NATIONAL DATA GOVERNANCE AND PROTECTION POLICY

3nd Draft (V1.1)

Table of Contents

EXECUTIVE SUMMARY

The National Data Governance and Protection Policy provides a framework for the responsible use, management, and governance of data across public and private sectors in Papua New Guinea. The policy aims to mitigate risks associated with the increased use of data, including data breaches and misuse, by providing clear guidelines on how data should be collected, stored, processed, and used.

This policy represents a significant milestone in Papua New Guinea's efforts toward digital transformation, and more importantly, the protection of personal data and privacy rights of its citizens. As the world becomes more digitized, data has become an asset and is fundamental to the economic, social, and political development of the country. However, with the increased use of data comes the risk of data breaches and misuse, which can have significant consequences for individuals and society.

The policy aims to promote a digital ecosystem that is secure, trustworthy, and respects the rights of the people of Papua New Guinea. The policy outlines the key principles of data governance and protection, including the need for transparency, accountability, and respect for privacy rights. It establishes the roles and responsibilities of stakeholders in the data ecosystem, including data controllers, data processors, and data subjects, and outlines the procedures for handling personal and sensitive data.

The policy establishes the legal framework for data protection and governance, which includes the principles of data minimization, purpose limitation, and data accuracy. The policy also recognizes the importance of cross-border data flows and provides for adequate safeguards to ensure that the transfer of data is done in accordance with international standards.

The policy recognizes the importance of promoting data literacy and building capacity in data management, and provides guidance on data ethics and security measures to ensure the protection of personal data. It also outlines the procedures for handling data breaches and the consequences of non-compliance with the policy.

This policy applies to all data controllers, processors, and handlers, both in the public and private sectors, that collect, store, process, and use personal data. It also sets out the roles and responsibilities of different stakeholders in ensuring compliance with the policy.

Overall, the National Data Governance and Protection Policy is a crucial step toward building a digital ecosystem that is secure, trustworthy, and respects the rights of the people of Papua New Guinea.

PART A: 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 development opportunities 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.

In recent years, information has increasingly become a critical resource that has to be managed carefully. Data, including personal data, is generated, processed, stored, and distributed in new and complex ways due to technological growth. The GoPNG acknowledges the importance of accessing data and safeguarding it as articulated in the National ICT Policy, ICT Roadmap, Digital Transformation Policy, Digital Government Act.

As a result, the transformative developments in computing are presenting major concerns for privacy and security in the way data is processed. On a daily basis, vast amounts of data, including personal data, are collected, transmitted, and stored globally by ever-growing computing and communication technologies. Data is a critical resource that drives economic growth and development in this century, and as such, data protection is increasingly becoming a critical area that requires careful management.

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 also increasingly use and collect 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 can 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.

Both the public and private sectors collect, use, and transfer data at an unprecedented scale and for multiple purposes. This data can be put to beneficial use, however, the unregulated and arbitrary use of data has raised concerns regarding the privacy and control over such data by the data subject.

The Government of PNG values the protection of data. All actors involved in the management of data are expected to respect the requirements of safeguarding data. The Government recognizes that this protection is an essential element in maintaining public trust in entities managing data and is essential for the socio-economic development of PNG in the fourth industrial revolution.

Today's digital technology ecosystem relies on data. Data increasingly underpin digital transformation and have become an important source of value, for example, for decision-making and production. While issues around data span across policy areas and are addressed throughout the report, it is important to first understand data as a critical resource and a source of value, as well as some transversal policy challenges related to data.

Access to data is crucial for competition and innovation in the digital economy – not only for businesses but also for governments and individuals. Overall, data access and sharing is estimated to generate social and economic benefits worth between 0.1% and 1.5% of gross domestic product (GDP), in the case of public-sector data, and between 1% and 2.5% of GDP when also including private-sector data.[1]

[1]OECD (2019), Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en.

1.0 BACKGROUND

Data is a vital resource for its monetisation potential and ability to contribute significantly to numerous processes and activities that drive commerce, government services, and other quotidian activities. There are significant risks associated with the misuse and manipulation of data. Moreover, consumer protection standards are being created to reduce potential harms arising from the use of data to protect individuals. Consumer protection principles are intended to achieve a fair, healthy, and sustainable digital economy.[2] Having a keen understanding of data policy and related issues aids in minimizing possible adverse effects of data usage and further promotes efficient and responsible data practices.

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 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 mission parameters, and maintains a unique culture. In this evolving environment, working with data and data management have become disciplines key to organizational success.

Privacy is becoming a flashpoint in digital transformation. 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.[3]

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 contribute around USD 2.8 trillion to global economic activity, or 3.5% of global GDP[4].

---

[2] European Consumer Organisation, Regulating AI to protection the Consumer: A Position Paper on the AI Act https://www.beuc.eu/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf

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

[4] 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.

In many cases, data access and sharing generate positive social and economic benefits for data providers (direct impact), their suppliers and data users (indirect impact), and the wider economy (induced impact). Quantifying the amount data access and sharing can increase the value of data to holders (direct impact), but it can help create 10 to 20 times more value for data users (indirect impact), and 20 to 50 times more value for the wider economy (induced impact). In some cases, however, data access and sharing may also reduce the producer surplus of data holders. Overall, these studies suggests that data access and sharing can help generate social and economic benefits worth between 0.1% and 1.5% of gross domestic product (GDP) in the case of public-sector data, and between 1% and 2.5% of GDP (in few studies up to 4% of GDP) when also including private-sector data.

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.[5] In 2013, the OECD recommended that "Any restrictions to transborder data flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing".[6] Currently, an array of measures is making some cross-border data flows conditional or banning them altogether, with economic consequences, not least for trade transactions.[7] 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. The challenge is to preserve the significant economic and social benefits flowing from data-enabled trade, research, and other activities. This underscores the importance also of better understanding the heterogeneity of data flows.

2.0 DEFINITIONS

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.

However, the increasing reliance on electronic data also raises concerns about data privacy, security, and access. Effective measures must be taken to protect electronic

[5] 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.
[6] OECD (2013), "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", OECD Digital Economy Papers, No. 229, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k3xz5zmj2mx-en.
[7] OECD (2019d), "Trade and Cross-border data flows", OECD Trade Policy Papers, No. 220, OECD Publishing, Paris, http://dx.doi.org/10.1787/b2023a47-en.

data from unauthorized access, use, disclosure, or destruction, as well as to ensure its accuracy, integrity, and availability.

Data Protection

Data protection refers to the measures taken to safeguard all ranges of data, including personal data, confidential information, intellectual property, and sensitive business data. It involves implementing appropriate security measures to prevent unauthorized access, theft, and loss of data. Additionally, data protection involves ensuring that data is not misused, mishandled, or unlawfully processed. By protecting data, individuals and organizations can safeguard their privacy, maintain the confidentiality of sensitive information, and prevent damage to their reputation and financial standing.

At its core, data protection is a right to privacy that people have against the possible unauthorized use of personal information by a data processor. The objective of this discipline is to protect the privacy of a person at risk for the collection and misuse of personal data. Data protection allows people to know who and for what purposes their personal data is being processed and gives them the ability to object to improper use. Control over personal data consists of the possibility of opposing the prosecution and/or obtaining, correcting, and objecting to the use of data once it has been obtained by a processor or a third party.

In any case, the processing must be fair, legitimate, and for a limited purpose. Data protection allows individuals and organizations more control over how they share their data with data processors, whether it be the state or an individual. On the other hand, it establishes the obligations of data processors: they must obtain the free and informed consent of the person prior to processing; ensure measures to guarantee the integrity and confidentiality of data; and in case of sharing information, they must ensure that third parties comply with the same level of protection. When a breach occurs by the data processor, the person may object and request the correction or deletion of personal data.

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 Protection Principles

While the data protection principles are primarily focused on protecting personal data, they can also be applied to other types of data sets, such as confidential business information, intellectual property, and sensitive government data. In general, the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability are fundamental to responsible data handling, regardless of the type of data being processed. By applying these principles to all data sets, individuals and organizations can ensure that information is handled in a way that is ethical, secure, and trustworthy.

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

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, organizations, 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.

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.

As technology continues to advance, the processing of personal data has become more common in various economic and social activities. This presents new challenges

for data protection, as the use of personal data must be balanced with the need to protect individuals' privacy. However, the meaning of privacy and the right to privacy varies across different countries and regions. 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.

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

Data portability

Data portability is the ability to use the same data for cross-sectoral purposes while at the same time, strengthening the rights of individuals over their personal data and businesses, especially SME's rights over their own data. Data portability provides restricted access through which data holders can provide customer data in a commonly used, machine-readable structured format, either to the customer or to a third party chosen by the customer.

However, it's important to note that in Papua New Guinea, some data is considered too confidential to be shared openly with the public. In these cases, restricted data-sharing arrangements may be more appropriate. This is especially true when there are privacy, intellectual property, and organizational or national security concerns that legitimately prevent open sharing.

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.

Data processing is subject to various laws and regulations that govern the collection, storage, use, and disclosure of personal data. It is important to ensure that data processing activities comply with these laws and regulations to protect individuals' privacy and prevent the misuse of personal data.

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

A Data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

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 protection in hands of public and private sector

There are two major categories of personal data processing: the government, and the private sector. It is important to understand the difference between the types of information and types of processors. On the one hand, aims and incentives for information collection varies depending on the type of actor and, on the other, individual rights are also different compared to the government than they are to the private sector. In several States, inclusive, there are different legal regimes for each.

Regarding the public sector, government agencies and state agencies, obtain personal information of citizens to control and regulation of the country, for example on personal identity, education, health services, tax collection, national security, and several other government services. The government processes data such as birth, death, marital status, property, and income of citizens, etc.

For the private sector, individuals and/or corporations (in particular the country's economic actors) use electronic platforms to perform daily activities. Also, the use of internet, search engines, social networks, and electronic communication systems, collect information about the person consistently. To this end, private companies may have access to personal information used for commercial purposes. This information may include credit information, phone number, political or religious preferences, home, travel, etc.

Both sectors, although the type of information they process is different, they must ensure the protection of personal data in accordance with the laws and practices.

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.

Data governance is the process of setting and enforcing priorities for managing and using data as a strategic asset. The key activities of data governance are:identification, policy, assessment, oversight and communications

Secured Data Exchange (SDE) is a secure and encrypted platform that allows users to exchange sensitive data and information with others. The platform provides a secure way to send and receive data, ensuring that the data is protected from unauthorized access, interception, or modification.

SDE platforms are typically used by organizations and individuals who need to share sensitive data, such as financial information, medical records, or personal data, with others. The platform may use encryption technologies to protect the data both during transmission and at rest, and may also provide features such as access controls, audit trails, and user authentication to ensure that only authorized users can access the data.

Restricted Data-Sharing Arrangements

In Papua New Guinea, some data are considered too confidential to be shared openly with the public. In this case, restricted data-sharing arrangements are more appropriate. This is the case when there may be privacy, intellectual property and organizational or national security concerns legitimately preventing open sharing.

PART B: POLICY OBJECTIVES, GOALS, AND ALIGNMENTS.

1.0. POLICY OBJECTIVES AND GOALS

1.1 Vision

The vision of this policy is to;

i. Enhance data centric decision that promotes better outcomes for socioeconomic developments.

ii. strengthen the national data protection and data sharing regime

iii. facilitate innovation and enable effective digital transformation initiatives

iv. enhance the trade and business environment

v. establish a national data governance architecture and legislative framework for the Government of Papua New Guinea

vi. emphasizes collaboration with other agencies as a keystone for the success of the GoPNG vision.

1.2 Mission

The mission of this policy is to;

i. implement a shared, integrated government data hub in a central coordinated manner, in order to improve the delivery of public services to all citizens and stakeholder in a cost-effective way.

ii. achieve an enhanced data protection and data sharing regime through the development of a framework which advocates and facilitates the infusion of international best practices, fosters enhanced accountability and data integrity,

iii. facilitate the expansion of the scope and coverage of the rights of data subjects where the privacy of individuals are protected, and data sharing is used to facilitate innovation and effective digital transformation in-line with international best practices.

1.3 Goals

Goals of the Data Governance and Protection policy:

- **Goal 1:** Develop and implement specific laws for data privacy, protection, and governance to safeguard all types of data, including personal, public, and business data, from unauthorized access, disclosure, or misuse.

- **Goal 2:** Educate and inform the PNG government on best practices for managing all types of data, and to ensure that the government is committed to protecting the data of its citizens and businesses, including sensitive data.

- **Goal 3:** Raise public awareness about the importance of managing data, and to encourage individuals and organizations to commit to protecting data and keeping it secure, irrespective of its type.

- **Goal 4:** Engage with stakeholders from various government agencies and businesses, and solicit their input on the current state of data management activities in PNG, and to use this information to select a data maturity assessment model that is appropriate for PNG's context.

- **Goal 5:** Establish and enforce data sharing policies and mechanisms that protect the privacy and security of all citizens and businesses and the information they supply, especially in cases where health information or personal information is being shared.

- **Goal 6:** Ensure that all data collected, processed, and stored in PNG is done so in compliance with the applicable laws and regulations and international best practices, and to establish penalties for non-compliance.

- **Goal 7:** Establish a data protection authority that will be responsible for overseeing and enforcing data protection and privacy regulations, as well as investigating complaints and breaches.

- **Goal 8:** Collaborate with other countries and international organizations to promote the exchange of best practices and lessons learned on data governance and protection.

- **Goal 9:** Promote the development of local expertise and capacity in data governance and protection, through training programs, seminars, and workshops.

- **Goal 10:** Continuously monitor and review the effectiveness of the data governance and protection policy and to make necessary adjustments and improvements to ensure that it remains relevant and effective in protecting the privacy and security of all citizens and businesses in PNG.

1.4 Objectives

This policy has been developed to;

i. ensure the effectiveness and secure management of data by;

   a. identifying, assessing, monitoring and mitigating privacy risks in programs or activities involving the collection, retention, use, disclosure and disposal of data.

ii. providing a framework for data sharing, management and governance across the public sector and with stakeholders by;

   a. ensuring that data is securely managed, accessed, and is used responsibly and for legitimate purposes.

   b. promoting the effective and efficient management of data assets for government and citizens.

iii. sets out the principles and objectives for data governance, as well as the roles and responsibilities of stakeholders by;

   a. encouraging the responsible use of data and respect for the privacy of individuals.

   b. creatings a shared data culture while facilitating the sharing of data between government, business, and the citizens.

   c. fostering a culture of awareness in respect to data protection and privacy

iv. provide a clear understanding of regulatory requirements, standards, and processes by;

   a. aligning the governance, regulatory, and institutional arrangements

   b. developing standards in relation to data privacy

   c. ensuring consistency in practices and procedures in developing and administering the privacy and data protection laws.

   d. ensuring that data is appropriately protected, stored, and disposed of in accordance with applicable laws and regulations.

v. promote the use of data to support government decision-making by;

   a. ensuring that data is used to support and improve the delivery of government services.

1.5 Policy Scope

This policy is a government-led initiative that seeks to establish a framework for the collection, management, analysis, use, and sharing of data across all sectors of the country. The policy focuses on five key areas:

i. **Establishing a data governance, data protection, and data privacy framework**.

These includes;

a. establishing a data protection and privacy structure,
b. setting out key principles and responsibilities, and
c. ensuring that data is stored and managed in accordance with the law.

ii. **Strengthening data management and sharing**

These includes;

a. developing a data management and sharing infrastructure and protocols,
b. providing training and capacity building to ensure the effective use of data.

iii. **Strengthening data access and use**.

These includes;

a. improving access to data across government, the private sector and civil society,
b. developing a system for the secure and responsible use of data.

iv. **Strengthening data security and privacy.**

These includes;

a. strengthening the protection of data and ensuring that privacy considerations are taken into account in the collection, management and use of data.

v. **Developing data-driven innovation.**

These includes;

a. encouraging the use of data to drive innovation and development,
b. identifying areas of opportunity for data-driven initiatives.

2.0. POLICY AND LEGAL MANDATE

2.1 Policy Mandate

The National Data Governance and Protection Policy is aligned with several key national policies and strategies, including the;

- ICT Sector Roadmap 2018
- Papua New Guinea Startegy for the Development of Statistics 2018 -2027
- PNG Digital Transformation Policy 2020
- National Cyber Security Policy 2021,
- Papua New Guinea Open Government Partnership National Action Plan 2022 - 2024
- Digital Government Act 2022
- Digital Government Plan 2023 -2027

The alignment with these policies and strategies highlights the importance of data governance and protection in achieving the country's development objectives and ensuring the security and privacy of citizens' data. The policy mandates the development and implementation of data privacy, data protection, and data governance laws that are specific to the needs and values of Papua New Guinea.

2.2 Legal Mandate

The National Data Governance and Protection Policy is aligned with various national legislations, including the;

- Digital Government Act 2022,
- Cyber Crime Code Act 2016
- Civil Registration (Amendment) Act 2014
- Statistics Act 1993
- Protection of Private Communication Act 1973
- Criminal Code Act

These legislations provide a strong foundation for the policy and ensure that data governance and protection practices are legally enforceable and supported by the government. The policy also mandates the government to develop and implement specific data privacy, protection, and governance laws that are tailored to the needs and values of Papua New Guinea, in order to protect personal, public, and business data from unauthorized access, disclosure, or misuse. It also aims to promote public awareness and educate stakeholders on best practices for managing all types of data, as well as enforce data sharing policies and mechanisms that protect the privacy and security of citizens and businesses.

3.0. POLICY STATEMENT

The Data Governance and Protection Policy aims to establish and enforce data sharing policies and mechanisms that protect the privacy and security of all citizens and businesses and the information they supply, especially in cases where health information or personal information is being shared. The policy recognizes that the effective management and protection of data is essential for maintaining public trust in entities managing data and essential for the social-economic development of Papua New Guinea.

The Data Governance and Protection Policy seeks to establish a comprehensive legal and regulatory framework for the protection, management, and sharing of all types of data in Papua New Guinea. The policy aims to align the national framework with international best practices and standards to ensure that data is managed and shared in a safe, secure, and transparent manner.

The policy recognizes the critical role that data plays in driving economic growth and development in the 21st century and seeks to ensure that this resource is managed carefully to protect the fundamental rights and freedoms of individuals, particularly the right to privacy.

To achieve these objectives, the policy seeks to promote and strengthen the institutional governance framework for data management, sharing, and protection. It defines governance mechanisms and establishes a legislative framework to ensure that all actors involved in the management of data respect the requirements of safeguarding data.

The policy also aims to raise public awareness about the importance of managing data and encourages individuals and organizations to commit to protecting data and keeping it secure. Additionally, it seeks to engage with stakeholders from various government agencies and businesses to solicit their input on the current state of data management activities in Papua New Guinea and to use this information to select a data maturity assessment model that is appropriate for the country's context.

PART C: PRINCIPLES OF DATA GOVERNANCE AND DATA PROTECTION

1.0 BASIC PRINCIPLES OF DATA GOVERNANCE

2.1 Privacy

The data governance policy framework;

i. includes provisions to protect the privacy of individuals and organizations who provide or use data.

ii. outlines specific measures for the protection of data privacy, such as the use of secure transmission and storage of data, the requirement of consent from data subjects, and the implementation of data access controls.

iii. outlines the measures that data controllers and processors must take to ensure the security of personal data.

iv. requires data controllers and processors to ensure that any data collected is used for the purpose for which it was collected and not used for any other purpose.

2.2 Security

This policy framework is designed to;

i. ensure the security and privacy of all data

ii. set out the responsibilities of relevant custodians in relation to data governance including data collection, storage, and processing as well as the management of data access and use.

iii. include measures to protect data from unauthorized access and disclosure,

iv. outline procedures for responding to security incidents, and data breaches.

v. provide guidance on how to use data responsibly and ethically.

vi. provide guidance on how to ensure the security and privacy of data.

2.3 Integrity

This policy framework is designed to;

i. maintain and ensure data integrity .

ii. outline the goals that should be followed to ensure the safe and secure use of data and information. These include principles such as data security, privacy, confidentiality, and data quality.

2.4 Transparency

This policy;

i. promotes the government's commitment to ensuring the responsible and effective use of data and its role in helping to improve the lives of citizens.

ii. provide guidance on the use of data and data governance principles

iii. defines and outlines the roles and responsibilities of different stakeholders.

2.5 Accessibility

This policy will ensure;

i. reliable access to data and information
ii. availability of data and information
iii. sharing of data and information

2.6 Accountability

This policy will;

i. ensure there's accountability for cross-functional data-related decisions, processes, and controls.

ii. define accountabilities in a manner that introduces checks-and-balances between business and technology teams as well as between those who create/collect information, those who manage it, those who use it, and those who introduce standards and compliance requirements.

iii. establish clear ownership and responsibilities for data throughout the organization, including data stewards who are responsible for the quality, security, and appropriate use of data.

iv. define accountabilities for stewardship activities that are the responsibilities of individual contributors, as well as accountabilities for groups of Data Stewards.

v. gives the responsibility to DICT for ensuring that the policy and strategy are implemented in accordance with the government's requirements, and for

providing guidance and advice to the stakeholders involved in their implementation.

vi. gives the responsibility to dict to monitor the implementation of the policy and strategy to ensure that they are meeting the objectives and goals set out in the policy and strategy.

vii. Gives the responsibility to DICT to report to the government on the progress of the implementation and any issues identified during the process.

2.7 Quality

This policy;

i. provides a framework to ensure sustainable data governance practices in the nation.

ii. outlines the roles of government and private sector stakeholders in the data governance process and outlines the national strategies to be adopted to ensure data governance is effective and up to date.

iii. outlines the principles and goals of data governance, including data security, data privacy, data integrity, data accuracy, and data accessibility.

iv. provides guidance on the implementation of data governance processes and outlines the roles and responsibilities of all stakeholders.

2.8 Confidence

This policy ensures;

i. the confidentiality of the data it collects and holds are maintained at all time.

ii. that all data collected and held by the Data Protection and Governance Authority is subject to strict confidentiality measures.

iii. data is only collected, used, and disclosed in accordance with the law and there are established procedures to protect the confidentiality and integrity of the data that all Government agencies collect and hold.

iv. There is procedures in place to maintain the confidentiality of data. These procedures include, but are not limited to;

   a. limiting access to data
   b. implementing security measures to protect data
   c. providing training to staff on how to manage data responsively.

2.9 Compliance

This policy will;

i. Ensure data-related decisions, processes, and controls subject to data governance will be auditable; they will be accompanied by documentation to support compliance-based and operational auditing requirements.

ii. ensure the safe and secure use of personal data across public and private sectors.

iii. establish a framework for data governance in the country, including the development of a national data landscape, data sharing mechanisms, and data security.

iv. It seeks to ensure that Papua New Guinea complies with international standards and best practice for data governance. This includes the implementation of effective data sharing mechanisms that protect personal data and ensure secure data access. The government will also work with stakeholders to

v. ensure that the policy is being implemented in accordance with the law.

vi. All stakeholders are expected to comply with the DGPF, as well as any other applicable laws and regulations.

2.0. BASIC PRINCIPLES OF DATA PROTECTION

1.1 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 in their operations and management. Moreover, the national governance frameworks must promote fairness and must not encourage, facilitate, or ignore the abuse of power in respect of data use, processing, management, or transfers.

1.2 Congruence with International Standards and Best Practices

International standards and best practices shall be pursued and implemented in the national data protection and data sharing architecture to preserve and protect the rights of persons as data subjects and govern the actions of data custodians.

1.3 Respect of Rights and Freedoms

The rights and freedoms of persons shall be respected in the accordance with the national legal framework and commitments of the Government of PNG under relevant regional and international agreements.

1.4 Responsible Data Management

Responsible data management is a key principle of data governance, and it involves ensuring that data is managed in a responsible and ethical manner. This includes ensuring that data is collected, stored, processed, and used in compliance with relevant laws and regulations, as well as with ethical and moral standards.

Responsible data management also involves ensuring that data is accurate, complete, and up-to-date, and that appropriate measures are in place to protect the data from unauthorized access, disclosure, or misuse. This includes implementing appropriate security measures, such as access controls, encryption, and firewalls, and ensuring that data is only accessed by authorized personnel who have a legitimate need for it.

In addition, 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. This includes obtaining informed consent from individuals before collecting their data and providing them with the opportunity to opt-out of certain uses of their data.

1.5 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.

It is essential to ensure that all relevant supporting laws underpinning key themes and elements to support the national ICT enabling framework are implemented. Key to this is national data sharing legislation which will enable the application of the once only principle to address issues such as effectiveness, efficiency and reduced administrative costs associated with the provision of government services. The importance and rationale for such a framework for data sharing is premised on the need for evidence-based planning and decision making, improved governance and the provision of guidance on the proactive disclosure of government data, among others.

1.6 Artificial Intelligence

Artificial Intelligence (AI) is no longer a mere 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.

AI solutions have been applied to identify and/or predict diseases and pests in crops just through the use of satellite images. It is further foreseen that AI can also be the transformative tool in addressing the global phenomenon of climate change. AI is therefore transforming the world one sector at a time. Noting the limited human involvement in AI, the cost savings in leveraging this technology can be as immense as the benefits it may yield.

1.7 Open Data and Data Sharing

The Data Protection and Governance Policy framework will promote innovation through the recognition and inclusion of principles and precepts relating to open data, data analytics, data sharing , and other data-drive products and services.

Open Data and Data Sharing are imperative in the current global context given the rise of electronic transactions, electronic commerce and electronic government services. Within PNG, the importance of these arrangements can be easily identified within the scope of the PNG's electronic Single Window or e-Government Portal. This Policy considers these concepts and offers relevant and adequate prescriptions.

Open Data refers to data that is available freely and easily accessible via the Internet. Open data is therefore downloadable, modifiable, and distributable without any legal or financial limitations.[8] The concept of "open data" represents one of several issues to be considered in respect of data sharing and it is therefore important that clear policy directions and decisions are made in this respect.

PNG's capacity to remain competitive in the digital economy is contingent upon its ability to harness the value of data. Data volumes are growing exponentially and so too is the potential value of this data. Publishing, linking, and sharing data can create

[8] https://www.library.yorku.ca/web/open/overview/open-data/

opportunities that neither government nor business can currently envisage. Publishing appropriately anonymised government data will stimulate innovation and enable economic outcomes.

The data held by the PNG Government is a strategic national resource that has considerable value for growing the PNG economy, improving service delivery, and transforming policy outcomes for PNG. The GoPNG recognizes the importance of effectively managing this national resource for the benefit of all PNG Citizens. In this policy we commit to optimizing the use and reuse of public data; to release non sensitive data as open by default; and to collaborate with the private and research sectors to extend the value of public data for the benefit of the PNG Citizens.

Public data includes all data collected by government entities for any purposes. Non-sensitive data is anonymized data that does not identify an individual or breach privacy or security requirements. This is defined in the Digital Government Act Paragraph 36.

3.0. DATA PROTECTION, CLASSIFICATIONS, DATA SHARING MODELS AND DATA GOVERNANCE

3.1 Data Classifications & Security

Data owners have to classify their data based on their sensitivity and apply appropriate security security measures in order to increase the protection of data when it's shared between different stakeholders.

Proper security controls must be in place at all times to protect data and information from unauthorized disclosure, alteration, or destruction. The consequences of mishandling or unauthorized disclosure of data could lead to significant harm to individuals, organizations, or national interests, and data owners should classify their data accordingly. By classifying data according to the categories identified, organizations can identify the appropriate security measures needed to protect it, such as encryption, access controls, and monitoring.

Following are categories of data classification identified:

i) **Public (Open) Data:** This category refers to data that is intended for or open to public disclosure, such as press releases or other publicly available information. It requires little to no protection and can be freely accessed by anyone but not modifiable by the public. Mishandling of public or open data does not have any significant consequences.

ii) **Internal Use Only Data:** This category refers to any data that is generated, collected, and stored within an organization for internal use only. It may contain sensitive information that should be protected, but not to the same extent as confidential or top secret data.

iii) **Confidential Data:** This refers to data that requires security protection beyond that determined to be public/open or office use only. It refers to data that contains sensitive or confidential information, such as personal or financial data, intellectual property, or trade secrets. Confidential data is classified into two categories based on sensitivity:

a) **Sensitive Data**: This includes data that, if disclosed or accessed without proper authorization, could result in minor to moderate reputational damage to the organization, financial loss, legal actions, compromise of national interest, or other negative impacts. Security requirements for sensitive data include access controls, encryption, and regular monitoring to detect and prevent unauthorized access. It requires strict protection and access controls to ensure that it is not disclosed to unauthorized parties.

b) **Restricted or Highly Sensitive Data:** This refers to data that justifies heightened protective measures to defend against determined and highly capable threat actors. If disclosed or accessed without proper authorization, highly sensitive data could result in major reputational damage to the organization, serious financial loss, legal actions,

compromise of national interest, or other negative impacts. Security requirements for highly sensitive data include strict access controls, multi-factor authentication, encryption, regular vulnerability assessments, and continuous monitoring. This category of data should be accessed only by authorized personnel. Examples include classified government information, sensitive research data, or medical records.

iv) **Top- Secret Data:** This refers to the most sensitive data that requires the highest level of protection from the most serious threats. If unauthorized disclosure, alteration, or destruction of top-secret data occurred, it could result in significant harm to national security or endanger sources of information. Security requirements for top secret data include strict access controls, multi-factor authentication, encryption, regular vulnerability assessments, continuous monitoring, and physical security measures.

Policies, standards and guidelines will be developed for the identified categories accordingly. All the standards, specifications and guidelines or code of practice will be developed in consultation with existing policies and legislations such as the Digital Government Act 2022.

3.2 Data Access

Data access refers to the ability of authorized users or entities to obtain and use data. Data access can be categorized into two types: public access and personal access.

Public access refers to the availability of data to the general public, often through open data initiatives such as open government, including forthcoming access to information policy and legislation or publicly available datasets. Public access data is usually made available with the aim of promoting transparency, accountability, and innovation. Examples of public access data include government statistics, environmental data, and social media data.

Personal access refers to the access of data by individuals or entities for specific purposes or tasks. Personal access data is often protected by data privacy laws and regulations, and access is granted only to authorized personnel who have been granted permission to access the data. Examples of personal access data include customer information, patient records, and financial records.

Both public access and personal access data require careful management to ensure that they are accessed only by authorized personnel and that they are used in compliance with data privacy laws and regulations. Data access controls such as authentication, authorization, and encryption are essential to ensure that data is accessed only by authorized personnel and that it is protected from unauthorized access, theft, or misuse.

Organizations should establishing a set of security measures that controls who has access to the data.

Policies, standards and guidelines will be developed for data access accordingly. All the standards, specifications and guidelines or code of practice will be developed in consultation with existing policies and legislations such as the Digital Government Act 2022.

3.3 Data Sharing (Government-to-Government, Government-to-Business, and Government-to-Citizens)

All key government agencies that deal data including statistical data, health data, citizen data, etc. are to collaborate and work closely with each other including the businesses. To provide effective and efficient delivery of services, data should be shared amongst government-to-Government (G2G), Government-to-Business (G2B), and Government-to-Citizens (G2C). Key data stakeholders such as NID, NSO, NDoE, NDoH, etc have to share data amongst themselves including business to complete business process, deliver services, development of planning, update citizen records, implement policies, etc. The G2G and G2B can collaborate with each other to share its data through one or all of the following ways:

a) **Memorandum of Understanding (MOU**): an agency can establish MOUs with other government agencies, research institutions, or non-governmental organizations to outline the terms of data sharing and collaboration.

b) **Data Sharing Agreements (DSA):** These are formal agreements between an agency and other organizations both government and non-government that specify the terms and conditions for sharing data. The agreements may include provisions for data security and confidentiality, data ownership, and permissible uses of the data.

c) **Data Access Policies:** an organization can develop its data access policies that outlines the procedures for requesting and accessing data. These policies can include provisions for data sharing with other organizations and businesses, including citizens subject to appropriate data security and confidentiality measures based on its sensitivity.

d) **Data Sharing Platforms:** all public bodies should use the Secured Data Exchange (SDE) platform that will be establish by DICT which will allow authorized users from other agencies to access its data. The SDE will be designed to ensure data security and confidentiality, while allowing for seamless data sharing between G2G, G2C and G2B.

e) **Interagency Data Sharing Workshops**: an agency can organize interagency data sharing workshops to promote data sharing and collaboration among different organizations. These workshops can provide an opportunity for agencies to share their data needs and capabilities, and identify opportunities for collaboration.

The sharing of data between agencies and organizations will ensure that there is no duplication in the collection of data, especially citizen data and ensure data privacy is respected. It will also enable integration of data and interoperability of systems. It is important to note that data sharing must be done in compliance with relevant laws, regulations, and policies governing data privacy and security.

3.3 Secure Data Sharing

Effective and efficient delivery of public services are achievable when data are shared securely between stakeholders for the automation of processes. For example, if different government agencies can access and share data with each other, it can help eliminate duplication of efforts and improve the accuracy and timeliness of information used to deliver services.

The sharing of data between stakeholders either government-to-government, Data owners should choose one of the decentralised data sharing models that best fit their operations: This means that data owners, such as government agencies, should choose a decentralized data sharing models that is most appropriate for their specific needs and operations. There are several types of decentralized data sharing models, including peer-to-peer (P2P) networks, blockchain technology, and distributed ledger technology (DLT) which allows data to be shared securely between different entities without the need for a centralized authority.

The sharing of data between stakeholders either government-to-government, government-to-businesses, or government-to-citizens should only be done on the Secured Data Exchange Platform: This means that all data sharing should take place on a secure platform developed by the Department of Information and Communications Technology (DICT) in accordance with the Digital Government Act 2022. This platform will ensure that data is shared securely and in compliance with data protection and privacy laws and regulations.

3.4 Data Governance

Data governance is an integral part of overall governance within an organization, as it helps to ensure that data is managed effectively and in alignment with the organization's goals and objectives. Here are some key activities for data governance for the whole of governance:

1. **Aligning data governance with organizational goals:** Data governance activities should be aligned with the organization's overall mission, vision, and strategic objectives. This involves understanding how data supports the organization's goals, and establishing data governance policies and practices that align with those goals.

2. **Ensuring executive sponsorship:** Data governance requires strong executive sponsorship to ensure that it is given the necessary resources, attention, and support. Senior executives should be involved in setting the organization's data governance agenda, providing oversight, and ensuring that the necessary resources are allocated to support data governance activities.

3. **Establishing a data governance framework:** A data governance framework provides a structured approach to managing data throughout its lifecycle. The framework should include policies, procedures, and guidelines for managing data quality, privacy, security, and access, as well as roles and responsibilities for implementing and enforcing these policies.

4. **Building a data governance team:** A dedicated data governance team can help to ensure that data governance policies and practices are effectively implemented and maintained. The team should include individuals with expertise in data management, data security, data privacy, and related areas.

5. **Engaging stakeholders:** Effective data governance requires engagement with stakeholders across the public sector, and the private sector as well. Stakeholders should be involved in the development of data governance policies and practices, and should be provided with training and support to ensure that they understand and comply with these policies.

6. **Overseeing data flow/data sharing between different agencies:** A data governance body should be established to oversee data sharing activities between agencies. This body should have the authority to review data sharing agreements, monitor compliance with data sharing protocols, and resolve disputes.

   By overseeing data flow and data sharing between different agencies, data governance can help to ensure that data is shared in a secure and controlled manner, while also protecting the privacy and confidentiality of individuals whose data is being shared. This can help to improve the effectiveness and efficiency of government services, while also ensuring that data is used in a way that is consistent with legal and ethical standards.

7. **Monitoring and measuring data governance effectiveness:** Data governance effectiveness should be monitored and measured over time to ensure that it is achieving its goals and objectives. Metrics such as data quality, data security incidents, and compliance with data governance policies can be used to track progress and identify areas for improvement.

Overall, effective data governance requires a holistic approach that takes into account the organization's overall governance structure, goals, and objectives. By aligning data governance with overall governance, organizations can ensure that their data is effectively managed and protected, and that it is used to support the organization's goals and objectives.

PART D: POLICY FOCUS AREAS

1.0. INSTITUTIONAL FRAMEWORK

The institutional framework for data governance and protection is the organizational structure and processes that will ensure the effective implementation of the policies and practices related to data governance and protection. This framework will help to ensure that there is a consistent approach to data management across all government agencies and businesses in Papua New Guinea.

The policy is under the responsibility and accountability of the Secretary of DICT. The compliance to this policy shall be ensured by the Office of Data Governance and Protection Regulator, which will be a new office established under this policy and under the future Data Protection Act. This policy provides mechanism on redress for administration, processing, and appeals.

1.1 Establishing of a Authority or Agency

The goal of this policy is to establish an independent and impartial National Authority to oversee and enforce compliance with data protection and privacy rights for individuals and businesses. The Agency or Authority will be a central agency oversighting on all matters related to national data governance, protection and privacy. The Authority or Agency will be empowered by a Data Protection Act (The Act), which will outline its scope of mandate, powers, and authority.

The Authority will be responsible for the protection of personal and business data, ensuring the proper processing of data, and enforcing data protection procedures. The Authority will receive complaints on data breaches, monitor and enforce the application of laws and regulations, advise and promote awareness on data protection, have powers of investigation and intervention, perform the function of authorizing and approving standardized safeguards relating to transborder data flows, make determinations relating to violations of the Act, and impose necessary administrative sanctions. Additionally, the Authority will instigate legal proceedings, administrate data breaches and other infringements, facilitate in investigating data breaches and other infringements, and define conditions for imposing administrative fines as mandated by the Act.

The Authority's mandate will also include taking part in international cooperation, promoting public awareness of their functions, powers, and activities, the rights of data subjects and exercising such rights, and raising awareness of controllers, processors and their legal obligations under the Act. The Authority shall be consulted on proposals for any legislative or administrative measures involving the processing of personal and business data, as well as requests and complaints from data subjects.

The Act will provide the Authority with the necessary resources to enable it to appoint skilled staff and/or build internal capacity to effectively perform its functions. Staff of the Authority may be bound by the obligations of confidentiality in the performance of their duties and exercise of powers. The Authority may appoint specialist staff or consultants to enable it to deliver its mandate. The Act should also allow the Authority

to seek possibilities for assistance in the establishment and funding of the PNG Data Protection and Governance Authority from available development programs led by international organizations.

1.2 Executive Sponsor

Prior to the establishment of the Authority or Agency, the Department of ICT (DICT) or any other appropriate government agency responsible for government data through an Act of parliament will the Executive Sponsor of this policy.

1.3 Lead Agency

The DICT will be the Lead agency on the development of the National Data Governance and Protection Policy and any future Data Governance Strategy development until such time the proposed Authority or an Agency is established through an Act of parliament if not through this policy.

The policy will be coordinated by DICT in consultation with relevant stakeholders for implementation and development of the implementation strategy. DICT will also lead the drafting of relevant Acts directed by this policy such as the Data Protection and Privacy Act.

1.4 National Data Governance and Protection Steering Committee

Until such time the Authority or agency is established, a multi sectoral steering committee will be established to oversight on all matters matters related to national data governance, protection and privacy. The Committee will be chaired by the Secretary for the Department of Information and Communication Technology (DICT) and will include the CEO of NICTA, the PNG Regulator as well as other relevant Government agencies, private sector, and civil society. The Steering Committee will be responsible for setting the strategy, policy, standards, and compliance for the effective governance and protection of data in Papua New Guinea. The Committee will meet regularly as necessary to review and update the policy. The Committee will also provides advice and support to give effect to the various stakeholders in the effective implementation of the policy and strategy including any international obligations.

1.5 Stakeholders Roles and Responsibilities

The DICT will continue to take responsibility in leading and collaborating with stakeholders in implementing this policy if an Authority or an Agency is not established by this policy until such time an it is eastblished by an Act of parliament. DICT will work closely with all relevant stakeholders from Government agencies, the Private Sector, civil society, the technical community, and academia.

1.5.1. Department of National Planning and Monitoring (DNPM)

The National Planning Act 1983 did provide for the establishment of the National Statistics Office, which is responsible for collecting and analyzing statistical data

for planning purposes. While the DNPM does not have a specific mandate to collect data, it works closely with other agencies, including the National Statistics Office, to gather and analyse

Over time, the government of Papua New Guinea has created additional agencies and departments to support national planning and monitoring efforts, and some of these entities may have responsibilities related to data collection. The Department of National Planning and Monitoring (DNPM) is one such agency that was established in 2002 to provide policy advice, planning, and monitoring services to the government.

The DNPM's responsibility as the leading agency in coordinating, facilitating, and planning sustainable development plans for the country needs to work closely with those agencies that produce data. Decisions in development planning, resource allocations, monitoring and evaluation, and strategic development of policies have to be data-driven. It is of imperative that DNPM work in partnership with other agencies, so it has access to reliable, accurate and trusted data to monitor and evaluate national projects as well and support strategic development planning.

1.5.2. Papua New Guinea Civil & Identity Registration (PNG NID)

The specific act that gives power to the National Identification (NID) project in Papua New Guinea (PNG) to collect data is the National Identification (NID) Act 2019. The Act establishes the NID project as a national initiative to establish a reliable and secure system of identification for all citizens and residents of PNG. The Act gives the NID project the power to collect personal information from individuals, including biometric data (such as fingerprints and facial images), demographic data (such as names, addresses, and dates of birth), and other relevant information required for identification purposes.

The Act also sets out strict rules and procedures for the collection, storage, use, and disclosure of personal data by the NID project, to ensure the privacy and security of individuals' personal information. The NID Act 2019 also establishes penalties for any unauthorized disclosure or misuse of personal information collected by the NID project.

The PNG NID's responsibility is to ensure that the data collected is accurate, secure, and compliant with all applicable regulations. It shall ensure that data is shared with other government agencies who need it on the SDE platform using data sharing models that best suits the work , and that it is used for legitimate purposes.

1.5.3. The National Information and Communication Technology Authority (NICTA)

The NICTA's mandate is primarily focused on the regulation and promotion of the ICT sector in PNG, it does have some responsibilities related to data

protection, particularly in relation to critical information infrastructure and the licensing of service providers.

Under the Cybersecurity and Cybercrime Act 2016, NICTA has the power to regulate and monitor the country's critical information infrastructure (CII). This includes setting standards and guidelines for the protection of CII, conducting risk assessments, and ensuring compliance with cybersecurity measures.

NICTA is responsible for granting licenses to telecommunications and ICT service providers, including internet service providers (ISPs). As part of the licensing process, NICTA may require service providers to comply with certain data protection and security measures. This will ensure all government data are protected.

Furthermore, NICTA has established the National Computer Emergency Response Team (CERT) to coordinate the country's response to cybersecurity incidents. The CERT is responsible for providing advice and guidance on cybersecurity matters, conducting vulnerability assessments, and responding to cyber incidents.

1.5.4. National Statistics Office (NSO)

The Statistics Act 1993 establishes the NSO as the central statistical authority for PNG and gives it the responsibility to collect, compile, analyse, and disseminate official statistics. The Act empowers the NSO to collect data from all sectors of the economy and society, including government agencies, private businesses, households, and individuals.

The Act sets out rules and procedures for the collection, storage, use, and dissemination of statistical information by the NSO to ensure the confidentiality and security of the data it collects. The Act also provides for penalties for any unauthorized disclosure or misuse of personal information collected by the NSO.

The NSO as the statistical authority for PNG is responsible to work closely with all government agencies so it can easily access accurate and reliable data. . The accurate and reliable statistical information will support evidence-based decision making in government, private sector, civil society, and international organisations. It should ensure that quality data are collected, shared, and used in a way that complies with relevant laws, regulations, and ethical standards.

1.5.5. Department of Health (DoH)

The Public Health Act 1973 gives power to the Department of Health (DoH) to collect healh-related ata from individuals, health facilities, and other relevant sources.

Under the Public Health Act 1973, the DoH is authorized to collect data on a range of health-related issues, including infectious diseases, environmental health hazards, health services and resources, and other public health concerns. The Act also provides for the establishment of a national health information system to facilitate the collection, analysis, and dissemination of health-related data.

The Act requires that all health facilities and health professionals provide the DoH with any health-related information that is requested and sets out rules and procedures to ensure the confidentiality and security of the data collected. The Act also provides for penalties for any unauthorized disclosure or misuse of personal health information collected by the DoH.

The DoH is responsible to share specific required data to other government agencies while considering the privacy and protection of an individuals' health status and information. The sharing anf exchange of data has to take place on the SDE.

1.5.6. National Department of Education (NDoE)

The Education Act 1983 is the primary legislation that governs the education system in Papua New Guinea. While the Act does not explicitly mandate the Department of Education to collect data, it does outline the functions of the Department, which include:

a) Promoting and facilitating the development of education in Papua New Guinea;

b) Collecting, analysing, and disseminating information relating to education in Papua New Guinea; and

c) Monitoring and evaluating the quality and effectiveness of education in Papua New Guinea.

Based on these functions, it is reasonable to assume that the NDoE would need to collect data in order to carry out its responsibilities effectively. However, the Act does not specify what type of data should be collected, as this would depend on the specific information needs of the Department and the education system as a whole. It is therefore necessary for NDoH to collaborate with other government agencies to access needed data.

1.5.7. Department of Higher Education, Research, Science & Technology (DHERST)

The DHERST is responsible to collaborate and work with other government agencies such as NDoE to ensure that it has access to reliable data to understand the current and future state of higher education in the state, inform

policy decisions, and create strategies to support the needs of students and the higher education system.

The Higher Education (General Provisions) Act 2014 empowers DHERST to collect data in order to carry out its functions. Section 89 of the Higher Education (General Provisions) Act 2014 specifically provides for DHERST to collect information and data from higher education institutions for the purpose of carrying out its functions. This data may include information on student enrolment, academic programs, research activities, and other relevant matters necessary for the effective regulation and promotion of higher education in Papua New Guinea.

The Department of Higher Education, Research, Science and Technology (DHERST) in Papua New Guinea may collaborate with other agencies to share its data through various mechanisms.

1.5.8. Department of Provincial & Local Level Government Affairs (DPLGA)

The DPLGA is responsible for data collected from the ward level . DPLGA is to ensure that all data collected at provincial level are integrated and updated consequently. As a responsible agency in supporting decentralized governance in Papua New Guinea, the data collected from the provincial levels will have great impacts on the development and policy intervention initiatives when it is shared with other government agencies.

The specific act that gives power DPLGA to collect data is the Organic Law on Provincial Governments and Local-level Governments. Under the Organic Law, the DPLGA is authorized to collect data on a range of issues related to provincial and local-level government administration, including population, land use, infrastructure, economic development, and social services. The DPLGA is also responsible for overseeing the collection and management of data by provincial and local-level governments and ensuring that data is accurate, reliable, and up-to-date.

The Organic Law requires that provincial and local-level governments provide the DPLGA with any information that is required to carry out its functions and sets out rules and procedures for the collection, storage, use, and disclosure of data to ensure the confidentiality and security of the information collected.

Under the Local-Level Government Administration Act 1997, each LLG is required to maintain a ward record book, which contains information on the population, land, and resources within the LLG's area of jurisdiction. The ward record book serves as a basic source of information for development planning and decision-making at the local level. Thus, it has to be shared with other government agencies through agreements.

1.5.9. Department of Personnel Management (DPM)

The Public Service Management Act 2014 gives power and sets out the legal framework for the management and administration of the public service in PNG. . The Act establishes the DPM as the primary agency responsible for the management of human resources in the public service and gives it the power to collect data on public service employees and their employment conditions.

Under the Public Service Management Act 2014, the DPM is authorized to collect data on a range of issues related to public service employment, including recruitment, appointment, promotion, performance, and remuneration. The DPM is also responsible for overseeing the collection and management of data by government agencies and ensuring that data is accurate, reliable, and up-to-date.

The Act requires that government agencies provide the DPM with any information that is required to carry out its functions and sets out rules and procedures for the collection, storage, use, and disclosure of data to ensure the confidentiality and security of the information collected. The Act also provides for penalties for any unauthorized disclosure or misuse of personal information

DPM is responsible for managing all personnel and human resource data on all civil servants. DPM's responsibility is to share specific required data to other government agencies, while at the same time ensuring that the privacy and protection of an individuals' personal identifiable data is held securely.

1.5.10. All Public Bodies

All public bodies are responsible in making data become available and accessible to stakeholders. The DICT as mandated by the Digital Government Act 2023, to provide the Secure Data Exchange platform for the exchange of data and a Central Electronic Data Repository for data storage. Public bodies will have to establish partnership with other agencies while working closely with DICT to ensure that data are exchanged and accessed in a secure manner while protecting the privacy of data.

All public bodies are to work collaboratively so data can be exchanged and shared amongst agencies to complete mandated activities in delivering services to citizens in an effective and efficient way.

1.5.11. Private Sector Entities and NGO

All private bodies engaged by a public agency to collect, and process data have to comply to this policy and the Digital Government Act 2023 which sets out the provision of handling government data including citizen data.

2.0. REGULATORY AND LEGISLATIVE FRAMEWORK

The strengthening of legislation and the regulatory environments in Papua New Guinea will support the e-Government and Digital Economy agenda in the country. The following are among the most important pieces of legislation and regulations that will support the implementation of the Data Governance and Data Protection Program in Papua New Guinea.

2.1 Data Protection Act

The PNG Data Protection Act will be a critical piece of legislation for Papua New Guinea, helping to protect the privacy and security of personal data while promoting effective and efficient data management practices.

In Papua New Guinea, the regulatory framework for data protection, security, and governance is currently incomplete. While there are specific clauses in existing Acts such as the Digital Government Act 2022 that address the protection of data, a comprehensive Data Protection Act is needed to ensure effective and comprehensive regulation of data in the country.

The DICT will be responsible for developing this Act, which will serve several important purposes;

i) It will provide protection for personal data and regulate the use and disclosure of such data, including outlining the rights and obligations of individuals and organizations that collect, use, and disclose personal data

ii) The Act will establish the Data Protection and Governance Authority, which will be responsible for overseeing the implementation and enforcement of the Act's provisions. The Authority will have the power to investigate data breaches and non-compliance, and to impose penalties and other sanctions where necessary.

iii) The Act will also strengthen the “Once-only Principle” of data governance, which is a key principle of efficient and effective data management. This principle dictates that data should only be collected once and used multiple times, rather than being duplicated unnecessarily, and

iv) The Act will further allow for private sector organizations to join the data exchange ecosystem and share data with all stakeholders over the Secure Data Exchange Platform, while ensuring that appropriate safeguards are in place to protect personal data including other datas sets.

2.2 Cybersecurity Laws

As Papua New Guinea's public sector undergoes digital transformation, more online activities and data exchange will take place. However, with this comes an increased vulnerability to various cyber risks and attacks. Therefore, it is necessary to strengthen the country's cyberspace through legislation. In accordance with the National Cyber Security Policy of 2021, it is imperative that Papua New Guinea implements a National

Cyber Security Legislation to protect its cyberspace. This legislation will provide a framework to address cyber threats and ensure the security of information systems, networks, and critical infrastructure.

It will also establish guidelines for cybersecurity incident reporting and response, as well as penalties for cybercrimes. The legislation should also provide for the establishment of a national cybersecurity authority responsible for overseeing and enforcing cybersecurity policies and regulations. Through the implementation of a National Cyber Security Legislation, Papua New Guinea can improve its cybersecurity posture and ensure the safety and security of its digital infrastructure.

3.0. INFRASTRUCTURE AND SECURE DATA EXCHANGE PLATFORM

3.1 Electronic Data Repository

The DICT is tasked with the responsibility of establishing and managing an Electronic Data Repository in accordance with the Digital Government Act 2022. The repository will;

i. serve as a storage server to back up all electronic data for public bodies, providing a safety net against potential unforeseen events that may cause data loss to public bodies.

ii. will be designed with the latest technology and security features to ensure the confidentiality, integrity, and availability of stored data.

iii. be maintained and regular update by DICT as their main responsibility. DICT will also:

   a. implement security measures such as access controls, encryption, and backup procedures to safeguard the data stored in the repository.

   b. provide guidelines and procedures for public bodies to follow in submitting their data to the repository,

   c. ensure that data stored in the repository is easily accessible and retrievable by authorized personnel when needed.

3.2 Secure Data Exchange Platform

The Secure Data Exchange Platform will be a key component of the government's digital transformation strategy, enabling seamless and secure data sharing among public bodies and private sector partners to drive innovation and improve service delivery for citizens.

As mandated by the Digital Government Act 2023, the DICT is responsible for developing, operating, and maintaining a Secure Data Exchange Platform (SDEP) for all public bodies. The SDEP will;

i. provide a secure and efficient means of sharing data among government agencies to enable effective service delivery.

ii. adhere to industry-standard security protocols, such as encryption and authentication, to ensure the confidentiality, integrity, and availability of data in transit and at rest.

iii. provide tools for monitoring and auditing data access and usage, as well as mechanisms for resolving any disputes or breaches of data sharing agreements.

iv. support the exchange of various types of data, including personal data, while ensuring compliance with relevant laws and regulations on data protection and privacy.

v. support private sector organizations that wish to participate in the government's data exchange ecosystem by providing a secure and transparent platform for sharing data with public bodies. Private sector partners will be required to comply with the same security and privacy standards as public bodies and adhere to the policies and procedures established by the DICT for data exchange.

The DICT will work with other government agencies to establish standardized data sharing policies and procedures that align with internaltion best practice principles and the Data Protection Act (DPA).

4.0. CAPACITY BUILDING

4.1 Building Data Capabilities across all Public Bodies

The Data Governance and Protection Authority will be responsible for providing training and capacity building for all Government agencies. The Data Protection Authority when operational will provide training and capacity building through partnership arrangements with the Somare Institue of Leadership and Governance (SILAG). The training will cover all the basics along with collecting or capturing only the information that is expressly required and no additional information.

Prior to the opening of this office the DICT will provide this training and capacity building to Government Agencies. Additionally, it is expected that DICT will provide training to all DTOs on data protection, data privacy and data governance.

Other training providers that provide online training are the International Data Governance Institute (IDGI), and the Institute of Internal Auditors (IIA).

The IDGI has several courses focused on data governance and privacy compliance in the public sector. The IIA offers a Certified Internal Data Auditor (CIDA) course to help government personnel better understand and audit data governance policies and procedures.

4.2 Building Data Capability across all Private Bodies.

The Data Protection and Governance Authority will be responsible for providing training and capacity building for all private sector, NGOs, and other organisations. The Data Protection and Governance Authority when operational will provide this necessary training and capacity building several times a year to NGOs, private sector companies and organisation, along with SMEs and MSMEs. The training will be on data protection, data privacy, and data governance for all Government Agencies. The training will cover all the basics along with collecting or capturing only the information that is expressly required and no additional information.

Prior to the opening of this office the DICT will provide this training and capacity building.

4.3 Sensitisation and Awareness Raising

Sensitization and awareness raising are crucial components in building a culture of data privacy and governance. It is essential to educate public and private sector employees, as well as the general public, about the significance of data protection and governance and the potential consequences of data breaches and misuse.

The Data Protection Authority will be responsible for conducting regular sensitization and awareness-raising campaigns on data protection and governance. These campaigns will target the public, private sector, NGOs, and other organizations to inform them about the importance of data protection, privacy, and governance and to educate them about the potential risks of data breaches.

The campaigns will focus on the following topics:

a) The importance of protecting personal and sensitive data
b) The potential consequences of data breaches and misuse
c) The rights of individuals with regards to their personal data.
d) The responsibilities of organizations when collecting, using, and storing personal data
e) Best practices for data protection and governance

The sensitization and awareness-raising campaigns will use a variety of channels to reach a wide audience, including social media, radio, television, and print media. The

campaigns will also include training sessions, workshops, and seminars for public and private sector employees.

The DPA will also leverage the International Data Privacy Day, set for January 28th every year, to promote its educational initiative that raises awareness among businesses and users about protecting personal information online. Data Privacy Day promotes events and activities that stimulate the development of technology tools that promote individual control over personally identifiable information, compliance with privacy laws and regulations, and create dialogues among stakeholders interested in advancing data protection and privacy.

PART E: ENFORCEMENT, MONITORING, AND EVALUATION

1.0. Enforcement

Enforcement is a crucial aspect of any data protection and governance policy, ensuring compliance with laws and regulations and respect for individuals' privacy rights. The Data Protection Authority (DPA) will enforce data protection laws and regulations, investigating and prosecuting violators and promoting compliance through guidance and support. Collaboration with law enforcement, the judiciary, and other stakeholders will strengthen the legal and regulatory framework for data protection and governance, building trust and confidence in these principles.

2.0. Monitoring and Evaluation

Monitoring and evaluation are critical components of ensuring the effectiveness of data protection and governance policies and building trust and confidence in the management of personal and sensitive data.

The Data Protection Authority (DPA) will be responsible for monitoring and evaluating the implementation of this policy. The DPA will establish a system for monitoring and reporting on compliance with data protection and governance laws and regulations in the public and private sectors.

The monitoring and evaluation system will include regular assessments of data protection practices and procedures, as well as data breaches and incidents. The DPA will also conduct periodic reviews of the policy to assess its effectiveness and identify areas for improvement.

In addition to monitoring and evaluation, the DPA will also establish a system for public reporting on data protection and governance. This will include publishing regular reports on data breaches and incidents, as well as trends and patterns in data protection practices and procedures.

Prior to and after the establishment of the Data Protection Authority, the Department of Information and Communications Technology (DICT) will be responsible for coordinating the monitoring and evaluation of the implementation of this Policy in close consultation with the Authority.

ANNEXES

ANNEX C: Basics Principles for the Protection of Personal Data

This section of the policy defines the guiding principles for the processing of personal data. To comply with the policy, information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. The principles applied in the Policy are based on the global best practices in data protection.

As a prerequisite, the policy requires that personal data and special categories of data are processed fairly, lawfully and transparently and in a manner that is proportionate in relation to the legitimate purpose(s) pursued, whether public or private, and the rights and freedoms of individuals at stake.

1.0 Fairness and lawfulness and Transparency

1.1 The processing of Personal Data must happen in a lawful way and have a legal or legitimate basis.

1.2 Personal data will be considered to have been obtained fairly if the data subject is informed of the name of the data controller and the purpose(s) for processing the personal data or any further information which is necessary, having regard to the specific circumstances in which the data is or is to be processed, to enable processing in respect of the data subject to be fair.

1.3 Data controller/ processor should be transparent regarding the processing of personal data and inform the data subject in an open and transparent manner. Personal data should only be processed if and only if there is a legitimate purpose for the processing of that personal data. A Data controller/ processor should practice transparency so that the data subjects will be sufficiently informed regarding the processing of their personal data. When processing personal data, the individual rights of data subject must be protected.

1.4 Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

1.5 A data provider and data recipient shall ensure that health information or personal information contained in public sector data that is capable of being shared is not collected, used, disclosed, protected, kept, retained, or disposed of otherwise than in compliance with this Act and any other data protection and privacy legislation.

1.6 The processing of Personal Data must happen in a lawful way and have a legal or legitimate basis.

1.7 Personal data must be processed in a transparent manner. Data subjects have right to know about the processing of their personal data. Controllers should be required to act transparently to ensure fairness of processing and to inform data

subjects in an appropriate form of the controller's identity and other key information about the processing and their rights in order to ensure fair and legitimate processing.

2.0 Specific Legitimate Purpose and Purpose Limitation

2.1 Personal data must be processed for explicit, specified, and legitimate purposes and the processing of that particular data must serve those purposes and shall not be incompatible with them.

2.2 Personal data must be processed only for the purpose that was defined before the data was collected.

2.3 Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes may be considered compatible with those purposes, subject to appropriate safeguards. Subsequent changes to the purpose are only possible to a limited extent and require legitimate basis.

3.0 Data Minimisation

3.1 Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purpose for which the data will be processed.

3.2 Before processing personal data, a data controller must determine whether and to what extent the personal data is necessary to achieve the purpose for which the data was required.

3.3 Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by law.

3.4 Privacy and security should be built and integrated in from the onset in all data management systems that collect and process personal data

3.5 This requirement not only refers to the quantity, but also to the quality of personal data.

4.0 Storage Limitations

4.1 Personal data shall not be kept for longer periods than is necessary to achieve the purpose for which the data was collected and processed.

5.0 Accuracy

5.1 Personal data undergoing processing should be accurate and up to date.

5.2 Suitable steps must be taken by a data controller to ensure that inaccurate or incomplete data is deleted, corrected, supplemented or updated.

6.0 Confidentiality and Integrity

6.1 Personal data must be processed securely to retain confidentiality and integrity in consistency, accuracy, and trustworthiness over its entire life cycle.

6.2 Steps must be taken to ensure that data cannot be altered by unauthorized entities or people.

6.3 Security of personal data shall be preserved by establishing suitable organizational and technical measures to prevent unauthorized access, illegal processing, or distribution, as well as accidental loss, modification or destruction.

7.0 Accountability

7.1 All Data Controllers/Processors shall take all appropriate measures to comply with the provisions set out in this policy and be able to demonstrate that the data processing under their control complies with them.

8.0 Legal Grounds For Processing

8.1 Data protection policy strives to ensure that collecting, processing, transmitting, using, storing and disposal of personal data is permitted only under lawful and legitimate basis.

9.0 Data Security and Security Breach Notification

9.1 The controller, and, where applicable the processor, shall take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification, or disclosure of personal data.

9.2 The controller shall notify, without delay, at least the competent supervisory authority of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

10.0 Special Categories of Data Processing & Safeguards

10.1 The processing of certain types of data, or the processing of certain data for the sensitive information it reveals, may lead to encroachments on the interests, rights, and freedoms of individuals. This can happen where there is a potential risk of discrimination or injury to an individual's dignity, physical integrity, or where the data subject's most intimate details, are being affected, or where processing of data could affect the presumption of innocence or other important rights and freedoms.

10.2 The processing of the following categories of data shall only be allowed where there are appropriate safeguards in place to protect people's data and rights:

a. genetic data;

b. personal data relating to offences, criminal proceedings and convictions, and related security measures;

c. biometric data uniquely identifying a person;

d. personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade union membership, religious or other beliefs, health, or sexual life.

10.3 The safeguards shall guard against risks that the processing of such data may present for the interests, rights, and freedoms of the data subject, notably the risk of discrimination.

10.4 Appropriate safeguards include:

a. with the data subject's explicit consent;

b. under a professional secrecy obligation;

c. a law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be permitted;

d. a particular and qualified organisation;

e. processing is necessary to protect the vital interests of the data subject or of another natural person.

11.0 Consent

11.1 Data Controller/Data Processor will obtain consent from Data Subject on the processing of Personal Data including sensitive personal data.

11.2 Data subject should clearly understand why his/her information is needed, who it will be shared with, and the possible consequences of them agreeing or refusing the proposed use of the data.

11.3 The processing of personal data for a child shall be done only with the consent of the child's parent or guardian.

12.0 Exceptions

12.1 The policy acknowledges that there will be exceptional circumstances where personal data can be processed without the data subjects' consent.

13.0 Third party data processing

13.1 Personal data shall not be disclosed or processed by a third party except when required by law or the third-party Data Processing Agreement has been approved and signed by the Data Controller and the Data Processor (i.e. the third party) and the Data subject is aware of this arrangement.

14.0 Cross Border Transfer

14.1 This policy may allow personal data to be transferred to other countries or entities if such countries or entities have met the adequate safeguards spelt out in this policy for maintaining the required protection for the privacy rights of the data subjects in relation to their personal data.

15.0 Big Data and Analytics

15.1 The use of big data and analytics is permitted subject to the processes involved in complying with the requirements of the Data Protection Laws.

16.0 Data Protection and Privacy by Design and Default

16.1 Privacy should be built in from the outset in all data management systems including critical systems.

16.2 Before carrying out processing, controllers (and, where applicable, processors), shall examine the potential impact on the rights and fundamental freedoms of data subjects prior to the commencement of the processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

16.3 Controllers (and, where applicable, processors), shall implement technical and organisational measures which consider the implications of the right to the protection of personal data at all stages of the data processing.

16.4 When setting up the technical requirements for default settings, controllers and processors should choose privacy friendly standard configurations so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default), and to avoid processing more data than necessary to achieve the legitimate purpose.

16.5 The Data Controller/Data Controller should apply appropriate personal data security controls such as encryption, anonymization and Pseudonymisation of personal data.

16.6 Data controller must manage any personal data breaches promptly and appropriately.

16.7 All data breaches are to be reported to the Data Protection Regulator. The reporting must be done expeditiously.

16.8 The frequency and severity of the breach will determine the next level of intervention.

17.0 Data controller shall uphold rights of data subject

17.1. Data controller is required to provide a copy of the information comprising personal data of a data subject at minimal cost and within a reasonable time of his/her request.

17.2. The Data Controller may disapprove a request for personal data but must provide reasons for denying the request.

17.3. When Data subject successfully demonstrates the inaccuracy or incompleteness of data, Data Controller will amend the data as required within a reasonable time.

18.0 Challenge to Compliance

18.1. Data Controller is required to put mechanisms and processes in place to receive and address complaints or inquiries about its policies and procedures relating to the handling of data including personal data.

19.0 Transborder Flows of Personal Data

19.1 The free flow of data is essential to the expansion of the digital economy, to harness all the benefit of the digital economy and the data processing techniques and technologies that it brings to society. These new technologies can contribute greatly to the inclusive growth of PNG. However, at the same time, it is essential to ensure that the same level of data protection is afforded to personal data when transferring this data across borders that is foreseen and guaranteed within the jurisdiction of PNG. The cross-border transfer of personal data may only take place where an appropriate level of protection is guaranteed.

19.2 An appropriate level of protection can, after a thorough assessment by the data controller, be secured by:

a. the law of the receiving country or international organization, including the applicable international treaties or agreements, or;

b. ad hoc or approved standardized safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing

19.3 The transfer of personal data may also take place if:

a. the data subject has given explicit, specific, and free consent, after being informed of risks arising in the absence of appropriate safeguards.

b. the specific interests of the data subject require it in the particular case;

c. in response to prevailing legitimate interest, in particular an important public interest, if it is provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society;

d. it constitutes a necessary and proportionate measure in a democratic society for the freedom of expression.

19.4 The supervisory authority is preferably to be involved in assessing if the criteria are met.

19.5 The supervisory authority is entitled to request that the data controller that transfers the data demonstrate the effectiveness of the safeguards or the existence of prevailing legitimate interests.

19.6 The supervisory authority may prohibit such transfers, suspend them or subject them to condition if they do not think these safeguards have been put in place.

19.7 For international law enforcement co-operation the same requirements should be applicable and proper legal bases for the transfer should be established and ensured. For this latter, joining international treaties (such as the Council of Europe's Budapest Convention), using appropriate international frameworks (as guaranteed by Interpol instruments) which enable the international cooperation in specific investigations related to specific crimes while alone or with other instruments guaranteeing the appropriate level of protection during the transfer between participating states could be envisaged.

20.0 Rights of Data Subjects

20.1 Every individual shall have a right:

a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;

b. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide to ensure the transparency of processing

c. to obtain, on request, knowledge of the reasoning underlying the processing of personal data about them;

d. to object at any time to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing that override his or her interests or rights and fundamental freedoms;

e. to obtain, on request, free of charge and without excessive delay, the rectification or erasure of such data processed contrary to the provisions of this policy and the proposed law;

f. to obtain, on request, free of charge and without excessive delay judicial and non-judicial remedy for violations of the law;

g. to benefit, whatever his or her nationality or residence, from the assistance of the Supervisory Authority in exercising his or her rights