instance, if biometric data is compromised or stolen, it cannot be replaced or reset like a password, and the affected individual may face significant harm as a result.
As such, organizations that collect and process biometric data must adhere to strict regulations and standards to ensure that the data is properly secured and protected. This includes obtaining informed consent from individuals prior to collecting their biometric data, implementing robust security measures to safeguard the data, and ensuring that the data is only used for its intended purpose.

Consent: is defined as any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Special categories of personal data

Special categories of personal data, also known as sensitive personal data or “special categories” under GDPR, refers to personal data that is particularly sensitive and requires extra protection. These categories include information such as a person's race, ethnicity, political beliefs, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a person, health data, and data concerning a person's sex life or sexual orientation.

Because this type of data can be used to discriminate against individuals or cause them harm, special categories of personal data are subject to stricter regulations and higher levels of protection under data protection laws. Organizations must obtain explicit consent from individuals before

collecting or processing such data, and they must have a valid reason for doing so, such as fulfilling legal obligations or protecting vital interests. They must also take additional measures to ensure that the data is kept secure and confidential, and that it is not used in a discriminatory or harmful manner. Failure to comply with these regulations can result in significant fines and other legal consequences.

Cross-Border Processing' means either:

1. processing of personal data which takes place in the context of the activities of establishments in more than one State of a controller or processor in a State where the controller or processor is established in more than one State; or
2. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor, but which substantially affects or is likely to substantially affect data subjects in more than one State.

Data controller

A data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the way any personal data are, or are to be, processed. A Data Controller can also refer to a public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Data owners

Data Owners are individuals or groups within an organisation who are responsible for the management and protection of specific sets of data. Data ownership implies accountability and decision-making authority over the data, including the authority to determine who has access to the data, how it is used, and what policies and procedures govern its management.

Data owners also involves ensuring that the data is accurate, complete, and up-to- date. Data Owners are responsible for ensuring that their data is of high quality and that it is being used in accordance with organisational policies and applicable laws and regulations.

Data Processor

A Data processor is defined as a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Cross-Border Data Transfer means a transfer of personal data to a recipient in another country.

Safe Harbour means a data transfer mechanism agreed between two countries.

Data Maps

Data Maps also known as a Data Dictionary or Data Schema, is a structured representation that provides an overview of the data elements present in a database, dataset, or information system. It serves as a reference document that describes the structure, format, and characteristics of the data used within an organization or a specific project.

Data Maps play a crucial role in data management and understanding the data assets of an organization. They serve as a communication tool between different stakeholders, including data analysts, database administrators, software developers, and business users. Data Maps promote data consistency, data integrity, and help avoid ambiguity or misunderstandings regarding the data elements and their meanings.

Data Maps are valuable during the design phase of databases or information systems. They help in planning and organizing the data structure before actual implementation, ensuring that the data collected aligns with the organization's needs and objectives.

A well-constructed Data Map enhances data governance, facilitates data sharing, and promotes better data-driven decision-making within an organization.

Data maps typically include the following:

- Data Elements: these are lists of the individual data items or attributes used in the dataset or database. Each data element is given a unique name or identifier for easy reference.

- Data Type: This specifies the type of data contained in each data element, such as text, numerical, date, boolean, etc. Each data element is accompanied by a description that provides additional information about its meaning, purpose, and any other relevant details.

- Data Constraints: This defines any constraints or rules associated with the data elements, such as minimum and maximum values, allowable data ranges, or any dependencies between different data elements.

- Relationships: this defines the relationships between the different dataset or database contains multiple tables or data entities.

- Source and Origin: This gives information about the source of the data, where it originated, how it was collected, and any data transformations that were applied.

- Data Usage: This describes how each data element is used within the organization or the specific project, providing context for its importance and relevance.

Datasets:

Datasets are collections of structured data that are organized and presented in a meaningful way for analysis, research, or other purposes. They consist of individual data points or instances, often represented as rows in a table, where each row corresponds to a specific observation or record. Each column in the table represents a particular attribute or feature of the data. Datasets can be used in various fields and applications, such as machine learning, data science, statistics, business intelligence, and academic research. They serve as the foundation for training machine learning models, conducting statistical analyses, making data-driven decisions, and drawing insights from the information contained within the data. Today's datasets include both Audio and Visual Datasets

Datasets can be created through data collection processes, such as surveys, experiments, observations, or web scraping. They can also be obtained from publicly available sources, research institutions, or data repositories. Some well-known datasets used for research and benchmarking in various domains include the MNIST dataset for handwritten digit recognition,

the Iris dataset for classification tasks, and the IMDb dataset for movie reviews sentiment analysis.

When working with datasets, it is essential to ensure data quality, handle missing values, and perform necessary preprocessing tasks to prepare the data for analysis or model training. Additionally, considering data privacy and adhering to ethical guidelines is crucial when dealing with sensitive information in datasets.

Datasets can come in different formats including:

- Tabular Datasets: Data is represented in tabular form, with rows and columns. Common formats include CSV (Comma Separated Values), Excel spreadsheets, and database tables.
- Image Datasets: Data contains images along with associated metadata or labels. They are widely used in computer vision tasks, such as object recognition and image classification.
- Text Datasets: These datasets consist of text documents or sequences of words, often used for natural language processing (NLP) tasks like sentiment analysis, language translation, and text classification.
- Time Series Datasets: These datasets contain data points recorded over time, making them useful for analyzing trends and patterns in temporal data.
- Graph Datasets: These datasets represent data as graphs or networks, where entities are nodes and relationships are edges. They are common in social network analysis and other graph-based applications.

ANNEX B: INTERNATIONAL CONTEXT

Some countries cover data protection and data sharing in a single piece of legislation, while others have separate pieces of legislation covering each subject.

A. EU GDPR

The European Union's Data Governance Act complements their 2019 Open Data Directive and seeks to establish sound mechanisms to facilitate not merely the use, but the secure reuse of specific categories of protected public-sector data. Such data include data that are subject to the rights of others, e.g. intellectual property rights, trade secrets and personal data. It is also important to underscore that the resource requirements for the implementation of the law are crucially important, in respect of human capacity and other capital. The Act further enhances trust in data intermediation services and further promotes data altruism.

The Data Governance Act and the European Data Act better positions the European Union to successfully implement digital transformation initiatives which promote and are intended to facilitate the achievement of climate goals, enhanced effectiveness and efficiency in commercial transactions and greater security in virtual social interactions; data represents a core component in this cycle. The Data Governance Act creates a framework for a new business model, providing an enhanced secured environment for companies to share data - data intermediation services. For businesses, these services may take the form of digital platforms, wherein voluntary data-sharing arrangements between companies or statutory data-sharing requirements will be featured. Through the utilization of these services, businesses can feel comfortable sharing their data.

The EU GDPR is recognised by many jurisdictions as one of the international standards for data protection. The EU GDPR features provisions which are intended to guarantee the rights of data subjects. Accordingly, this model regime establishes the following in respect of data processing:

- processing should be based on clear, precise and accessible rules;
- the data controller should demonstrate the necessity and proportionality of the processing based on legitimate objectives;
- the processing should be subject to independent oversight; and
- data subjects should have access to effective remedies.[2]

These precepts of necessity, proportionality, sound governance and redress are noted to be some of the core features of the GDPR which are intended to govern the protection of the rights of individuals in respect of data sharing.

Another principal development in the international sphere which must be considered both within the scope of this policy framework and the legislative framework relates to open data and data sharing. The EU Data Report on Data Sharing for Public Good[3] was released in February 2020 and speaks to the proposal of the creation of a regulatory framework for Open Data. Many of their provisions can be adopted for PNG.

Furthermore, with Artificial Intelligence (AI) no longer being an abstract concept but a real reality that affords numerable significant benefits. Globally, countries and regional blocks have

been developing blueprints to guide their strategies in respect of leveraging the benefits which AI present.

One way of increasing Business-to-Government (B2G) data sharing is to make data sharing in the easier by taking policy, legal and investment measures in three main areas:

Governance of G2B data sharing: such as putting in place national governance structures, setting up a recognised function ('data stewards') in public and private organisations, and exploring the creation of a cross APEC regulatory framework.

B. UNITED KINGDOM

The United Kingdom combined data sharing and protection provisions into a single law, the Data Protection Act of 2018.[6] Under the Act, the Information Commissioner prepares a mandatory code of practice, which contains practical guidance on the sharing of personal data according to section 121.

Under this law, the Data Protection commissioner may also include any other guidance promoting good practices in the sharing of personal data that he considers appropriate.

C. NEW ZEALAND

New Zealand merged both its data protection and sharing principles into one piece of legislation, the New Zealand Privacy Act of 2020[7]. The Act took effect in 2020, replacing an older Act from1993 and making New Zealand GDPR compliant. Through its thirteen Privacy Principles, the Act governs all handling of personal information and is enforced by the Privacy Commissioner. It makes it mandatory for users to be informed about collection, use, and sharing of their personal information. Additionally, it empowers users to access and correct their data. This applies to all websites, companies, or organizations that handle personal information within New Zealand, regardless of where in the world they are located.

New Zealand's Privacy Act of 2020 is principles-based and "open-textured," meaning that the application of the Act must be undertaken utilizing one's judgement and the privacy principles are therefore applied and assessed relative to each individual case.[8]

One of the foremost features of The Privacy Act 2020 of New Zealand is its flexibility, thus allowing it to be applied in the ever-changing dynamic global environment. The Act is principles-based and 'open-textured' meaning that the application of the Act must be undertaken utilizing one's judgement and the privacy principles are therefore applied and assessed relative to each individual case.

A key theme of the Privacy Act is information sharing. Data and information sharing are quite crucial to the operations of several public and private entities. A multiplicity of organisations

[6] 90 UK Public General Acts. Data Protection Act 2018.
[6] Parliamentary Council Office. New Zealand Legislation. Privacy Act 2020. Version as of 28 October 2021

[8] Parliamentary Council Office. New Zealand Legislation. Privacy Act 2020. Version as at 28 October 2021. https://www.nationalassembly.gov.bz/wp-content/uploads/2021/10/Act-No-27-of-2021-Public-Sector-Data-Sharing.pdf

often needs to collaborate and share data and information to provide efficiency and effective services. The importance of data sharing, particularly through electronic platforms has been underscored during the current pandemic. Public organisations have recognized that through joint collaborations, quality services can be delivered in an easily accessible and cost-effective manner.[9] The efficiency of the delivery of service is further enhanced should the service user only be required to access an online platform at one place, and through interoperable systems, access information stored on several e-platforms of public organisations and government departments.

To achieve this, there must be a user-friendly interface, system connectivity and interoperability and information sharing protocols. In addition, issues in respect of privacy and data protection are also relevant to the discussion. Ensuring that these key elements are featured in information sharing systems to promote collaboration and efficient service delivery can be challenging, owing to issues relating to:

- Data Accessibility, Reliability and Management
- Identifying and Implementing Cost Sharing Mechanisms
- Varying levels of data maturity
- The application of subjectivity to the interpretation of 'Data Privacy'
- Governance and Ownership

New Zealand created the Integrated Data Infrastructure (IDI) where data sets held by Statistics New Zealand are collated from a range of public organisations. Strict rules and principles of confidentiality, privacy and anonymity of the data were applied in the implementation of this intervention. The IDI provides a mechanism through which organisations were afforded the unique opportunity to locate and use reliable data to inform their policy decision making processes.

Data management is also key, and the New Zealand model adopted the following principles in the use of its IDI: [10]

- The application of the Once only principle to Data, meaning that data is collected once and reused as many times as required
- Real time compilation of data
- Development of clear data management standards in alignment with national laws and international best practices
- Open data

D. South Australia

South Australia has a stand-alone Public Sector (Data Sharing) Act 2016. Their Act establishes an Office for Data Analytics and prescribes requirements and responsibilities in respect of information sharing in South Australia, more specifically sharing of data between public sector agencies and the provision for the sharing of data between public sector agencies and other entities.

The Act establishes provisions for facilitating public sector data sharing and prescribes trusted access principles and authorization requirements in respect of public sector data sharing activities. Data sharing safeguards are also established under the Act particularly in respect of confidentiality

[9] https://oag.parliament.nz/2018/public-sector-data/sharing-data
[10] https://oag.parliament.nz/2018/public-sector-data/sharing-data

and commercial-in confidence, data custody and control safeguards and other data sharing safeguards. The Act grants the Minister the power to enter into data sharing agreements with relevant entities.