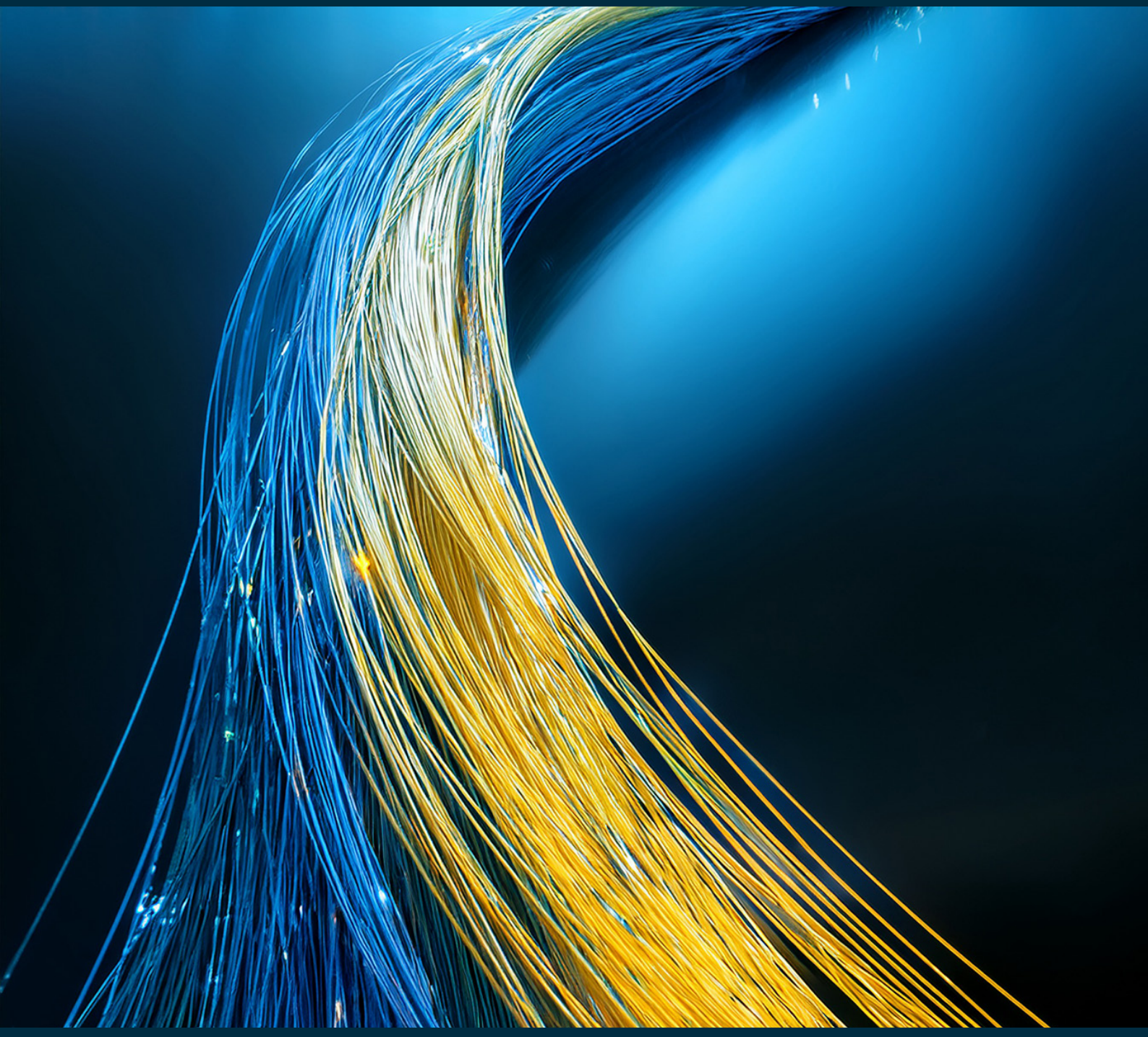
ANNEXES TO THE

MAURITIUS NATIONAL DATA STRATEGY

FOR PUBLIC AND PRIVATE ORGANISATIONS



Data Protection Office

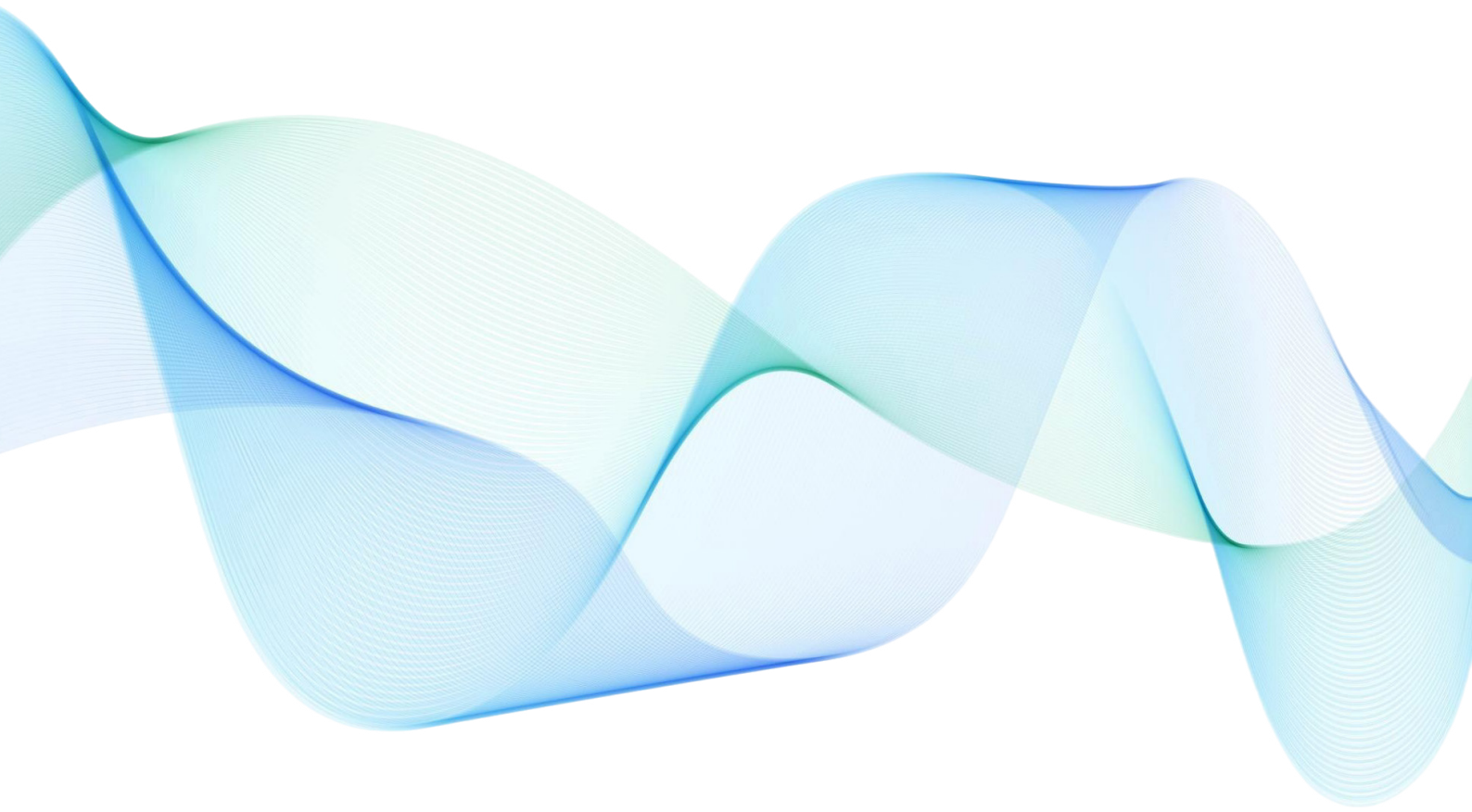
MAURITIUS NATIONAL DATA STRATEGY

MODEL DATA GOVERNANCE FRAMEWORK

ANNEX 1

Data Protection Office

Data governance is the cornerstone of effective data management and utilization guaranteeing accuracy, security and accessibility. Robust data governance is essential to ensure data remains reliable, secure and responsibly managed. A well-established data governance framework not only enhances decision-making and regulatory compliance but also leverages data to improve service delivery while mitigating risks associated with data breaches or mismanagement.



Contents

1.0 Background and Significance

"Data is a powerful asset; its responsible use defines its true value."

Data is revolutionizing the way entities operate in today's world. By consolidating vast amounts of data into a centralized location and effectively organizing it, advanced digital technologies can unlock critical insights. A disciplined approach to data collection empowers organizations with a significant advantage, enabling them to identify opportunities, make informed decisions and deliver improved services that might otherwise remain elusive.

The rapid advancement of digital technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), robotics and big data analytics has profoundly transformed operations. These technologies depend on extensive access to both structured and unstructured data to function effectively. Without a robust data governance framework, the potential of these innovations remains largely untapped. A well-defined approach ensures that data is readily available for strategic decision-making while maintaining stringent security and privacy compliance controls.

The evolution of data management has shifted significantly with the advent of unstructured data and the looming "data tsunami." Historically, governments relied on structured data housed in tables or basic systems. This approach either led to bespoke systems designed for specific needs or rigid processes governing all governmental data. While these traditional methods were once effective, they now struggle to keep pace with the increasing complexity and volume of data flowing from various internal and external sources. According to the International Data Corporation (IDC), the annual global data creation and replication is projected to reach an astonishing 163 zettabytes (ZB) by 2025, a tenfold increase from just nine years ago. This explosive growth highlights the escalating urgency for solid data governance frameworks, especially in public sectors involved with government data management.

For decades, governments have prioritized securing their networks from external threats while managing internal data access. Traditional systems were designed with centralized control mechanisms making it challenging to adapt to evolving technological needs. However, with the advent of next-generation technologies, a shift from rigid control to dynamic data management is essential.

Today, new technologies that are crucial for efficient operations and automation require greater data access and faster processing speeds. This shift necessitates a change to dynamic data management. The new approach is more cost-effective, efficient, scalable and compatible with next-generation technologies. However, it comes with significant responsibility. The data will always remain the responsibility of the organization and comprehensive data governance and security plans are essential to prevent compromises. This vast amount of data necessitates an adaptive approach to governance that can accommodate real-time processing, cross-border data transfers and compliance with multiple regulatory frameworks.

A well-structured governance framework will:

- Enhance transparency and accountability in data management.
- Support compliance with national and international regulatory requirements.
- Facilitate secure and efficient data sharing across agencies.
- Promote trust among citizens by ensuring responsible data handling.
- Enable data-driven decision-making to improve services.

With the increasing scale and complexity of data ecosystems, we must adopt an adaptive governance approach that is both secure and flexible. The successful implementation of a data governance framework will strengthen the nation's position as a digital leader while ensuring compliance with evolving regulatory requirements. The shift from traditional control models to modern, scalable governance practices is essential for unlocking the full potential of digital transformation.

By investing in structured governance mechanisms, we can ensure that data remains a strategic asset empowering decision-makers, enhancing service delivery and fostering trust among citizens. The time to act is now to build a resilient, future-ready data governance framework that supports national development and economic growth.

2.0 What is a Data Governance Framework?

A data governance framework is a set of rules, processes, and responsibilities that dictate how an organisation collects, organizes, stores, and uses its data. The goal of a data governance framework is to set a standard on how data is managed (to ensure its integrity), leveraged by internal teams, and protected from security risks.
Without a data governance framework in place, organisations cannot guarantee data quality or compliance with privacy regulations. This opens the door to mismanaging customer data, which could land organisations in hot water legally (resulting in hefty fines and reputational damage).

A data governance framework allows the organisation to establish data democratization, giving employees of all technical skill sets, the ability to access and act on data. This autonomy and confidence in data allows teams to accurately set goals, measure performance, strategize, and discover new opportunities.

Data democratization has been notoriously difficult for businesses to achieve in the past few years (83% of companies admit they're unable to turn fragmented data points into comprehensive user records). It is one of the reasons behind the growing adoption of customer data platforms (CDP) to help manage and centralize customer data so everyone can benefit from it.

The framework will establish the foundation for data accountability, quality, privacy and accessibility ensuring that data supports informed decision-making, innovation and public trust

2.1 Benefits of a data governance framework:-

With the right framework in place, organisations can transform their data into a valuable and powerful asset. This will enable them to achieve or even surpass their objectives and enhance service delivery.

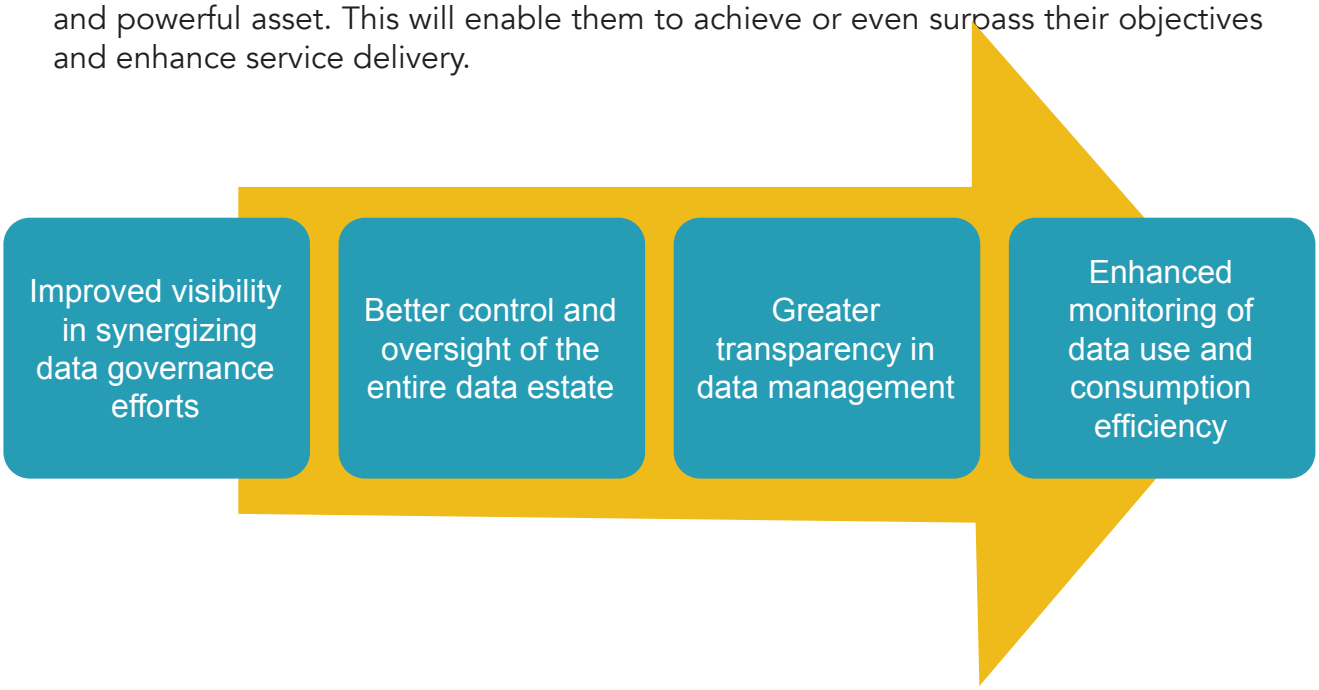


Figure 1: Benefits of a data governance framework

At a minimum, a data governance framework should establish the following policies for each data asset:

- Structure: Defines how data will be organized, retrieved and stored.
- Access: Designates which employees and authorized third parties will have access to data.
- Usage: Establishes parameters and restrictions on use to minimize legal risks, ensure citizens' data privacy and comply with regulations in general.
- Classification: Categorizes data into levels of sensitivity such as internal vs. public or classified vs. restricted.
- Integrity: Establishes standards to ensure accuracy, validity and reliability such that data can be trusted for decision-making.

2.2 What defines an outstanding data governance in today's evolving data landscape?

The future of data governance extends beyond improving operational efficiency, decision-making, and regulatory compliance. It also aims to mitigate risks associated with poor data management. As a vital component of data management, data governance is based on five essential pillars:

- Processes, policies, standards, and procedures: Establishes clear guidelines and protocols for data handling.
- Organizational structure, roles, and responsibilities: Defines the framework for who is responsible for data governance tasks.
- Technology and tools: Utilizes the right technologies and tools to support data management efforts.
- Metadata management (or data catalog): Manages and organizes metadata to ensure data is easily accessible and properly cataloged.
- Compliance and Risk Management: Mechanisms to ensure adherence to data security and data protection and measures to mitigate risks.

2.2.1 Pillar 1

Processes, policies, standards and procedures

- **Without well-defined and organized policies, chaos and inefficiency are unavoidable**

Clear and well-defined policies are crucial for maintaining order in data management. A data governance policy should articulate the strategic direction, outlining both the desired behaviors and expected outcomes. Standards act as governing rules to ensure that data is fit for its intended purpose. In parallel, processes and procedures provide detailed instructions on how to implement these standards effectively.
Commonly established standards include metadata management, data quality, data security, data architecture and data modeling.

- **Managing data security becomes more challenging in a distributed environment**

Ensuring data security in a distributed environment is more complex due to data being spread across multiple locations. This increases the risk of breaches and makes consistent monitoring difficult. Various access points and devices add to the challenge. Compliance across different systems and locations requires extra effort. Remote access also heightens vulnerabilities demanding adaptive and robust security measures.

- **Unstructured data presents new challenges for data quality**

Managing large volumes, diverse types and fast-moving data can significantly increase the time required for routine data quality assessments, potentially changing how entities define and execute data quality management.

For example, assessing the quality of unstructured data involves identifying patterns, converting it into structured datasets and validating it against trusted sources. This process enhances confidence in unstructured data, uncovers valuable insights and improves decision-making processes.

- **As analytics evolve, new innovations in data quality become essential**

The vast amounts of data managed by next-generation platforms enable interactive, experimental and evolving analytics unlike traditional platforms that are typically used for specific functions such as regulatory reporting. Consequently, the assessment of data quality and the resources allocated to this process should be adjusted accordingly. Analytical tools should include built-in features to manage and accommodate acceptable data quality issues ensuring that entities can leverage data effectively while maintaining high standards.

2.2.2 Pillar 2

Organizational structure, roles and responsibilities

- **Establishing Accountability**

The responsibility ultimately lies within the organisation. It should clearly establish formal structures, roles and responsibilities to manage and oversee processes related to data management and governance. For instance, creating a data governance committee can help oversee the development and implementation of processes, policies, standards and procedures. It is essential to appoint both policy and technical leaders who will be accountable for and take ownership of the data governance framework.

Data Governance Roles	Responsibilities
Data Owner	Holds authority over specific data sets,defines access permissions and ensures appropriate use of data.
Data Steward	Maintains data quality, enforces governance policies and ensures data integrity within their respective domains.
Data Protection Officer (DPO)	Oversees data protection strategy, ensures compliance with data protection regulations and addresses data privacy concerns[1].
Chief Information Officer (CIO)	Leads data governance efforts, ensures regulatory compliance and aligns data strategy with organizational goals.
Data Custodian	Manages technical aspects such as data storage, security and backup processes to safeguard data.
Data Specialist	Provides technical expertise and support to ensure the effective management, quality and usability of data.
Data User	Ensures the accurate and responsible use of data within the governance framework.
Data Management Committee (DMC)	Sets strategic direction, approves policies and oversees data governance implementation across the organization.

Table 1: Roles and Responsibilities

[1] The link provides further information on the roles and responsibilities of the DPO:

https://dataprotection.govmu.org/Documents/Roles%20and%20Responsibilities%20of%20Data%20Protection%20Officer%20V3.pdf

2.2.3 Pillar 3

Technology and tool capabilities

• Emerging Tools for Data Governance Management

New technological advancements encompass platforms, tools and subject-matter experts that are essential for supporting effective data governance. Common tools used for data governance such as metadata management, data quality, workflow management and data security tools have undergone significant transformations. Modern tools now adopt a proactive approach to data governance in contrast to the reactive strategies of the past.

• Data-quality tools require real time processing

Data governance and data quality tools must be capable of integrating with next-generation platforms to address their scale and complexity. These tools should include features such as the ability to assess data quality for unstructured data and perform real-time data processing.

Moreover, these tools should provide feedback to execution algorithms allowing them to resolve data quality issues as they arise in production environments. This capability is essential for organisations to maintain high standards of data quality and ensure the effective functioning of their data governance frameworks.

• How can data security tools be elevated to meet new challenges?

Elevating data security tools to meet new challenges involves addressing vulnerabilities in distributed environments, especially during migration to the cloud. Organisations must focus on preventing data breaches, securing data interfaces, ensuring robust identity and access management. Implementing industry-standard protocols and strengthening access control in microservices are crucial. These measures enhance data security and privacy within the data governance framework.

2.2.4 Pillar 4

Metadata content (or data catalog)

- **What will the future of metadata look like?**

Metadata content (or data catalogs) involves cataloging the technical and operational attributes of data. This content plays a crucial role in managing, overseeing and evaluating future data governance processes. Current metadata tools tend to focus primarily on technical metadata and support a limited range of metadata assets and their relationships. However, these tools must evolve to meet the growing needs of data management.

- **Big data requires a diverse range of metadata assets.**

Emerging platforms heighten the complexity of metadata management in data governance frameworks as big data requires diverse and extensive metadata assets. Next-generation platforms introduce advanced techniques such as statistical similarity measures (e.g. Dice coefficient, Levenshtein distance) to improve metadata collection, cataloging, and discovery. While this shift primarily impacts the technology and metadata pillars, traditional and next-gen platforms will coexist in hybrid ecosystems. Organisations must ensure cohesive management of these platforms to maintain interoperability and governance consistency. This evolution drives enhancements across all data governance pillars to address increasing technical and operational demands

2.2.5 Pillar 5

Compliance and Risk Management

- **Unified Regulatory Framework: -**

Compliance and Risk Management are key parts of a governance framework. Compliance ensures that organizations follow data protection laws and regulations like securing personal data and getting proper consent. Risk management involves identifying and mitigating risks, such as data breaches, by implementing measures like strong passwords and regular updates.
To achieve compliance and manage risks, organizations must implement various mechanisms:

- Policies and Procedures: Clear guidelines on secure data handling.
- Training: Educating employees about data security.
- Audits and Monitoring: Regular checks to ensure adherence to rules and identify risks.

- **Improving Compliance and Risk Management**

Trusted emerging platforms enhance compliance and risk management in data governance by automating regulatory adherence, reducing human error and improving efficiency. Secure Cloud-based solutions enable real-time data monitoring and automated compliance checks. Safe AI-driven tools improve risk prediction and anomaly detection while blockchain technology ensures secure and transparent data transactions. These platforms help organisations maintain regulatory compliance protect sensitive information and foster trust and accountability. Overall, they streamline data governance processes making them more effective.

3.0 Core elements of a Data Governance Framework

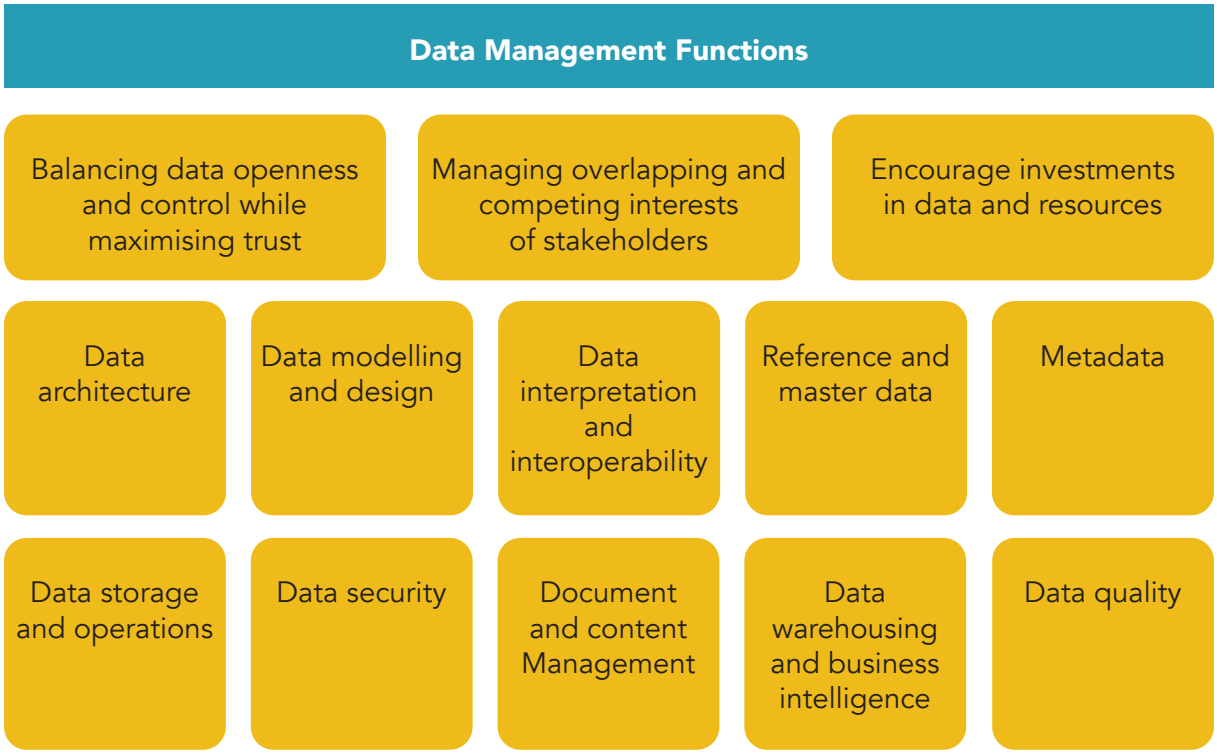


Figure 2: Components of a Data Governance Framework

3.1 Data architecture and technology infrastructure

Data architecture and technology infrastructure form the cornerstone of data governance frameworks. The data architecture defines the design and structure of data including its classification and inventory, ensuring it aligns with regulatory and operational requirements.

The technology infrastructure encompasses the hardware and software systems utilized to collect, store, and manage data, such as databases, data lakes, data warehouses

and specific systems like enterprise resource planning (ERP) platforms. It also covers the network connections necessary to facilitate the secure exchange of data across various departments and services.

3.2 Data discovery

A data governance framework includes details about how data discovery should be handled to create a unified view of all information. Data discovery includes data as well as other elements, such as:

- Collaboration
- Data certification
- Data classification
- Data engineering
- Data lineage
- Data profiling
- Data relationships
- Metadata

3.3 Data Integration

A data governance framework for governmental operations ensures the effectiveness of data integration, which involves combining data from various sources to create unified views and ensures compatibility for optimal use.

The data integration component of these frameworks ensures that data from across agencies as well as external sources can be seamlessly merged. This enables the data to be used for powering applications conducting analysis and supporting decision-making processes in a way that aligns with applicable laws and regulations.

3.4 Data lifecycle management

Data lifecycle management is the aspect of a data governance framework that directs the oversight of data from creation and collection through use and end of life. Data creation forms the cornerstone of data lifecycle management. It involves the generation and collection of reliable, high-quality information to support decision-making and public service delivery. Establishing efficient processes for data creation ensures accuracy, consistency and security. This foundational step enables the effective management, storage and use of data across all entities.

It includes setting policies and procedures for the following:

1. **Data archiving**
   - What is acceptable media for archiving?
   - What security is required for the archived data?
   - How long should it be archived?

2. **Data disposal**
   - When should data be destroyed?
   - What are approved methods for data destruction?
   - What proof is required for data destruction?
   - Data retention

3. **How long should data be kept?**
   What happens at its end of life (e.g., destroyed or permanently archived)?

3.5 Data literacy

Data literacy must be included in data governance frameworks. It refers to the skills required to understand the data that an organization creates, collects, stores and processes. It also includes understanding how elements of the data governance framework should be applied to the data.

3.6 Data management

Data management is the section of the data governance framework that specifies the processes and rules that define how an organization's data assets are created, stored, and accessed. It sets forth rules about how data can be used and shared internally and externally. It also includes details about what metadata (e.g., data source, creation date, last update, and owner) is required and how it is formatted to ensure that data can be easily found.

3.7 Data quality

The data quality component of a data governance framework focuses on establishing and maintaining the accuracy, completeness, consistency and reliability of data. This includes identifying and putting into place the processes, tools and automation needed to minimize error, identify inaccuracies and direct corrections throughout the data lifecycle. Elements of the data quality component of a data governance framework include: -

Data collection
- Data entry
- Data cleaning
- Data profiling
- Data validation
- Data monitoring
- Data auditing

3.8 Data security and privacy

Data security and privacy are a part of the data governance framework that influences most other parts. This includes all measures taken to protect data from unauthorized access, ensure the privacy of all sensitive and personal data and maintain compliance with the many laws and regulations related to data privacy and security.

3.9 Data stewardship

Data stewardship supports data governance efforts by working with groups, departments and external users to ensure that the policies and procedures detailed in the data governance framework are implemented correctly. Data stewards may also help with addressing data issues (e.g., access, quality, and security), including:
- Defining data elements
- Ensuring compliance
- Establishing and maintaining data quality standards

3.10 Regulatory compliance

Data governance frameworks help organizations with processes for identifying and staying on top of changes to compliance requirements related to data. It also includes guidance on specific data management practices necessary to ensure compliance.

4.0 Data Management Functions Checklist

key areas	Questions to Consider	Best Practices/ Recommendations
Balancing data openness and control while maximising trust	Is risk management and transparency across the data ecosystem being encouraged?	Implement risk management throughout the data lifecycle and ensure clear communication.
	What is the right balance between open and closed data?	Create data governance structures that balance varying levels of data accessibility, making data to be as open as possible and as closed as necessary. Leverage existing platforms for Open Data by consulting the Open Data Team.
	Are individuals provided with options and tools to improve control over their data?	Provide different consent models and allow data portability where appropriate.
	Are technological and organizational measures promoted to maximise trust?	Use access controls, privacy-enhancing technologies and secure systems.
	Does the framework promote compatibility between different agencies?	Ensure standardized formats, metadata and documentation for easier data exchange.
Managing overlapping and competing interests of stakeholders	Is the contribution of all stakeholders in the data value cycle considered?	Use an inclusive approach to engage contribution of all stakeholders through the data life cycle.
	Is cooperation across agencies considered?	Encourage collaboration between different areas including policy makers and regulatory bodies.
Encourage investments in data and resources	Are knowledge and skills for responsible data usage considered?	Identify gaps and invest in skills and expertise needed. All stakeholders in the data life cycle must be trained to handle data responsibly.
	Is funding for data infrastructure promoted?	Invest in secure and scalable data storage, processing and analytics tools and infrastructure.

key areas	Questions to Consider	Best Practices/Recommendations
Data Architecture (overall structure and design of the data systems, including the models, policies, rules, standards and guidelines that govern the collection, storage, management, integration and sharing of data)	What are the core data systems and platforms? How are data sources integrated and managed? What structures and formats are being used? How is scalability and flexibility in data architecture ensured?	Standardization of Data Models and Formats: Create and enforce consistent data standards to ensure compatibility, interoperability and shared understanding of the data. Data Integration Strategy: Implement an integrated data architecture that allows for seamless data flows. This includes designing systems that facilitate easy access and sharing of data, while ensuring data quality and compliance. Scalability and Flexibility: Design a scalable and flexible data architecture that can adapt to new technologies, increased data volumes and evolving business requirements.
Data Modeling & Design (structured models that represent the organisation, relationships and flow of data)	What are the primary data sources and how are they structured? Are the data models aligned with needs and the organisation's objectives? How are data flows through various systems tracked and maintained?	Adopt Standardized Data Models: Establish uniform data modeling standards to ensure that data structures and definitions are consistent across government facilitating easier integration and collaboration. Align Data Models with Objectives and Policies: Ensure that data modeling efforts are closely tied to the overarching goals of the organisation, such as improving services, transparency and policy effectiveness. Incorporate Interoperability in Data Model Design: Design data models that facilitate data sharing and integration ensuring that systems can exchange and use data in real-time. Implement Metadata Management Practices: Develop a centralized metadata management strategy to provide clarity on data definitions, lineage and usage. Establish Clear Data Definitions and Documentation: For every element within the data model, define clear and precise meanings, relationships and rules. Comprehensive documentation will help ensure that data is consistently understood and used correctly. Track and Monitor Data Lineage (flows across systems): Implement processes to track data lineage, ensuring that the flow of data from its source to its final destination is clearly understood. This aids in data traceability, accountability and auditability.

key areas	Questions to Consider	Best Practices/Recommendations
Data Categorization (classification of data into distinct categories based on its sensitivity, value and use)	What are the different categories of data? What criteria are used to determine the categorization of data?	tablish Clear Data Categories Based on Sensitivity and Use: Use clear and consistent data classification scheme, such as categories like "public", "internal" "confidential" and or "classified." This will ensure that all data is properly categorized based on its importance and sensitivity. Define Data Categorization Criteria and Standards: Develop specific guidelines and criteria for categorizing data considering the potential risks, legal implications and impact on privacy. This may include the sensitivity of the data, the potential harm from unauthorized access and compliance with legal requirements. Implement a standardized process for categorizing data.
Data Integration & Interoperability (ensuring that different data systems and platforms can work together seamlessly)	What are the primary data sources and how are they structured? Are the data models aligned with needs and the organisation's objectives? How are data flows through various systems tracked and maintained?	Adopt Standardized Data Models: Establish uniform data modeling standards to ensure that data structures and definitions are consistent across government facilitating easier integration and collaboration. Align Data Models with Objectives and Policies: Ensure that data modeling efforts are closely tied to the overarching goals of the organisation, such as improving services, transparency and policy effectiveness. Incorporate Interoperability in Data Model Design: Design data models that facilitate data sharing and integration ensuring that systems can exchange and use data in real-time.
Reference & Master Data (data definitions to ensure consistency and interoperability)	What standards and processes are in place to ensure data consistency and accuracy across reference and master data?	Centralisation of master data: Collecting master data into a central database is essential. By consolidating the master data into a centralised repository and connecting it to all participating applications, organisations can create a single view of the data. This centralisation facilitates better data management and accessibility, enabling efficient data governance practices. Track and Audit Changes to Master Data: Implement audit trails to track changes and updates to reference and master data. This allows for transparency, accountability and the ability to reverse or correct data errors when necessary.

key areas	Questions to Consider	Best Practices/Recommendations
Data Storage & Operations (how data is stored, managed and maintained in a secure, efficient and compliant manner)	Where is data stored (e.g., on-premises, cloud, hybrid) What data storage technologies are currently being used? What are the data retention and archiving policies for stored data? How is data backed up, and what is the disaster recovery plan for data storage?	Implement a Clear Data Storage Strategy: Develop and document a comprehensive data storage strategy that clearly outlines where and how different types of data will be stored, whether on-premises or in hybrid environments. Selecting an efficient and flexible storage infrastructure, maintaining a Data Asset Register and monitoring the effectiveness of storage are essential. Adopt Secure and Compliant Storage Solutions: Use storage solutions that incorporate strong security and data privacy measures, including encryption (both at rest and in transit), access controls and secure authentication methods. Define Data Retention and Archiving Policies: Establish clear data retention and archiving policies that specify how long different data types should be stored and when they should be archived or securely deleted. Ensure that these policies are consistent with legal requirements and needs. Implement Comprehensive Data Backup and Disaster Recovery Plans: Establish regular data backup procedures and disaster recovery plans to ensure that critical data is regularly backed up, stored securely and can be restored in case of failure or disaster. Test the effectiveness of Disaster Recovery.

Data Security (ensuring the integrity, confidentiality and availability of data)	What data security policies and frameworks are in place? Who has access to sensitive data and how are access controls enforced? What measures are in place to detect and respond to potential data breaches or security incidents? How are third-party vendors and contractors vetted and monitored for data security compliance? What encryption standards and technologies are used to protect data? How is user activity related to data access and usage monitored and logged?	Establish a Comprehensive Data Security Policy and framework: Develop and implement a clear and comprehensive data security policy that defines standards, roles and responsibilities for protecting data. This could include adopting established frameworks such as ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 42001. Use Strong Encryption and Secure Solutions: Encrypt data both in transit and at rest using industry-standard encryption. Implement Robust Access Control and Authentication: Apply role-based access control (RBAC) and multifactor authentication (MFA) to ensure that only authorized personnel can access data. Review access controls regularly and update them as needed. Deploy Intrusion Detection and Monitoring Systems: Implement monitoring tools and intrusion detection systems (IDS) to continuously scan for suspicious activity, vulnerabilities and potential data breaches. Real-time alerts should be set up to ensure swift action in case of a security incident. Regularly Perform Risk Assessments and Vulnerability Scans: Conduct regular risk assessments and vulnerability scans to identify and address potential data security weaknesses. Apply security patches and updates to systems and software in a timely manner. Create Incident Response and Disaster Recovery Plans: Develop a comprehensive incident response plan that outlines procedures for identifying, responding to and recovering from data breaches or security incidents. Ensure that the disaster recovery plan includes strategies for quickly restoring data and systems after an attack or breach. Monitor and Log User Activity: Set up logging and monitoring systems to track user activity related to data access and usage. Use audit trails to detect unauthorized access, anomalies or potential data misuse. Logs should be retained and analyzed to identify security incidents. Monitor third party vendors for Compliance: Implement a vendor risk management process to evaluate and monitor third-party vendors and contractors for data security compliance. Ensure that vendors adhere to the same standards, security and data protection protocols as government. Ensure that third-party vendors and contractors are registered controllers and/or processors. Ensure Compliance with Data Protection Laws: Regularly review and update data security practices to ensure compliance with relevant data protection laws and regulations. This includes notification of data breaches to the Data Protection Office and completing data protection impact assessments (DPIAs).

key areas	Questions to Consider	Best Practices/Recommendations
Data Quality (ensuring data is accurate, complete, timely, relevant and reliable)	What processes are in place to ensure data accuracy and consistency? Is data quality monitored?	Use Automated Data Quality Tools: Implement tools to automate the processes of cleansing, validation and monitoring of data. These tools can help identify and resolve issues such as duplicates, inaccuracies, and missing data automatically. Conduct Regular Data Audits and Quality Assessments: Monitor and regularly assess the quality of data through audits to identify issues and evaluate performance against established data quality metrics. Make necessary improvements based on audit findings. Establish Data Validation and Error-Detection Processes: Create automated validation rules and error-detection systems to ensure that incoming data is accurate and complete before it is stored or integrated into systems. These rules should be based on predefined standards and guidelines. Implement Data Cleansing Processes: Introduce routine data cleansing processes to correct errors, remove duplicates and fill in missing data. This should be an ongoing part of the data lifecycle to maintain high-quality data at all times.

key areas	Questions to Consider	Best Practices/ Recommendations
Data Sharing (ensuring that data is shared securely, efficiently and in compliance with relevant laws and regulations)	What are the policies and guidelines for sharing data? What platforms are used to facilitate secure and efficient data sharing? Adherence to the Data Protection Act for Data Exchange: Ensure that data sharing is justified by the necessity of the task. Ensure Compliance with the Electronic Transactions Act for Data Sharing between a public sector agency and an institution: In line with Section 8A of the Electronic Transactions Act 2000, public sector agencies may share information with institutions through their electronic systems for the purpose of business facilitation, provided that a formal agreement is established between the public sector agency and the institution. Leverage Existing Platforms for Data Sharing: Make use of centralized and secure platforms, such as the InfoHighway (MITCI), to facilitate seamless data exchange between public sector agencies and institutions.	Standardization of Data Models and Formats: Create and enforce consistent data standards to ensure compatibility, interoperability and shared understanding of the data. Data Integration Strategy: Implement an integrated data architecture that allows for seamless data flows. This includes designing systems that facilitate easy access and sharing of data, while ensuring data quality and compliance. Scalability and Flexibility: Design a scalable and flexible data architecture that can adapt to new technologies, increased data volumes and evolving business requirements.
Performance Monitoring	How effectively are data governance policies and procedures being adopted across different departments and what metrics can be used to track this adoption?	Establish clear Key Performance Indicators (KPIs) to measure the success of data governance initiatives. Examples include data quality scores, compliance rates and the number of resolved data issues. Metrics should cover areas like data accuracy, consistency, accessibility and security. Monitor the adoption rate of data governance practices among employees and stakeholders. Leverage data governance platforms and tools to automate performance monitoring and reporting.

References

1. OECD (2022), Going Digital Guide to Data Governance Policy Making, OECD Publishing, Paris, https://doi.org/10.1787/40d53904-en

2. https://atlan.com/data-governance-framework/

3. Data Governance Framework, Human Resource Management Information System, Ministry of Civil service and Administrative Reforms, 2015

4. NSW Data Governance Framework, https://data.nsw.gov.au/data-governance-toolkit-0/module-1-introduction-to-data-governance

MAURITIUS NATIONAL DATA STRATEGY

DATA SHARING POLICY TEMPLATE
ANNEX 2

Data Protection Office

CONTENTS

Data Sharing

Data sharing is the process of making data accessible to others, whether individuals, organizations or systems for specific purposes such as collaboration, service delivery, research or decision-making. It can involve personal, sensitive or non-personal data and is typically governed by agreements, policies or legal requirements to ensure that data is handled responsibly, securely and in compliance with Data Protection Act (DPA) and other applicable legislations. Proper data sharing fosters transparency, efficiency and trust while safeguarding privacy and confidentiality. Data sharing is definitely a good practice but it has to be balanced with the protection of individual privacy.

Some examples of countries that have implemented data sharing policies:

1

Mexico

Established the National Digital Strategy Office to coordinate the Digital Strategy, focusing on infrastructure, digital skills, interoperability, legal frameworks and open data.

2

Chile

Developed a centralized social information system under the Ministry of Social Development and Family to coordinate data use agreements and integrate data collection.

3

Singapore

Created the Smart Nation and Digital Government Group (SNDGG) to manage shared digital infrastructure, enforce standards and

Data sharing normally takes place in a variety of situations:

- several organisations collecting information and disclosing to each other;
- several organisations collecting information and disclosing to a third party/ies;
- one-off disclosures of data in unexpected or emergency situations; or
- different parts of the same organisation disclosing data to each other.

Before sharing any personal data you manage, you must consider all the express and implied legal implications. Your power to share information is subject to a number of legal constraints which normally go beyond the requirements of the DPA such as specific statutory prohibitions on sharing found in diverse pieces of legislations, copyright restrictions or a duty of confidentiality that may affect your power to share personal data. A duty of confidentiality may be expressly provided or implied depending on the nature of the information – medical or banking information, amongst others.

Some data sharing do not involve collection of personal data at all, for example where only statistics collected are shared without identifying any living individual. The DPA does not apply to anonymous data. For instance, records may be shared for research or data matching purposes.

You need to ask yourself these questions before effecting data sharing:-

Is the sharing justified?

- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing necessary and proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

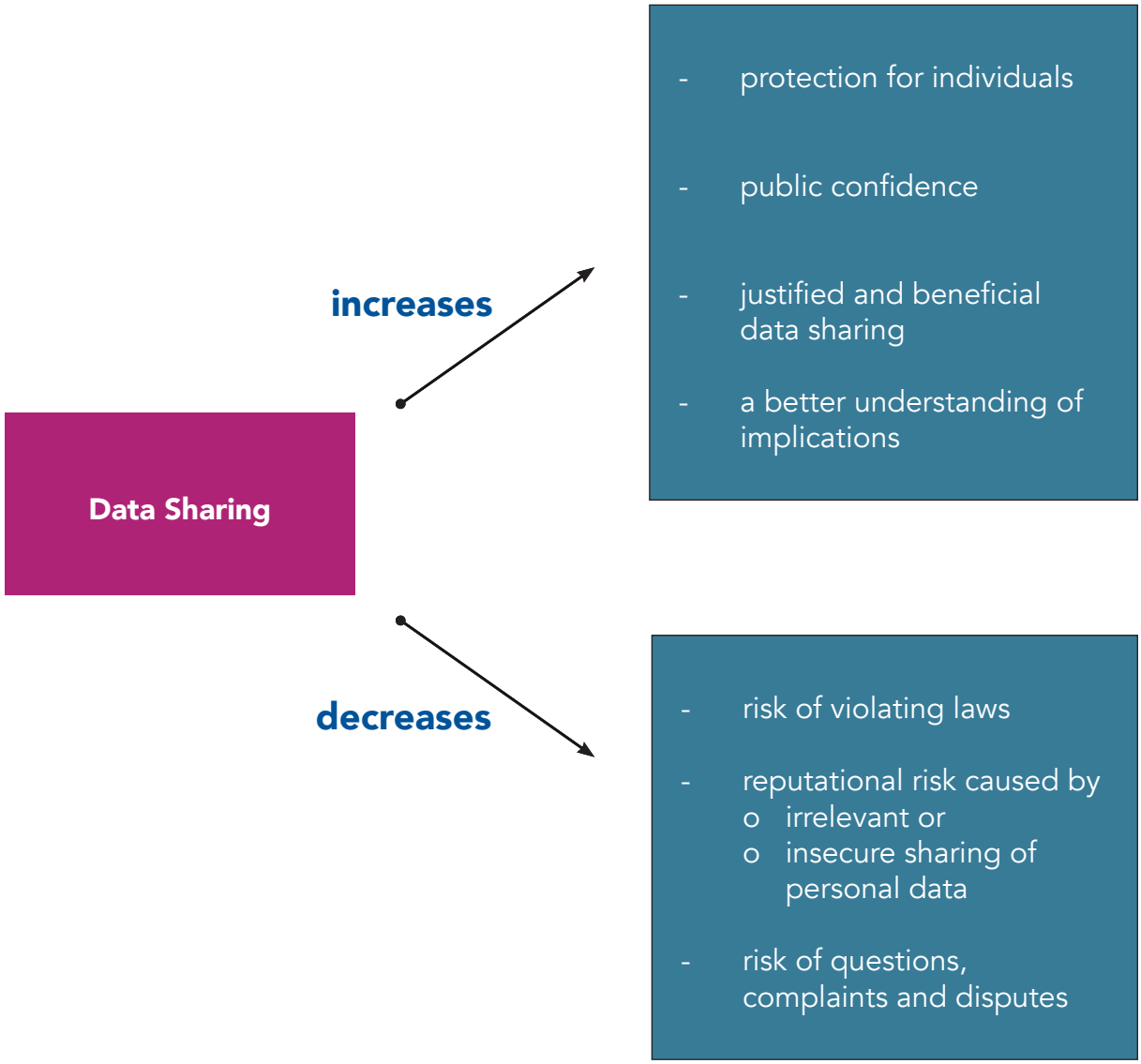
Do you have the legal power to share?

- The nature of the information you have been asked to share (for example, is it confidential?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

The DPA sets out the broad legal requirements to be considered when sharing personal data under section 28 of the DPA but it does not describe the practical measures to be taken for compliance, which is the purpose of this policy.

There is a multitude of benefits that may be acquired by controllers and processors through data sharing which include:

- minimised risk of violating laws and consequent enforcement actions by the Data Protection Office or other regulators;
- increased public confidence by ensuring that legally required safeguards are complied with;
- increased protection for individuals when their data is shared;
- increased justified and beneficial data sharing;
- reduced reputational risk caused by the irrelevant or insecure sharing of personal data;
- a better understanding of when, or whether, it is acceptable to share information without people's knowledge or express consent or in the face of an objection; and
- reduced risk of questions, complaints and disputes about the manner in which personal data is shared.


Data Sharing
increases
- protection for individuals
- public confidence
- justified and beneficial data sharing
- a better understanding of implications
decreases
- risk of violating laws
- reputational risk caused by
o irrelevant or
o insecure sharing of personal data
- risk of questions, complaints and disputes

The public sector

Most public sector organisations such as para-statals, other than government departments headed by a Minister, derive their powers entirely from an Act of Parliament which sets them up or from other such legislations regulating their activities. Your starting point in deciding whether any data sharing initiative may proceed, should be to identify the legislation that is relevant to your organisation. Even if it does not cater for data sharing explicitly, and usually it will not do so, it is the founding stone which can guide you.

The relevant legislation normally defines the organisation's functions in terms of its objects and the powers which the organisation may exercise in order to achieve these purposes. So it is necessary to identify where the data sharing in question would fit, if at all, within the range of activities that the organisation should carry out. Broadly speaking, there are three ways in which it may do so:

Express obligations – For instance, a public body may be legally obliged to share specific information with an organisation.

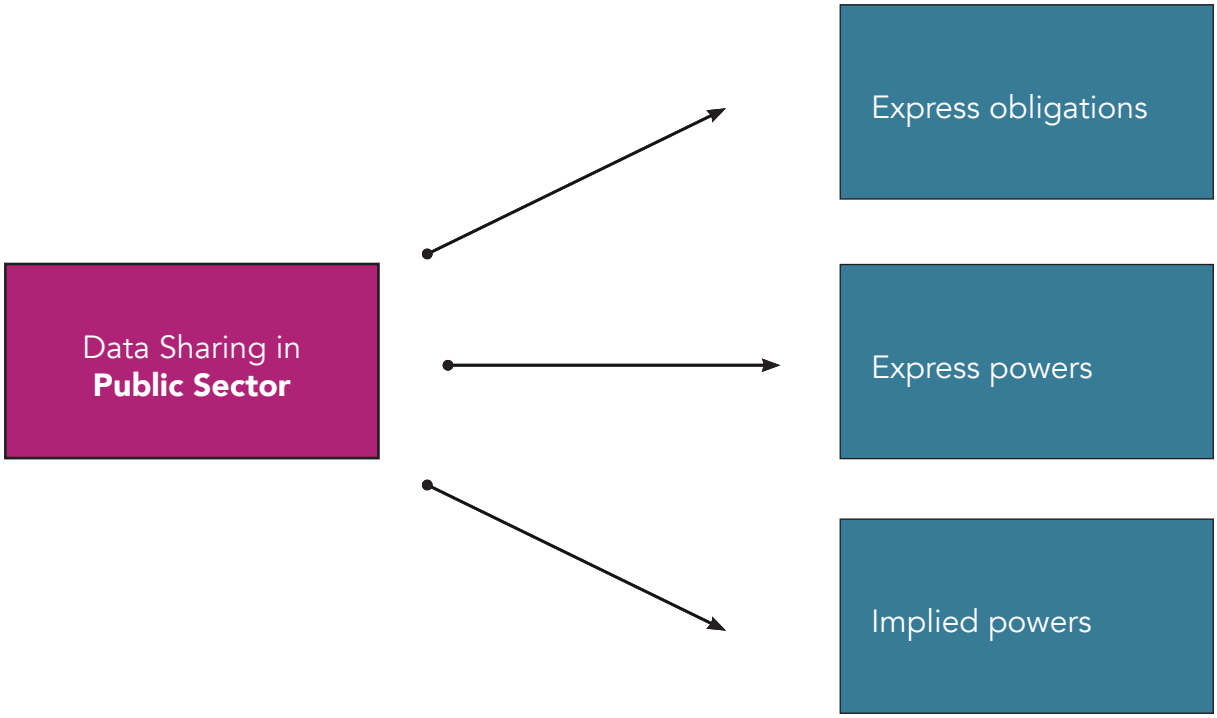
Express powers – A public body may be granted express power to share information by law to allow disclosure of information for specific purposes. Express statutory obligations and powers to disclose information are commonly called "gateways".

Implied powers

Often, the legislation regulating a public body's activities is silent on the issue of data sharing. In these circumstances it may be possible to rely on an implied power to share information derived from the express provisions of the legislation. This is because express statutory powers may be taken to authorise the organisation to do other things that are reasonably incidental to those which are expressly permitted.

To decide if you can rely on an implied power, you will need to identify the activity to which the proposed data sharing would be "reasonably incidental" to and then check that the organisation has the power to engage in that activity.

Whatever the source of an organisation's power to share information, you must check that the power covers the particular disclosure or data sharing arrangement in question – otherwise, you must not share the information unless, in the particular circumstances, there is an overriding public interest in a disclosure taking place. Whilst a disclosure in the public interest may be a legal defense in a particular case, it does not constitute a legal power to share data.

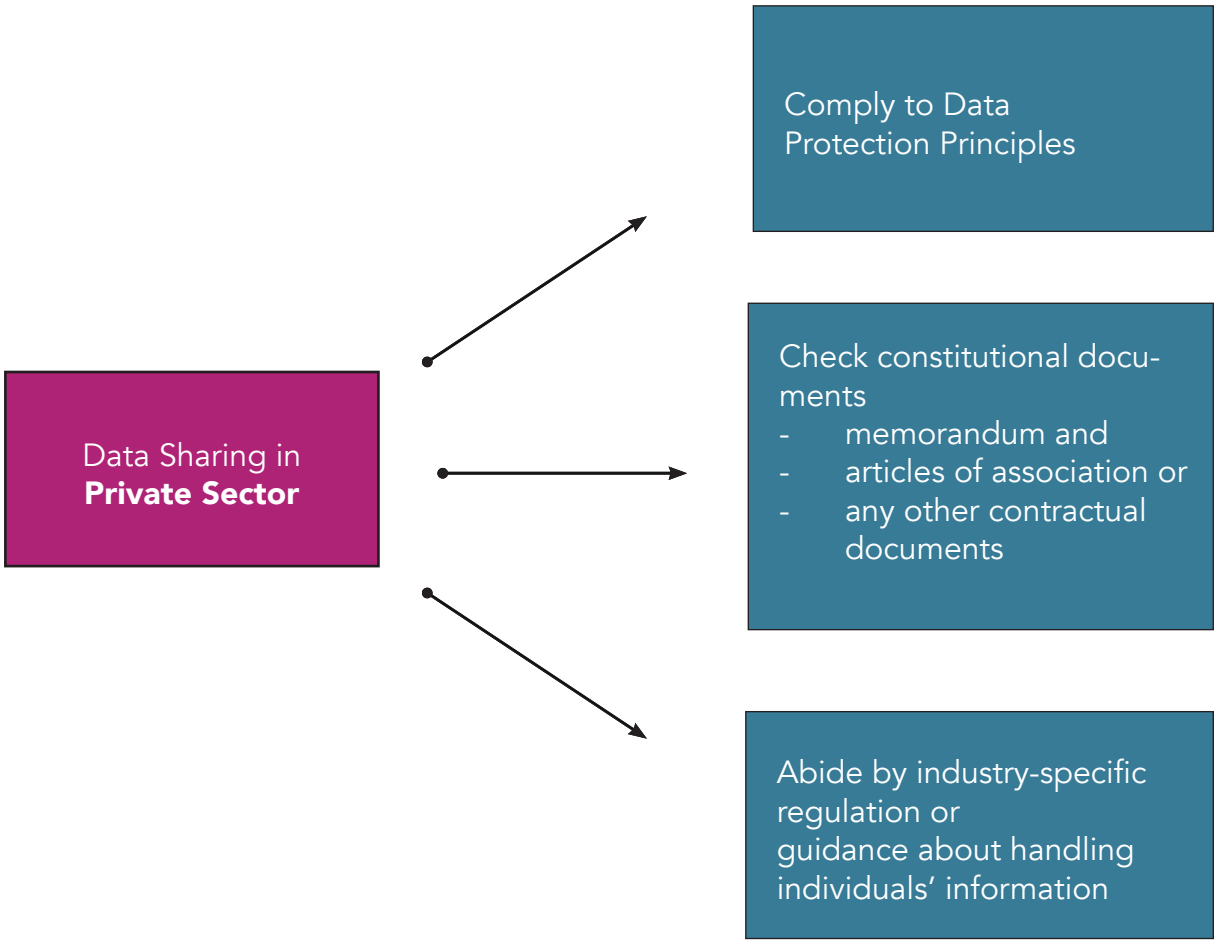


Private and Third Sector Organisations

The legal framework that applies to private and third sector organisations differs from that which applies to public sector organisations, which may only act within their statutory powers.

However, all organisations are required to comply fully with data protection principles. It is advisable for a company to check its constitutional documents, such as its memorandum and articles of association or any other contractual documents, to make sure there are no restrictions that would prevent it from sharing personal data in a particular context.

Private and third sector organisations should also have regard to any industry-specific regulation or guidance about handling individuals' information as this may affect the organisation's ability to share information.



Sharing with a 'processor'

This policy is mainly about sharing personal data between controllers – i.e. where organisations determine the purposes for which and the manner in which the personal data is processed.

However, there is a form of data sharing where a controller shares data with another party that processes personal data on its behalf. In the DPA, these organisations are termed 'processors' who are not employees of the controller but an external partner.

The DPA draws a distinction between one controller sharing personal data with another and a controller sharing data with its processor. The DPA requires that a controller using a processor must ensure in a written contract, that:

- the processor only acts on instructions devolving from the controller; and
- it has appropriate security and organisational measures in place equivalent to those imposed upon the controller.

Thus, a processor involved in data sharing does not create direct data protection responsibilities of its own; they are all imposed on it through the contract with the controller who decides on the responsibilities of the processor.

Data Sharing with a Processor

"31 of DPA: Security of processing

(1) A controller or processor shall, at the time of the determination of the means for processing and at the time of the processing -

(a) implement appropriate security and organizational measures for-

i. the prevention of unauthorised access to;

ii. the alteration of;

iii. the accidental loss of; and

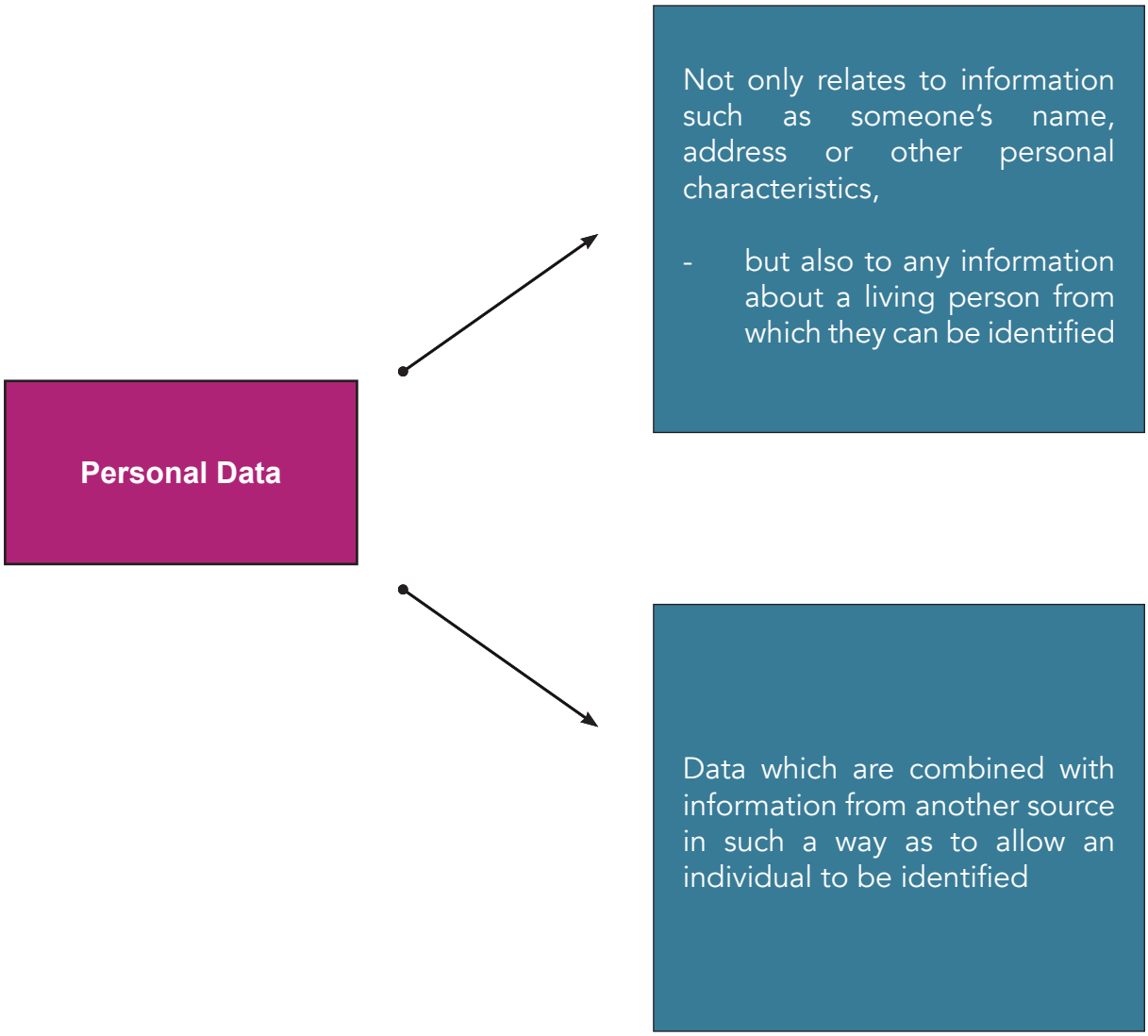
iv. the destruction of, the data in his control;"

A processor involved in data sharing

- does not create direct data protection responsibilities of its own; they are all imposed on it through its contract with the controller

Personal data: -

First, there is a need to understand that 'personal data' not only relates to information such as someone's name, address or other personal characteristics, but also to any information about a living person from which they can be identified. This means, for example, that even in making a request for statistical data from another organisation, there could still be a risk of disclosing the people concerned (eg, where there are very small numbers of the specified population in a particular neighbourhood). Data primarily not personal can also become 'personal' if they are combined with information from another source in such a way as to allow an individual to be identified.



Secondly, "special categories of personal data", in relation to a data subject as defined under section 2 of the DPA. –

(a) his racial or ethnic origin;

(b) his political opinion or adherence;

(c) his religious or philosophical beliefs;

(d) his membership of a trade union;

(e) his physical or mental health or condition;

(f) his sexual orientation, practices or preferences;

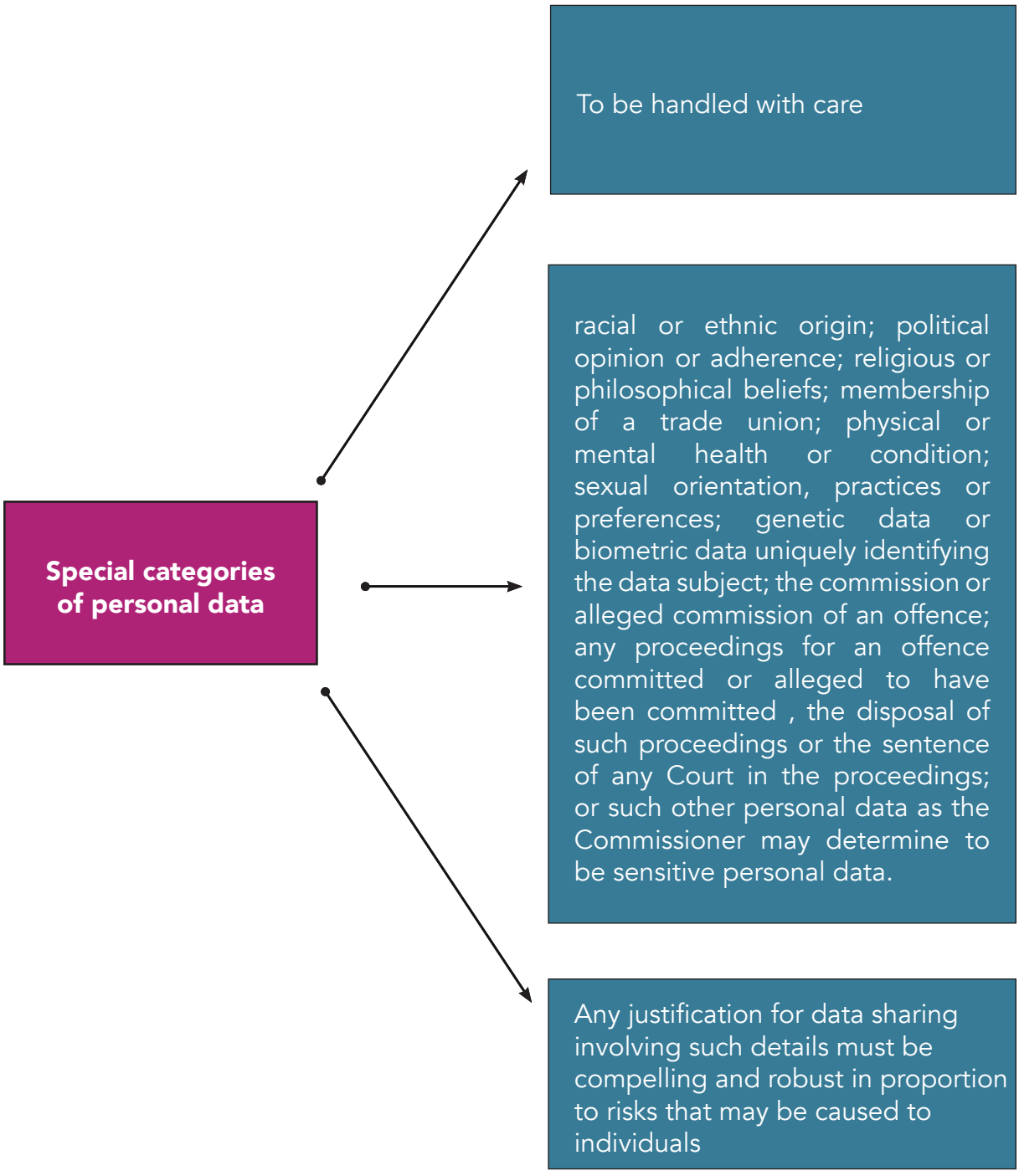
(g) his genetic data or biometric data uniquely identifying him;

(h) the commission or alleged commission of an offence by him;

(i) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or

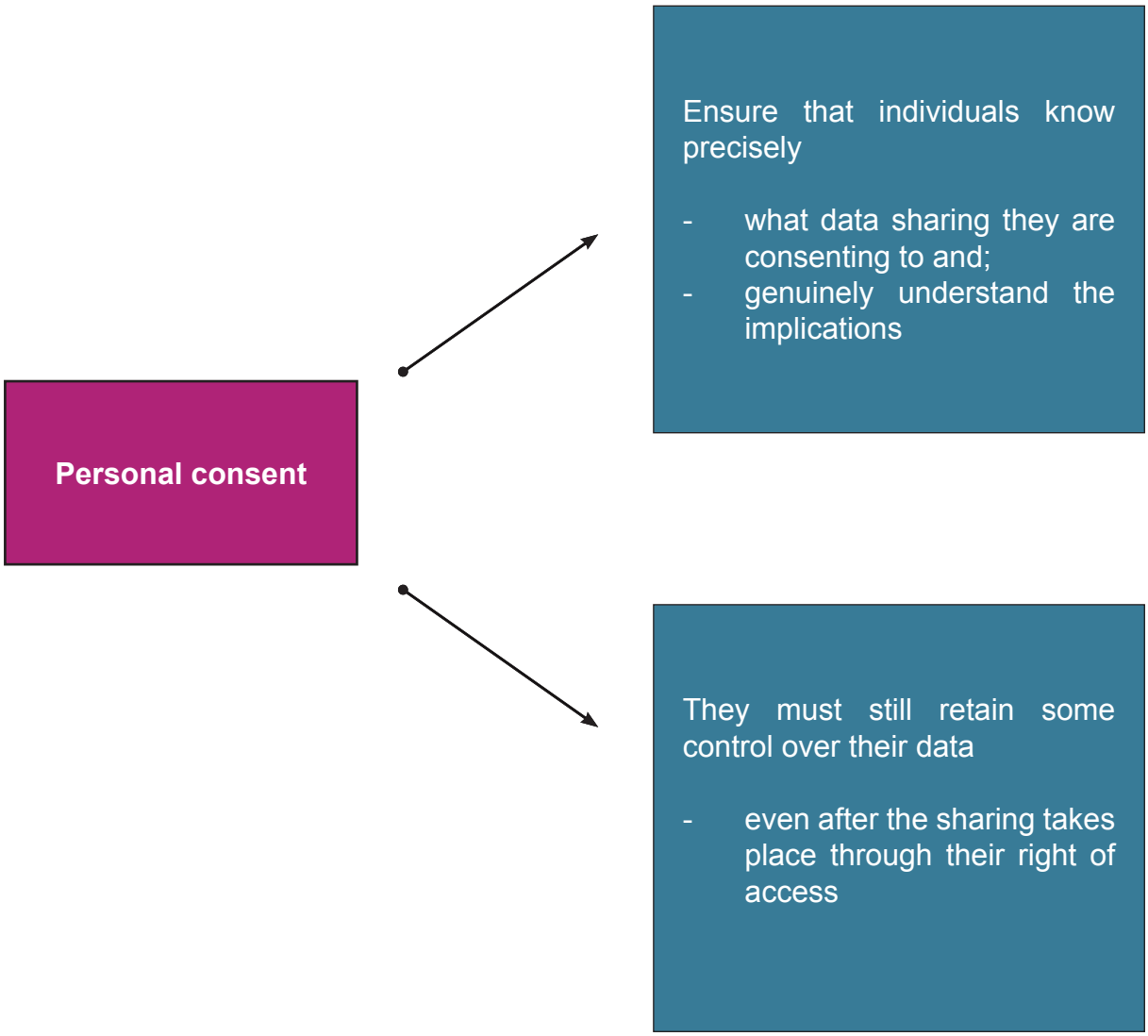
(j) such other personal data as the Commissioner may determine to be sensitive personal data;

"Special categories of personal data" have to be handled with care. It is necessary to avoid the interests of the individual being prejudiced in any way by the use of shared data. Any justification for data sharing involving such details must be compelling and robust in proportion to those risks.


Special categories of personal data
To be handled with care
racial or ethnic origin; political opinion or adherence; religious or philosophical beliefs; membership of a trade union; physical or mental health or condition; sexual orientation, practices or preferences; genetic data or biometric data uniquely identifying the data subject; the commission or alleged commission of an offence; any proceedings for an offence committed or alleged to have been committed , the disposal of such proceedings or the sentence of any Court in the proceedings; or such other personal data as the Commissioner may determine to be sensitive personal data.
Any justification for data sharing involving such details must be compelling and robust in proportion to risks that may be caused to individuals

The importance of personal consent:-

If you are going to rely on consent as your legal justification for sharing, you must ensure that individuals know precisely what data sharing they are consenting to and genuinely understand the implications. They must still retain some control over their data even after the sharing takes place through their right of access.



Legal Disclosures under the DPA:-

section 42 of the Data Protection Act further highlights the criminalisation of unlawful disclosures of personal data where any controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purposes for which the data was collected, he is committing an offence, liable on conviction to a fine not exceeding Rs 200,000 and to imprisonment not exceeding 5 years.

section 44 of the Data Protection Act also provides for exemptions for disclosures of personal data as follows:

"section 44 of the DPA. Exceptions and restrictions

(1) No exception to this Act shall be allowed except where it constitutes a necessary and proportionate measure in a democratic society for –

(a) subject to subsection (4), the protection of national security, defence or public security;

(b) the prevention, investigation, detection or prosecution of an offence, including the execution of a penalty;

(c) an objective of general public interest, including an economic or financial interest of the State;

(d) the protection of judicial independence and judicial proceedings; or

(e) the protection of a data subject or the rights and freedoms of others;

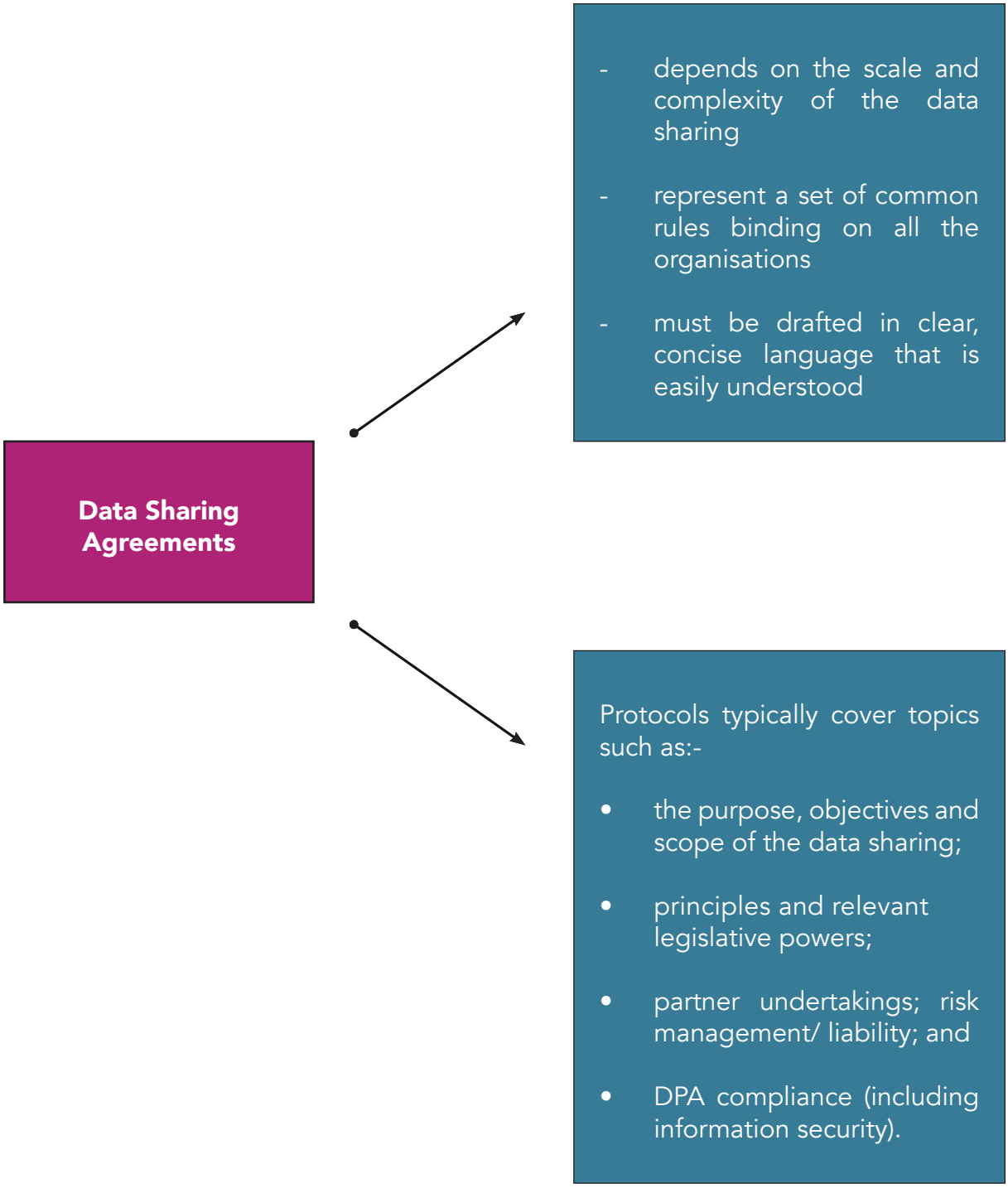
(f) issue of any licence, permit or authorisation during the COVID-19 period.

[Added 1/20 (cio 23/3/2020]

(2) The processing of personal data for the purpose of historical, statistical or scientific research may be exempt from the provisions of this Act where the security and organisational measures specified in section 31 are implemented to protect the rights and freedoms of data subjects involved."

Data Sharing Agreements:-

Data Sharing Agreements can be drafted in various flexible ways, depending on the scale and complexity of the data sharing endeavour in question. They represent a set of common rules binding on all the organisations involved in a data sharing initiative. The agreement should be drafted in clear, concise language that is easily understood.



Data Sharing Protocols may additionally be developed to strengthen data sharing agreements, clarifying the process and types of information that may be exchanged. Developing a protocol may assist in managing the potential uncertainties about what can be shared, by whom and under what circumstances, and reduce apprehensions about what is legal and what is not.

Protocols typically cover topics such as:-

- the purpose, objectives and scope of the data sharing;
- principles and relevant legislative powers;
- partner undertakings; risk management/ indemnity; and
- DPA compliance (including information security).

A data sharing agreement should at least document the following issues:

- the purpose, or purposes, of the sharing;
- the potential recipients or types of recipient and the circumstances in which they will have access;
- the data to be shared- Could the objective be achieved without sharing the data or by anonymising it?;
- data quality – accuracy, relevance, usability etc;
- data security;
- retention of shared data;
- individuals' rights – procedures for dealing with access requests, queries and complaints;
- review of effectiveness/termination of the sharing agreement;
- sanctions for failure to comply with the agreement or breaches by individual staff; and
- your agreement should also deal with the main practical problems that may arise when sharing personal data. This should ensure that all organisations involved in the sharing:
    - have detailed advice about which datasets may be shared, to prevent irrelevant or excessive information being disclosed;
    - make sure that the data being shared is accurate, for example by requiring a periodic sampling exercise;
    - are using compatible datasets and are recording data in the same way.

- The agreement could include examples showing how particular data items – for example dates of birth – should be recorded;

- The agreement must have common rules for the retention and deletion of shared data items and procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules;

- The agreement must have common technical and organisational security arrangements, including for the transmission of the data and procedures for dealing with any breach of the agreement;

- The agreement must have a timescale for assessing the ongoing effectiveness of the data sharing initiative and of the agreement that governs it; and

- The agreement must develop systems to facilitate data sharing. Build the need for data sharing into data capture and IT/ database systems design. This will avoid later costs and reduce risks of resistance to data sharing.

- Staff should be aware of security policies and procedures and be trained in their application. In particular you will need to:

    - design and organise your security to fit the type of personal data you disclose or receive and the harm that may result from a security breach;

    - be clear about which staff members in the organisations involved in the sharing are responsible for ensuring information security.

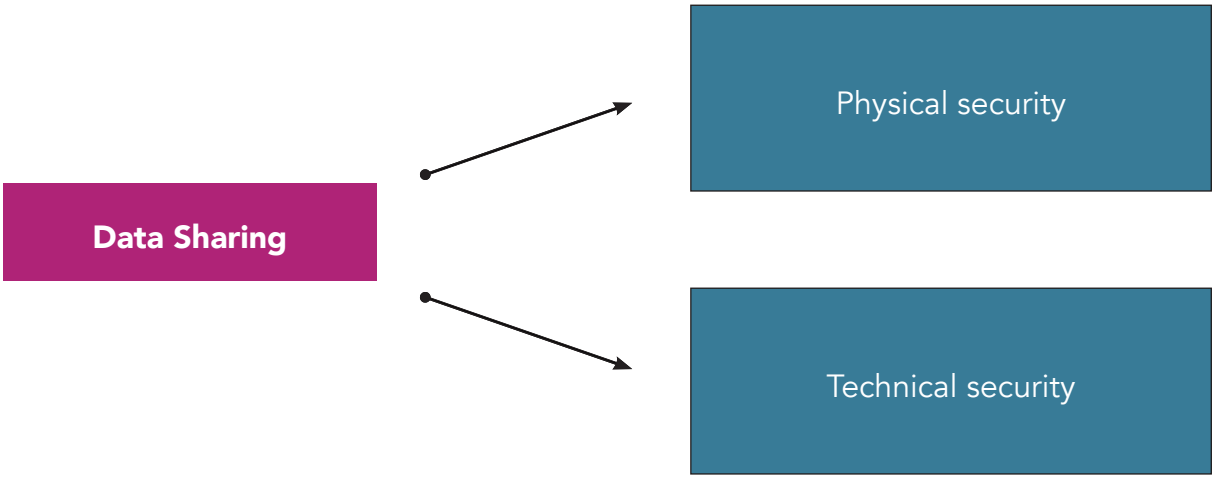
    - They should meet regularly to ensure appropriate security is maintained.

    - Have appropriate monitoring and auditing procedures in place; and

    - be ready to respond to any failure to adhere to a data sharing agreement swiftly and effectively.

    - Finally, you are required to register with the Data Protection Office as Controller and Processor and appoint a Data Protection Officer.

Data Sharing Security



Physical security

- Do you have good quality access control systems for your premises?
- How are visitors supervised?
- Is paper based information stored and transferred securely?
- Are laptops and removable media such as discs and memory sticks locked away at night?
- Do you dispose of paper waste securely, for example by shredding?
- Do you advise staff on how to use their mobile phones securely and minimise the risk of them being stolen?

Technical security

- Is your technical security appropriate to the type of system you have, the type of information you hold and what you do with it?
- If you have staff that work from home, do you have security measures in place to ensure that this does not compromise security?
- How is encryption of personal data implemented and managed?
- Have you identified the most common security risks associated with using a web-product – e.g. a website, web application or mobile application?
- How do you control access to your systems?
- Do you set privileges to information based on people's need to know?
- What measures are in place for the security of information in transit?

Respect the need for privacy of the individual

The use of 'mitigation measures' which compensate partially or wholly for possible negative impacts. Examples include:

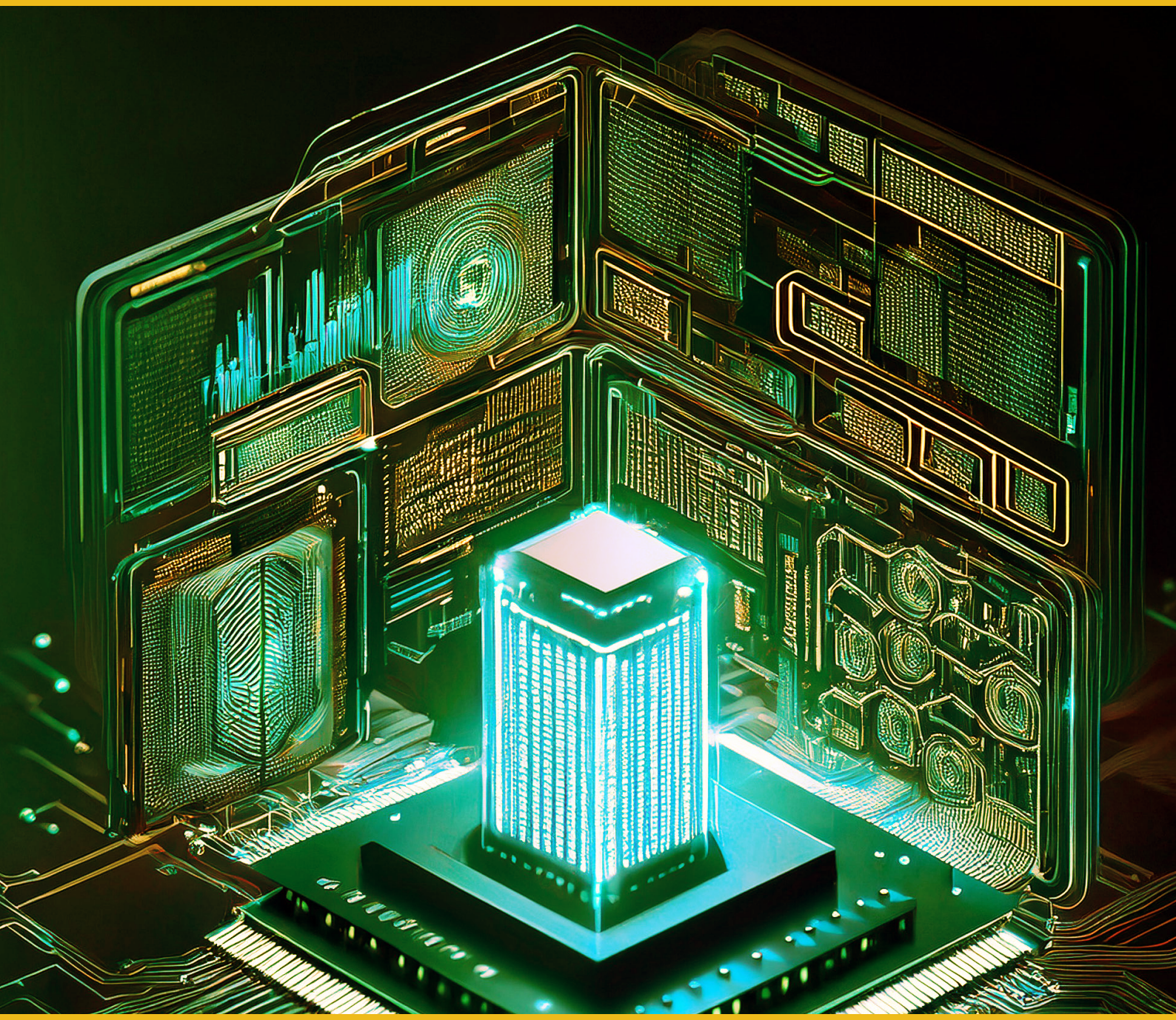
- minimising the retention of personal data and adopting 'destruction schedules' under section 27 of the DPA.
- limiting the use of information to a very specific purpose, with organisational and technical safeguards preventing its broader application
- incorporating a complaints handling system, backed by sanctions and enforcement powers.

When sharing personal data there are some practices that you should avoid which could lead to regulatory action:

- Misleading individuals about whether you intend to share their information. For example, not telling individuals you intend to share their personal data because you think they may object.
- Sharing excessive or irrelevant information about people. For example, routinely sharing details about individuals that are not relevant to the purpose that the information is being shared for.
- Sharing personal data when there is no need to do so – for example where anonymised statistical information can be used to plan service provision.
- Not taking reasonable steps to ensure that information is accurate and up to date before you share it. For example, failing to update address details before sharing information, leading to individuals being pursued at the wrong address or missing out on important information.
- Using incompatible information systems to share personal data, resulting in the loss, corruption or degradation of the data.
- Having inappropriate security measures in place, leading to loss or unauthorised disclosure of personal details. For example, sending personal data between organisations on an unencrypted memory stick which is then lost or faxing sensitive personal data to a general office number.

MAURITIUS NATIONAL DATA STRATEGY

DATA SHARING PROTOCOL TEMPLATE
ANNEX 3



Data Protection Office

CONTENTS

Data Sharing Protocol Template

1. Preface

This Data Sharing Policy outlines the principles, requirements and procedures governing the sharing of personal data in compliance with the Data Protection Act (DPA). Under the Act, organizations have a legal duty to ensure that personal data is handled lawfully, securely and transparently with respect for individuals' rights. Achieving the right balance between sharing data to improve services and protecting personal privacy is crucial.

2. Scope

2.1 This protocol sets out the rules that all people working for or with the government must follow when using and sharing information.

2.2 This protocol applies to all information shared by organisation. It covers all forms of data sharing, including internal and external sharing, whether electronic, verbal or written.

3. Aims and Objectives

3.1 The protocol aims to provide guidance to ensure the secure transfer of information which is shared for justifiable and lawful purposes.

3.2 These aims include:

a. To guide entities on how to share information lawfully.
b. To explain the security and confidentiality laws and principles of information sharing.
c. To increase awareness and understanding of the key issues.
d. To emphasise the need to develop and use Information Sharing Agreements.
e. To support a process that will monitor and review all information flows.
f. To encourage flows of information.
g. To identify the legal basis for information sharing under the provisions of the DPA and other applicable legislations.
h. To comply with Section 36 of the DPA for transfer of personal data abroad.

4. The Legal Framework

4.1 The principal legislations concerning the protection and use of personal information are listed below:

- Data Protection Act (DPA);
- Electronic Transactions Act;
- Cybersecurity and Cybercrime Act; and
- Freedom of Information laws and other legislations pertaining to data handling and management

5. Information covered by this Protocol

This protocol covers all information, including personal data and special categories of personal data as defined in the Data Protection Act (DPA).

5.1. Under section 2 of the DPA, personal data means any information relating to a data subject.

5.2. Anonymised Data

5.2.1 Organizations must ensure anonymised data, especially when combined with other information from different agencies, does not identify an individual, either directly or indirectly.

5.2.2 Anonymised data about an individual can be shared without consent, in a form where the identity of the individual cannot be ascertained when: reference to any data item that can lead to an individual being identified has been removed.

6. Principles for Data Sharing

- Lawfulness: Compliance with all relevant legal and regulatory frameworks.
- Transparency: Clear documentation and justification of data sharing practices.
- Purpose Limitation: Data shared only for legitimate, defined purposes.
- Minimization: Sharing only the minimum data necessary.
- Security: Adherence to national cybersecurity and data protection standards.
- Interoperability: Use of standardized formats and metadata.

7. Responsibilities When Sharing Information

7.1 General

Under section 14 of the DPA, every controller or processor has the legal obligation to register with the Data Protection Commissioner and to fulfil the legal obligations set out under Part IV of the DPA. Thus, each entity is responsible for ensuring that its organisational and security measures protect the lawful use of information shared under this Protocol in accordance with sections 21 and 22 of the DPA. These include:

7.1.1 The appointment of a Data Protection Officer to oversee data protection compliance in the organisation.

7.1.2 Organisations are responsible for independently or jointly auditing compliance with the Information Sharing Agreements in which they are involved within reasonable time-scales.

7.1.3 Every organisation must consider making it a condition of employment that employees will abide by their rules and policies in relation to the protection and use of confidential information. This condition must be written into employment contracts and any failure by an individual to follow the policy must be dealt with in accordance with that organisation's disciplinary procedures.

7.1.4 Every organisation must ensure that their contracts with external service providers include a condition that they abide by their rules and policies in relation to the protection and use of confidential information.

7.1.5 The organisation originally supplying the information must be notified of any breach of confidentiality or incident involving a risk or breach of the security of information.

7.1.6 Organisations must have a written policy for retention and disposal of information in accordance with section 27 of the DPA.

7.2 Personal Data

Personal data must only be shared for a specific lawful purpose under section 28 of the DPA or where appropriate consent has been obtained.

7.2.1 Staff must only be given access to personal data when authorised, in order for them to perform their duties in connection with the services they deliver.

7.2.2 In case of an occurrence of a personal data breach.in an organisation, the latter shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Commissioner under section 25 of the DPA.

7.2.3 Pursuant to section 34 of the DPA, a data protection impact assessment is required in situations where data processing is likely to result in a high risk to the rights and freedoms of individuals.

7.2.4 In accordance with section 37 of the DPA, an organisation must provide data subjects with access to their personal data upon their written requests and free of charge unless the request is manifestly excessive.

7.3 Non-Personal Data

7.3.1 Organisations must not assume that non-personal information is not sensitive and can be freely shared and the organisation from whom the information is originated should be contacted before any further sharing takes place.

8. Restrictions on use of Information Shared

8.1 All shared information, personal or otherwise must only be used for the purpose(s) specified at the time of disclosure(s) as defined in the relevant Information Sharing Agreement unless obliged under statute or regulation or under a court order or as agreed contractually.

9. Consent

9.1 Consent is one of the lawful grounds on which personal data processing has to be based, pursuant to section 28 of the DPA. However, subject to section 28 (1) (b) consent of the data subjects is not required where the processing is necessary-

(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; or

(ii) for compliance with any legal obligation to which the controller is subject; or

(iii) in order to protect the vital interests of the data subject or another person; or

(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

(v) the performance of any task carried out by a public authority; or

(vi) the exercise, by any person in the public interest, of any other functions of a public nature; or

(vii) for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or

(viii) for the purpose of historical, statistical or scientific research.

9.2 The DPA introduces requirements for controllers to make additional arrangements to ensure they obtain, maintain and are able to demonstrate valid consent. Section 24 of the DPA sets out these additional conditions for valid consent, with specific provisions on keeping records of consent and the right to easily withdraw consent.

9.3 Consent has to be notified by some communication between the organisation and the data subject unless the organisation relies on any criteria under section 28 (1) (b) mentioned above where consent is not required. As regard the processing of special categories of personal data, the organisation should comply with Section 29 of the DPA. Where consent is given to process special categories of personal data, the organisation must ensure that the data subject's consent is clear and cover items such as the specific details of processing, the data to be processed and the purpose for processing.

9.4 Children's personal data enjoys specific protection under section 30 of the DPA. Children have the same rights as adults over their personal data. For children under 16, consent is required from whoever holds parental responsibility for them. The organisation must take every reasonable effort to verify consent has been given or authorised.

10. Liability

10.1 Each entity must take full responsibility for any breach of this protocol agreement. This includes cases of unauthorized access, loss, theft, misuse, destruction or improper disclosure of personal data shared under this agreement, whether caused by the entity itself, its employees, contractors or anyone under its control.

11. Security

11.1 Under section 31 of the DPA, organisations must secure sharing of data by implementing robust security and organizational measures. These

measures must prevent unauthorized access, data alteration, accidental loss, unauthorized disclosure and destruction of data. Appropriate steps should also include pseudonymization and encryption of personal data, maintaining the confidentiality and integrity of systems, and restoring access to data in case of incidents. Organisations must ensure that the minimum standards of security that they require are agreed with organisations with whom their information will be shared.

11.2 Each entity signing this protocol as well as any individual agreeing to the confidentiality terms commits to complying with the established data security standards. This ensures that all parties involved in data sharing uphold the principles of data privacy by maintaining the confidentiality, integrity and security of shared information in line with the requirements of the DPA.

12. Information Quality

12.1 Information quality needs to be of a standard fit for the purpose information is to be used for, including being complete, accurate and as up to date as required for the purposes for which it is being shared. Without this, any decision made on the information may be flawed and inappropriate actions may result. Personal data must be accurate and where necessary regularly updated. Every reasonable step must be taken to promptly erase or correct any personal data that is found to be inaccurate as outlined in section 21 of the DPA.

12.2 All organisations are expected to give undertakings that information meets a reasonable quality level for the proposed purposes for which it is being shared and be able to evidence this by maintaining a record of processing operations under section 33 of the DPA.

13. Training

13.1 All organisations processing information shared under this protocol are expected to be trained to a level that enables them to undertake their duties confidently, efficiently and lawfully.

14. Individual Responsibilities

14.1 Every individual working for the organisation is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.

14.2 Every individual must know how to obtain, use and share information they legitimately need to do their job.

14.3 Every individual has an obligation to request proof of identity or takes steps to validate the authorisation of another before disclosing any information requested under this protocol.

14.4 Every individual must uphold the general principles of confidentiality, follow the guide-lines set out in this protocol and seek advice when necessary.

14.5 Every individual must be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that can lead to their dismissal. Criminal proceedings may also be brought against that individual.

15. General Principles

15.1 The principles outlined in this protocol are recommended good standards of practice and legal requirements that should be adhered to by all organisations.

15.2 This protocol sets the core standards applicable to all organisations and to secure the flow of personal information.

15.3 All parties signed up to this protocol are responsible for ensuring that organisational measures are in place to protect the security and integrity of personal information and that their staff are properly trained to understand their responsibilities and comply with the law.

15.4 This protocol has been written to set out clear and consistent principles that satisfy the requirements of DPA that all staff must follow when using and sharing personal information.

16. Roles and Responsibilities

Role	Responsibility
Data Management office (DMO)	Approve, monitor and audit data sharing agreements and practices.
Data Provider	Ensure data is accurate, lawful and suitable for sharing.
Data Recipient	Use data only for agreed purposes and maintain confidentiality.

17. Data Sharing Request Process

Step 1: Submission

- Submit a Data Sharing Request Form
- Include data description, purpose, legal basis and protection measures

Step 2: Assessment

- DMO reviews the request for compliance, impact and feasibility

Step 3: Agreement

- Sign a Data Sharing Agreement (DSA)

Step 4: Implementation

- Share data via secure channels
- Apply data standards, encryption and audit logs

Step 5: Monitoring & Review

- Periodic reporting by DMO
- Review against performance indicators and compliance checks

18. Review and Amendments

This protocol will be reviewed periodically to ensure continued compliance with the DPA and any relevant regulatory changes.

19. Contact Information

Data Management Office

Email: [Insert]

Phone: [Insert]

Website: [Insert]

Chief Data Officer: [Insert Name]

Appendix A: Data Sharing Request Form

Section	Details
1. Requesting Entity	Name of organization, department or agency
2. Contact Person	Name, title, email, phone
3. Purpose of Data Sharing	Describe the objective (e.g., research, service improvement, policy development)
4. Description of Data Requested	Types of data, data fields, format, historical range
5. Legal Basis	Cite legal provisions, agreements, or statutory authority
6. Data Sensitivity Level	Public / Internal / Confidential / Highly Sensitive
7. Data Protection and Security Measures	Anonymization, encryption, access controls, etc.
8. Intended Recipients	Organizations, individuals or platforms receiving the data
9. Data Retention Plan	Duration and method of disposal/ deletion after use
10. Additional Documentation	Attach data maps, risk assessments, ethics approval if needed
11. Signature	Authorized requester's name, signature and date

MAURITIUS NATIONAL DATA STRATEGY

DATA RETENTION POLICY TEMPLATE
ANNEX 4

Data Protection Office

CONTENTS

Data Retention Policy Template

1.Purpose & Objective

This policy outlines guidelines for the storage, retention and disposal of personal data. It is designed to ensure proper handling of data to safeguard data subjects' privacy rights.

The policy aims to:

- Ensure lawful data processing and retention practices.
- Establish clear data retention periods across different categories.
- Safeguard personal data against unauthorized access, breaches and misuse.
- Promote accountability, transparency and ethical data management.

2. Scope & Applicability

This policy applies to all departments, employees, contractors and third-party service providers who handle data within [Organization Name]. It covers various types of data, including:

- **Employee Records** (contracts, payroll, performance evaluations)
- **Customer & Client Information** (contact details, purchase history, complaints)
- **Financial Data** (transactions, audit reports, tax filings)
- **Legal & Contractual Documents** (agreements, intellectual property records)
- **Operational & Technical Data** (server logs, analytics, backups)

3. Data Classification

Data is classified into categories based on its sensitivity and legal requirements which determine data retention periods and applicable security measures.

- Category 1 (Define Category 1 and its retention period)
- Category 2 (Define Category 2 and its retention period)
- Category 3 (Define Category 3 and its retention period)

4. Legal Compliance & Principles

[Organization Name] is committed to adhering to data protection laws and ethical principles, in particular Part IV of the Data Protection Act (DPA).

The key principles include:

- **Minimum Retention:** Retain data only as long as necessary for legal, regulatory or operational reasons.
- **Purpose Alignment:** Ensure retention supports the original lawful purpose of collection.
- **Security:** Protect data throughout its lifecycle, including storage and disposal.
- **Accountability:** Maintain documented retention schedules and review logs.
- **Disposal:** Delete or anonymize data securely at the end of the retention period.

5. Data Retention Schedule

Data will be retained based on legal requirements, business necessity and industry best practices.

Exceptional Retention Periods: Certain sensitive data (e.g., investigation records, litigation documents) may be retained beyond standard timelines, subject to executive approval or legal mandates.

Each organization must populate and maintain a retention schedule using the template below:

Data Type / Record Name	Data Owner	Legal / Regulatory Basis	Retention Period	Storage Location	Disposal Method
[e.g., Employee Records]					

6. Secure Storage & Access Control

To ensure data integrity and security, all personal data must be stored in a controlled environment, utilizing:

- **Access Restrictions:** Data access must be limited to authorized personnel based on job roles.
- **Encryption & Anonymization:** Sensitive records must be encrypted or anonymized to prevent unauthorized exposure.
- **Backup & Recovery Plans:** Secure backups must be regularly maintained and disposed of after expiration.

7. Secure Data Disposal Procedures

Data reaching the end of its retention period must be disposed of securely to prevent accidental leakage.

- **Digital Data:** Secure permanent deletion, overwriting, or anonymization to ensure recoverability.
- **Physical Records:** Confidential shredding or disposal through accredited data destruction providers.
- **Third-Party Systems:** Cloud-hosted or outsourced data must be destroyed per contractual agreements.

Each organization must populate and maintain a schedule for secure data disposal using the template below:

Method	Suitable For	Description
Digital Shredding	Internal servers, databases	Irretrievable deletion using certified software
Overwriting	Reusable media	Multiple write passes using sanitization protocols
De-identification	Statistical datasets	Anonymization or pseudonymization
Physical Destruction	Paper records, devices	Shredding, incineration, or degaussing

8. Monitoring, Audits & Policy Review

- Regular Audits: Periodic checks will be conducted to ensure compliance with this policy. The Data Management Office (DMO) will conduct annual retention audits.
- Employee Training: Staff handling data must receive mandatory training on secure data retention and disposal practices.

9. Compliance Responsibilities & Enforcement

The Data Protection Officer (DPO) and senior management are responsible for enforcing this policy. Non-compliance may result in:

- Disciplinary action against employees violating retention rules.
- Legal consequences for external entities breaching contractual data requirements.
- Regulatory fines and /or imprisonment when data management does not meet data protection standards under the DPA.

10. Role and Responsibilities

Role	Responsibility
Data Management Office	Define standards, audit compliance and publish national schedules
Controller	Ensure compliance with retention periods and secure deletion
Processor	Follow the retention and disposal terms in contractual agreements

11. Review

This policy may be reviewed and updated periodically to ensure alignment with legal requirements and best practices.

12. Contact

Data Management Office

Website: [Insert]

Email: [Insert]

Phone: [Insert]

Chief Data Officer: [Insert Name]

Design and Print
The Government Printing Department

2026