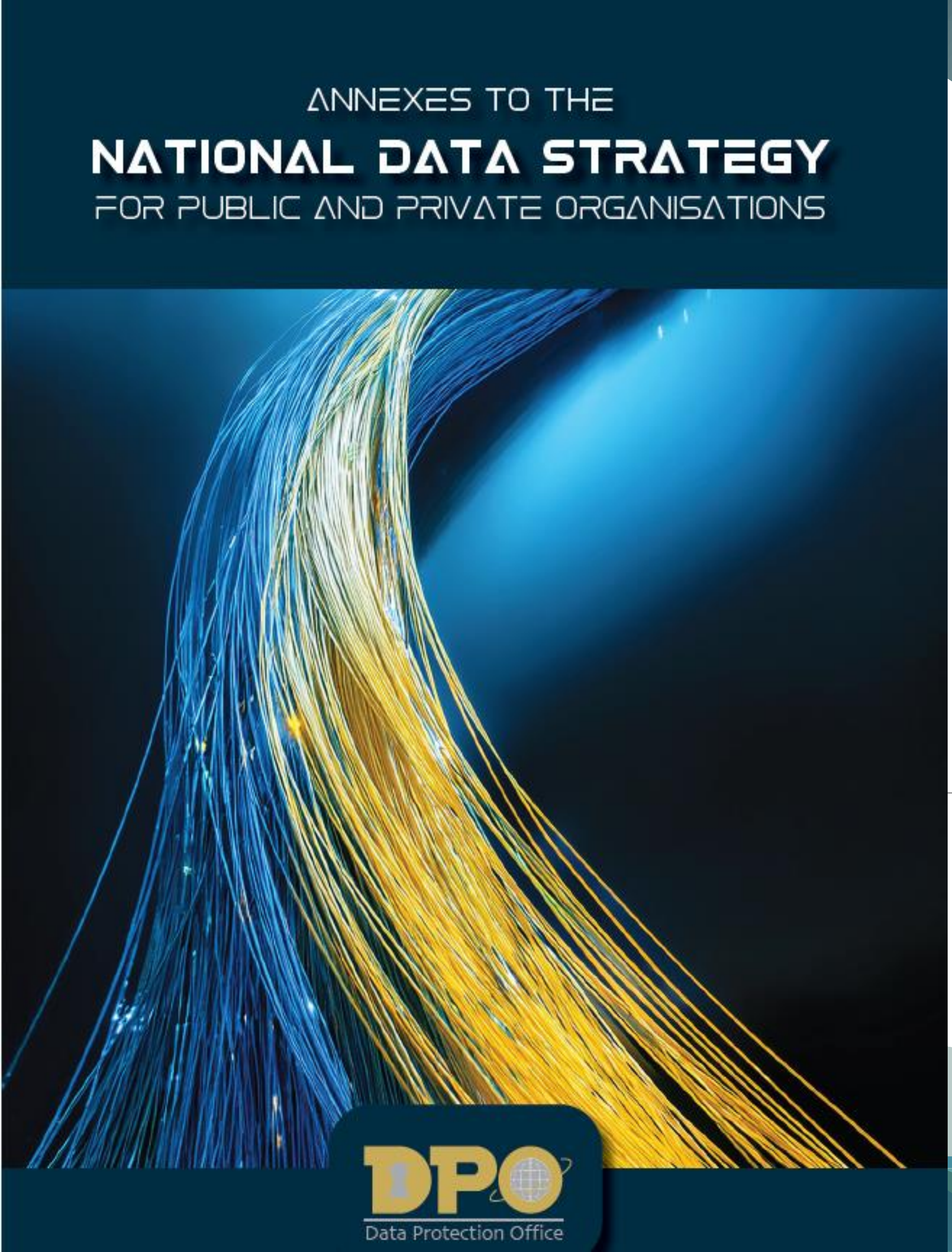


ANNEXES TO THE

NATIONAL DATA STRATEGY

FOR PUBLIC AND PRIVATE ORGANISATIONS

DPO

Data Protection Office

Part 2
Annexes to the National Data Strategy

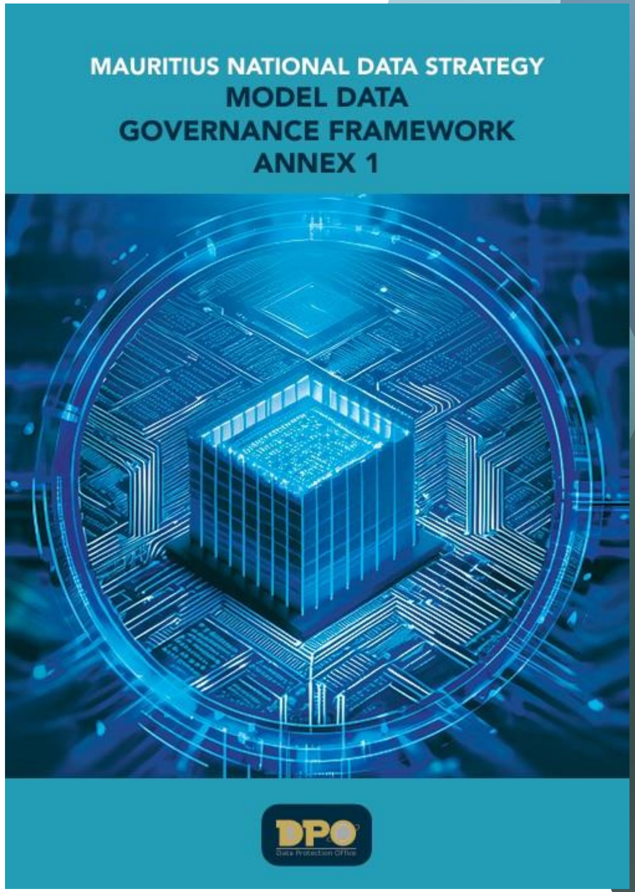
by Mr Reza Mukoon

What is a Data Governance Framework

- A set of rules, processes and responsibilities that dictate how an organisation collects, organizes, stores and uses its data.

- It enables data democratisation by giving all **staff**, regardless of technical background, trusted access to data to support informed decision-making, performance measurement, strategic planning and innovation.

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



MAURITIUS NATIONAL DATA STRATEGY
MODEL DATA
GOVERNANCE FRAMEWORK
ANNEX 1

DPO

Data Governance Framework rests on 5 Pillars

1. Processes, policies, standards and procedures.

Clear and well defined policies are required to articulate strategic direction, for desired bahaviours and expected outcomes

2. Organizational structure, roles and responsibilities.

The organization should appoint the Data Owner, Data Steward, Data Protection Officer, Chief Information Officer, Data Custodian, Data Specialist, Data User and the Data Management Committee and their respective responsibilities.

3. Technology and Tool Capabilities

Modern tools for data quality and data security are essentials for data governance management

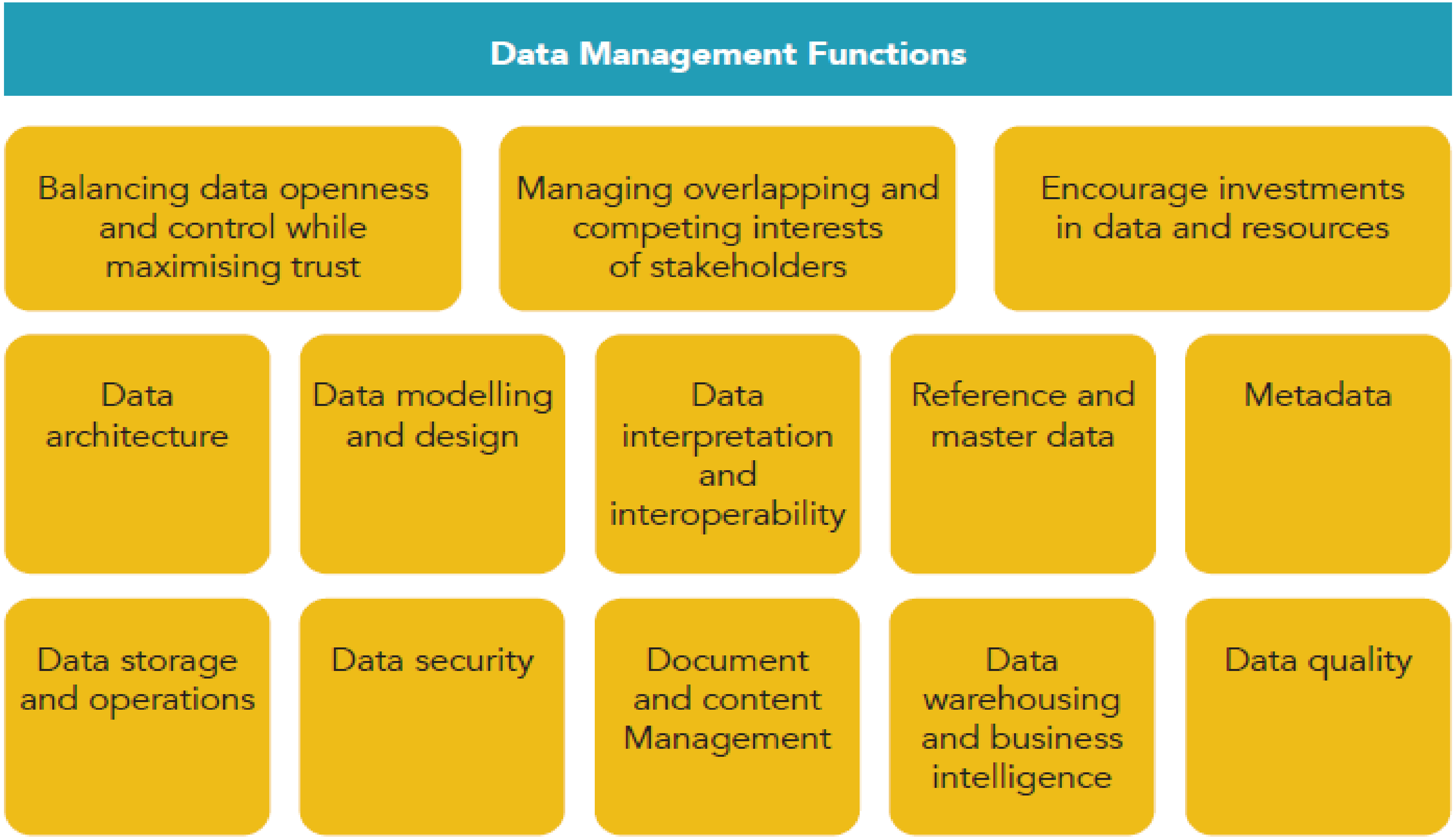
4. Metadata content or data catalog

Catalogue the technical and operational attributes of data to handle Big data

5. Compliance and Risk Management

Train employees, performs Audits and Monitoring with clear guidelines on secure data handling to adhere to data protection law and mitigate risks such as data breaches.

Core Elements of a Data Governance Framework



Data Management Functions

Balancing data openness and control while maximising trust

Managing overlapping and competing interests of stakeholders

Encourage investments in data and resources

Data architecture

Data modelling and design

Data interpretation and interoperability

Reference and master data

Metadata

Data storage and operations

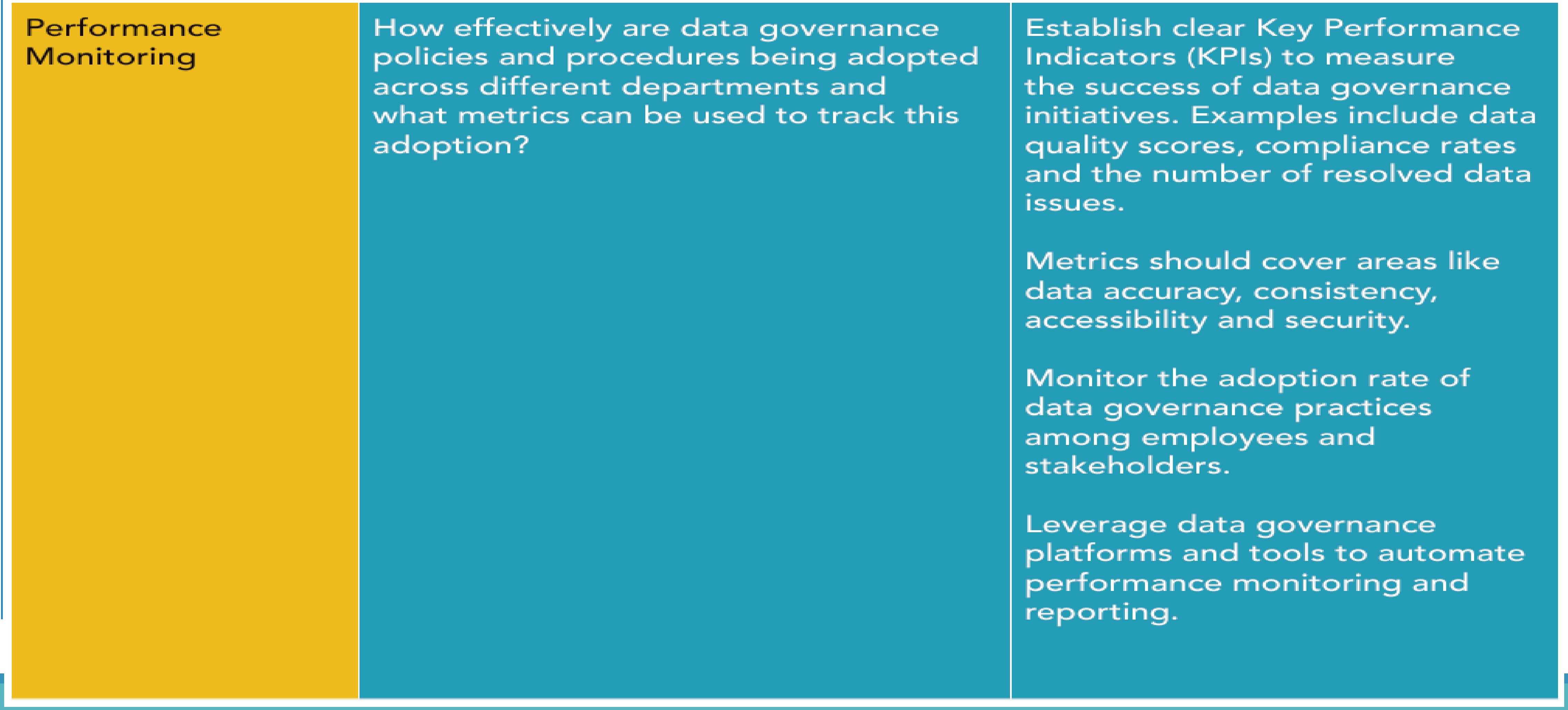
Data security

Document and content Management

Data warehousing and business intelligence

Data quality

Data Management Functions Checklist



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.

DATA SHARING POLICY TEMPLATE
Annex 2

- This Annex defines the rules for 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.
- A good practice that has to be balanced with the protection of individual privacy.

Data Sharing normally occurs:-

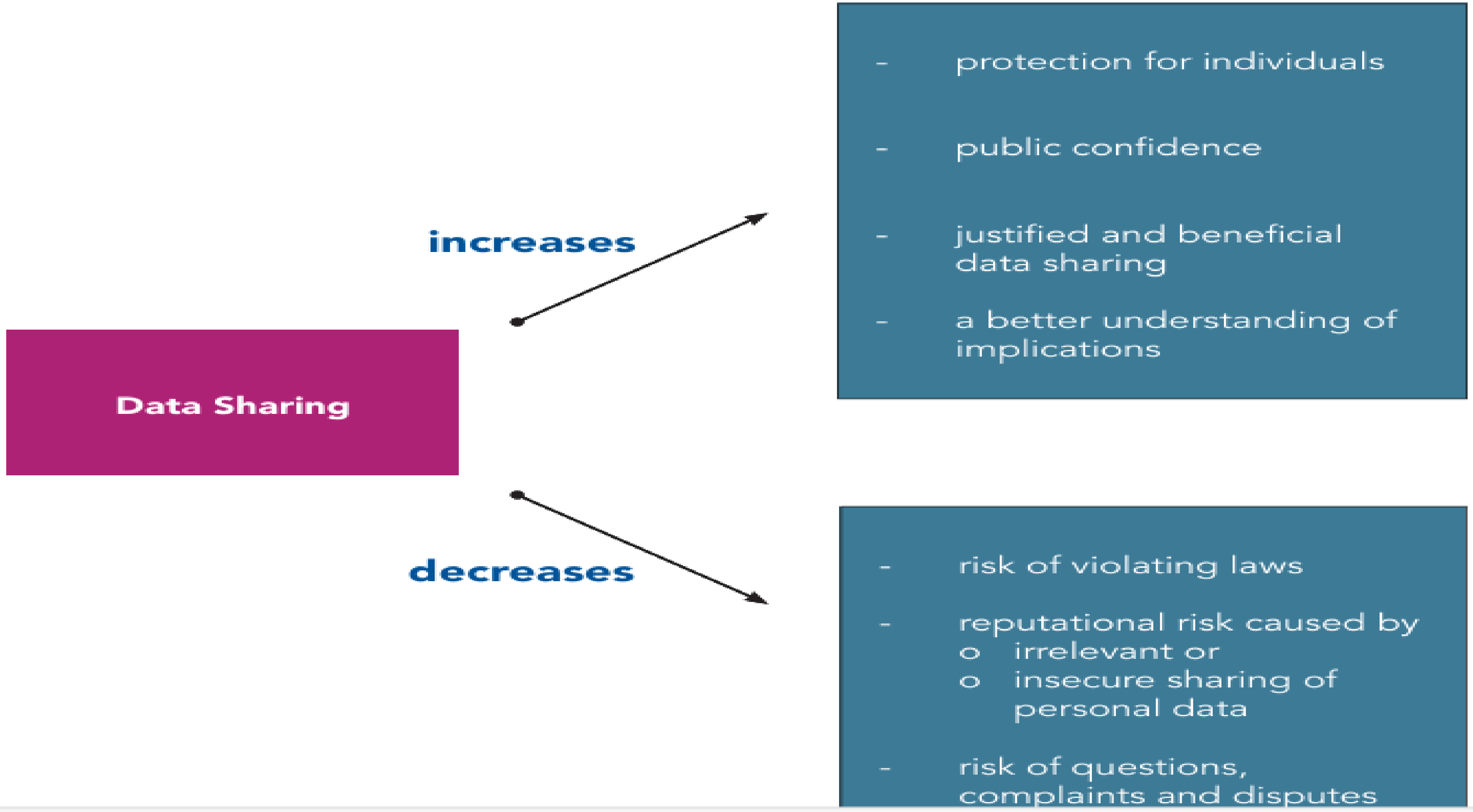
among organisations, with third party/ies, in emergency situations or within the same organization

MAURITIUS NATIONAL DATA STRATEGY

DATA SHARING POLICY TEMPLATE
ANNEX 2

DPO
Data Protection Office

Data Sharing Policy



Data Sharing

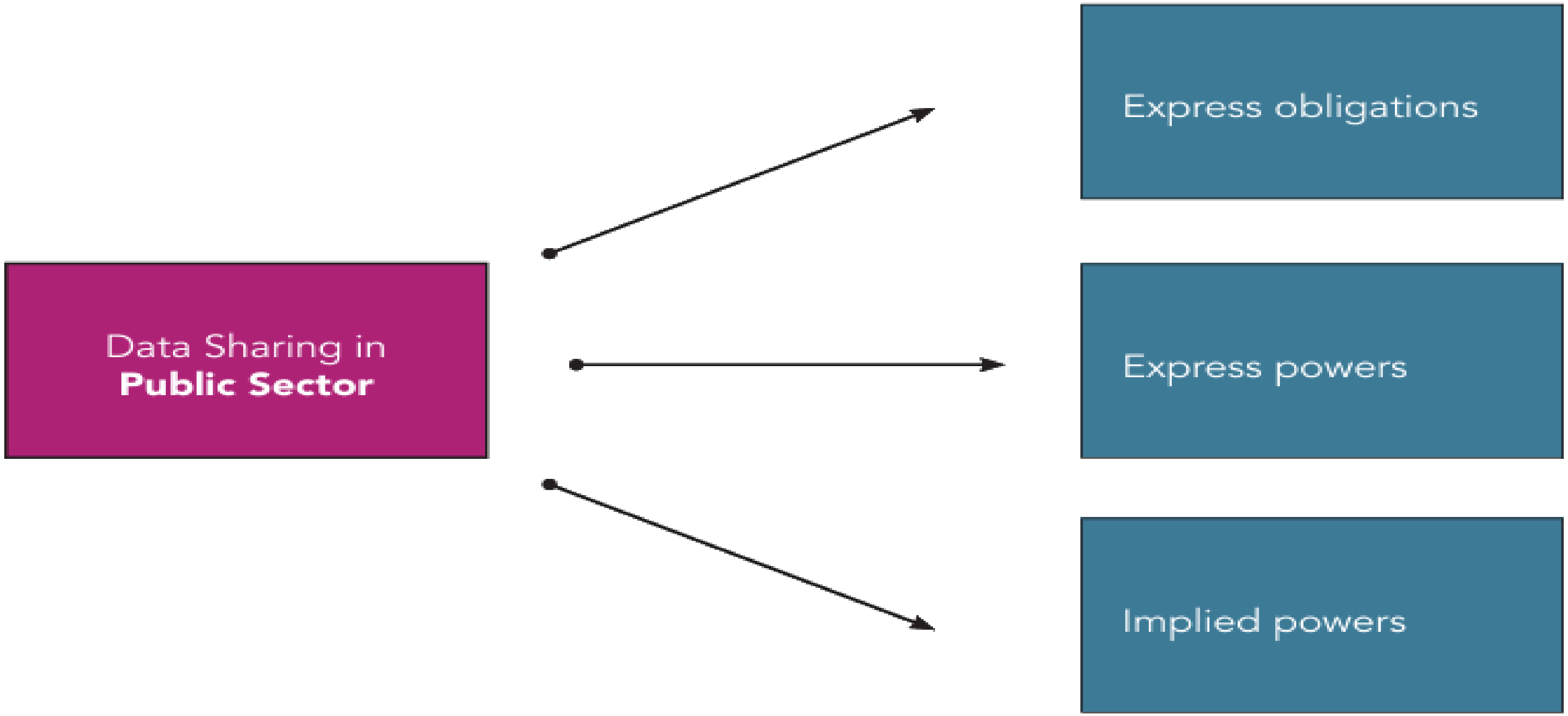
increases

- protection for individuals
- public confidence
- justified and beneficial data sharing
- a better understanding of implications

decreases

- risk of violating laws
- reputational risk caused by
  - irrelevant or
  - insecure sharing of personal data
- risk of questions, complaints and disputes

Data Sharing in Public Sector



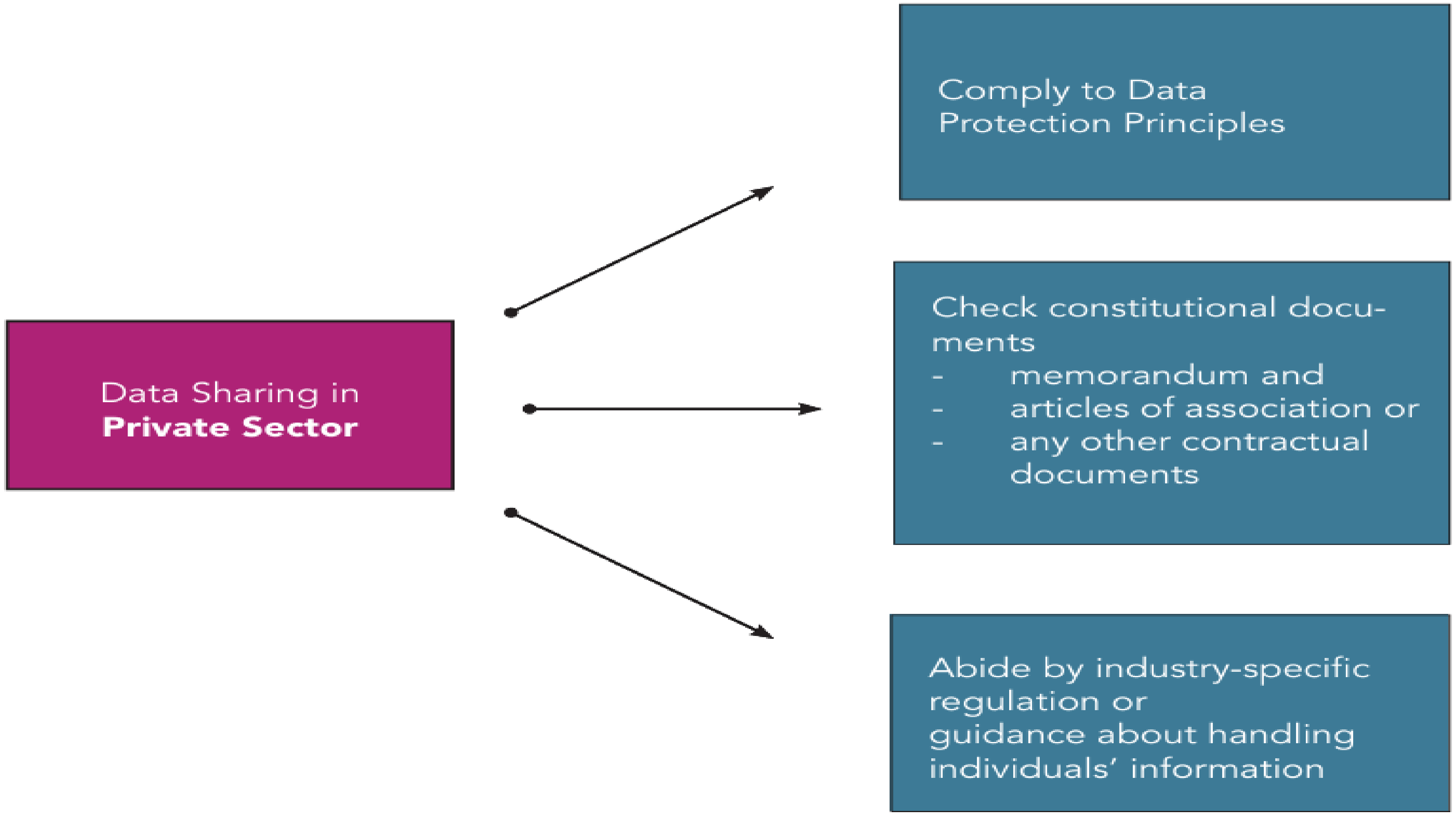
Data Sharing in **Public Sector**

Express obligations

Express powers

Implied powers

Private and Third Sector Organisations



Data Sharing in **Private Sector**

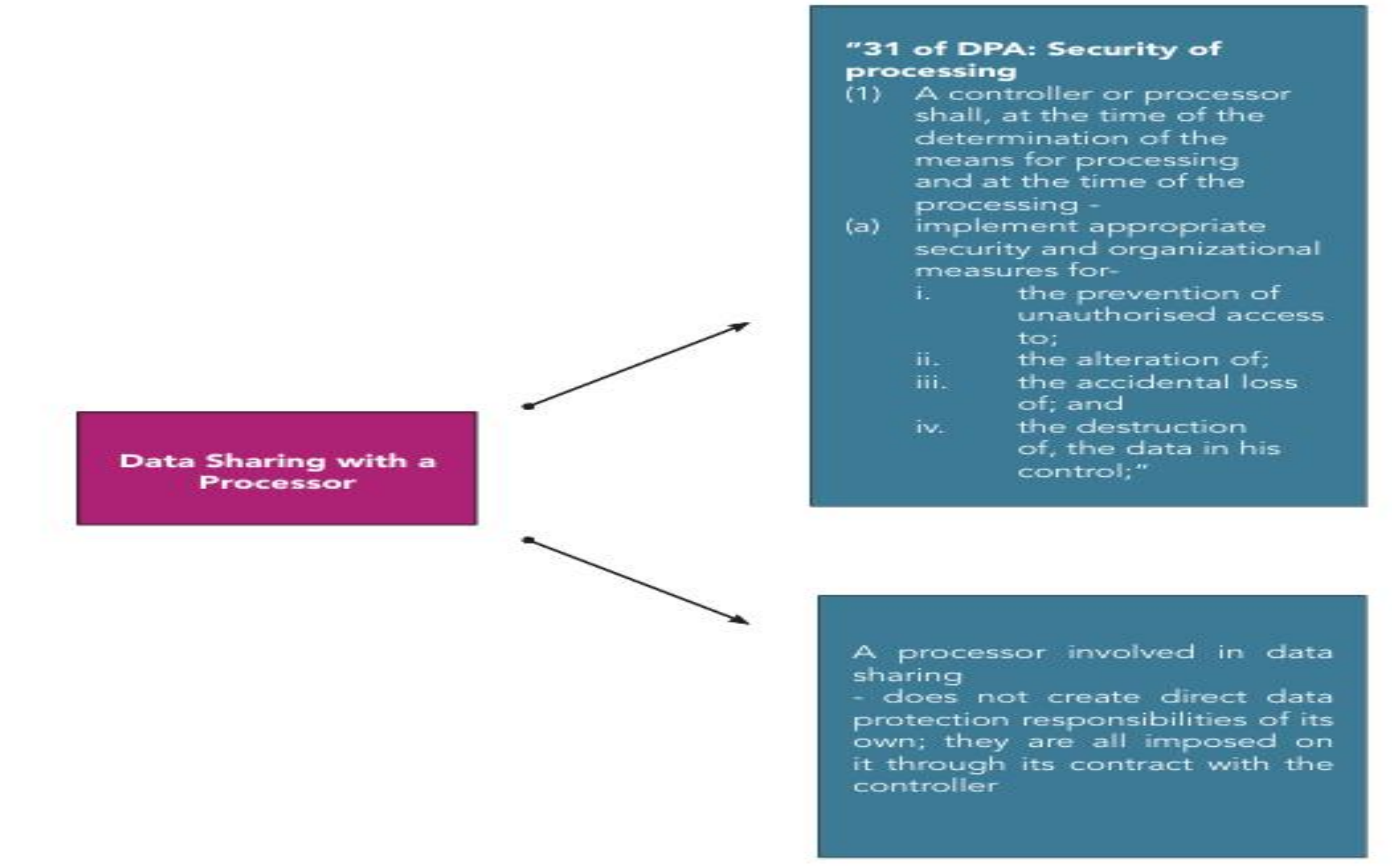
Comply to Data Protection Principles

Check constitutional documents

- memorandum and
- articles of association or
- any other contractual documents

Abide by industry-specific regulation or guidance about handling individuals' information

Sharing with a 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;

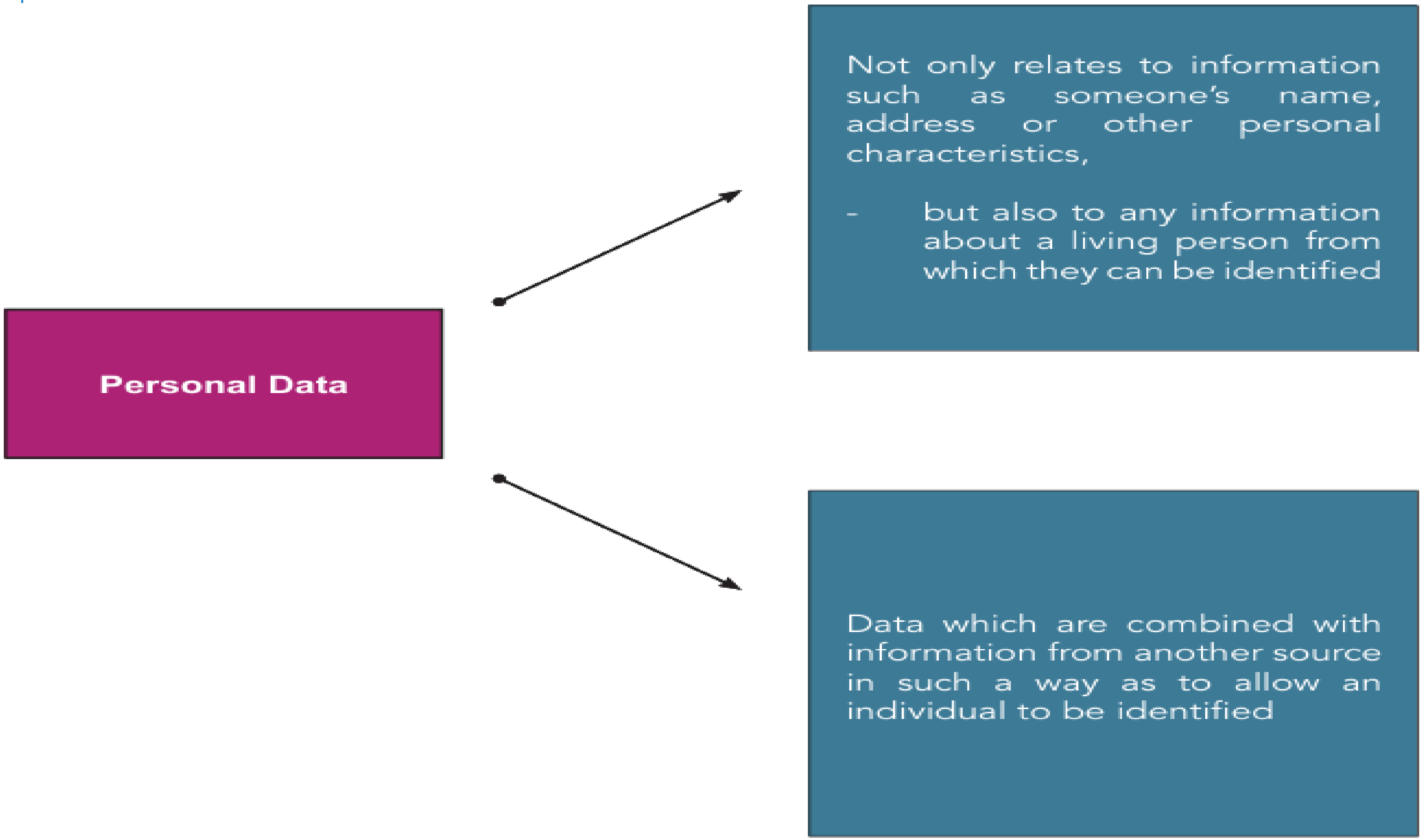
iii. the accidental loss of; and

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



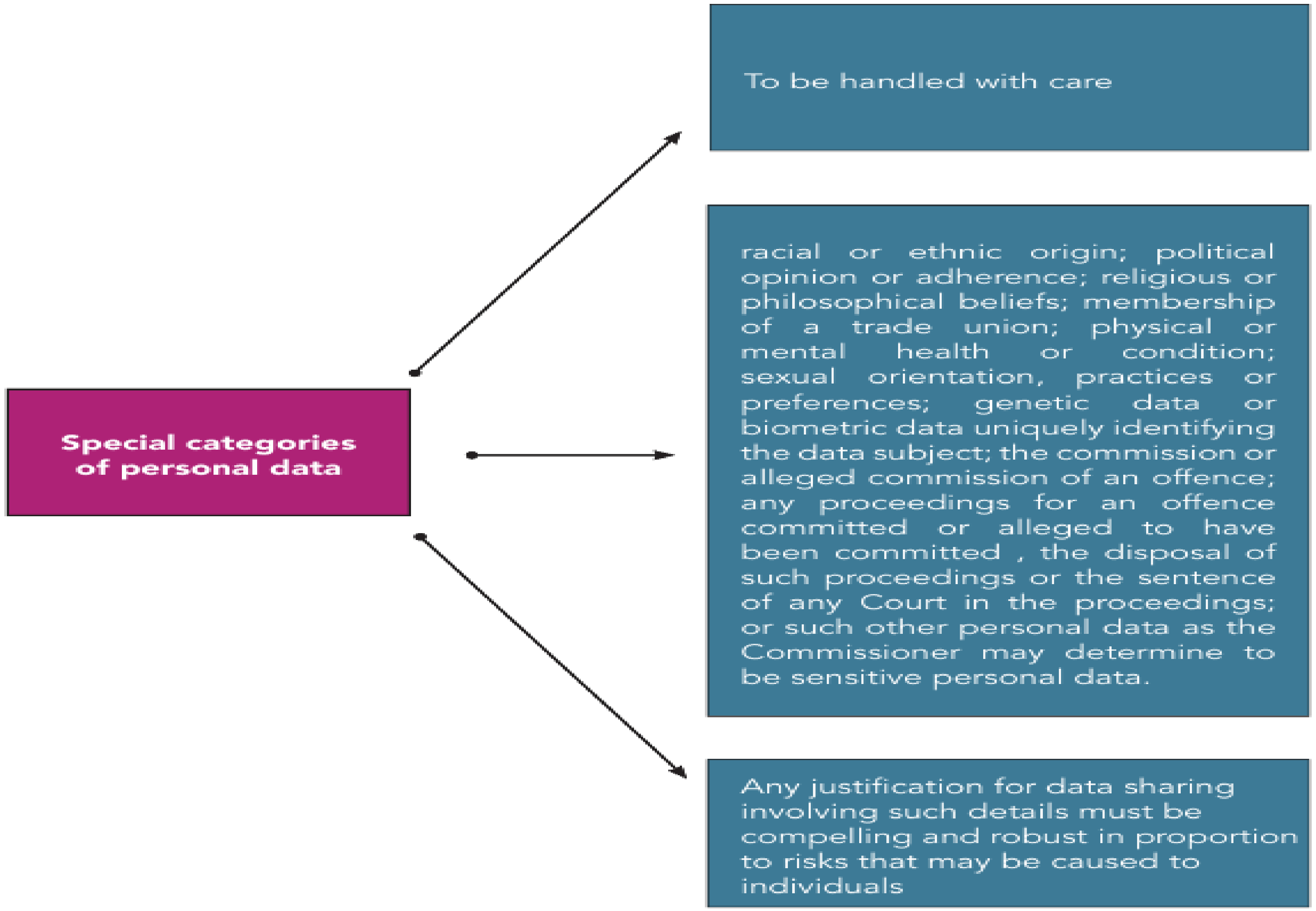
Personal Data

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

Data which are combined with information from another source in such a way as to allow an individual to be identified

Special Categories of Personal Data



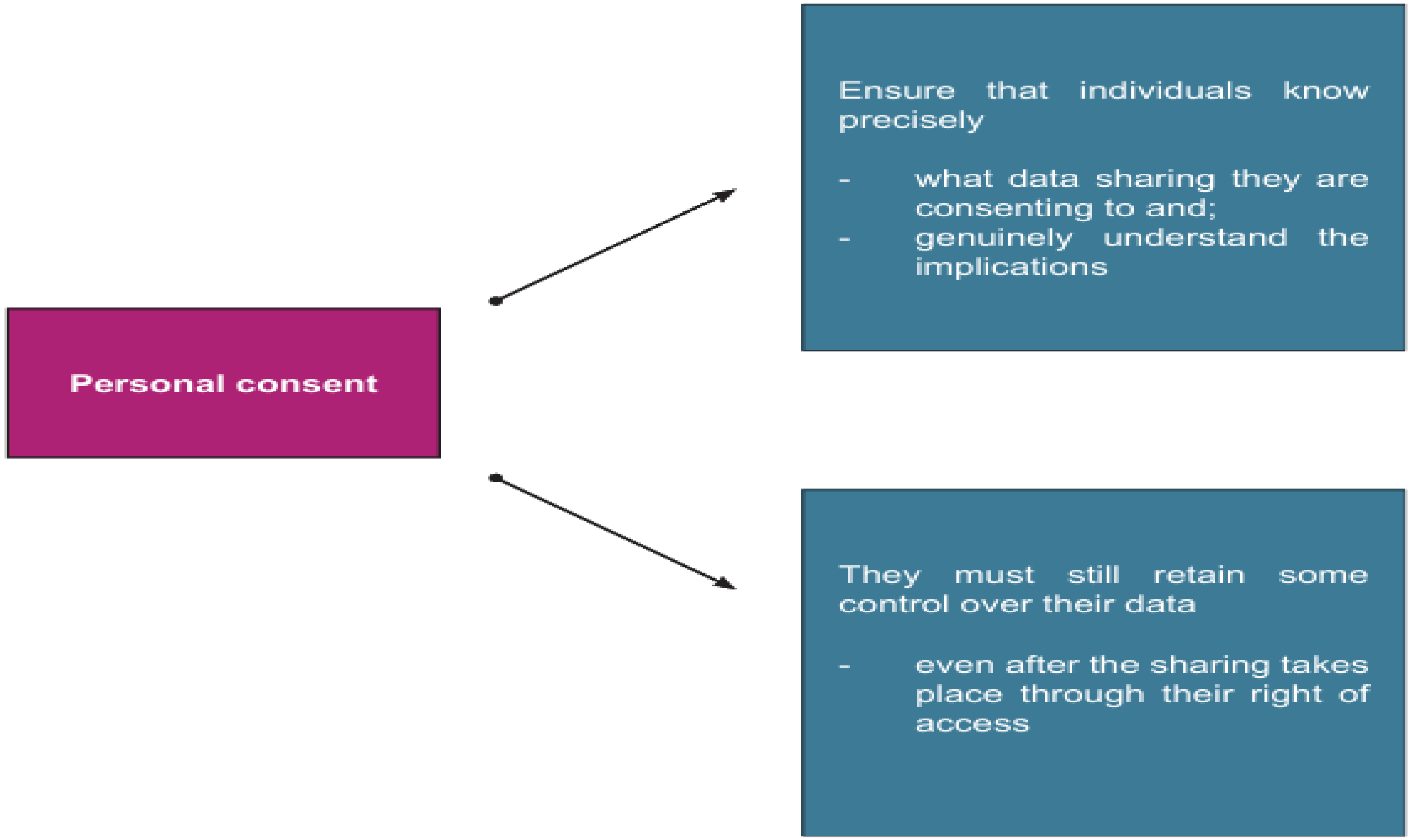
Special categories of personal data

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

Personal consent



Personal consent

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 DPA 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.

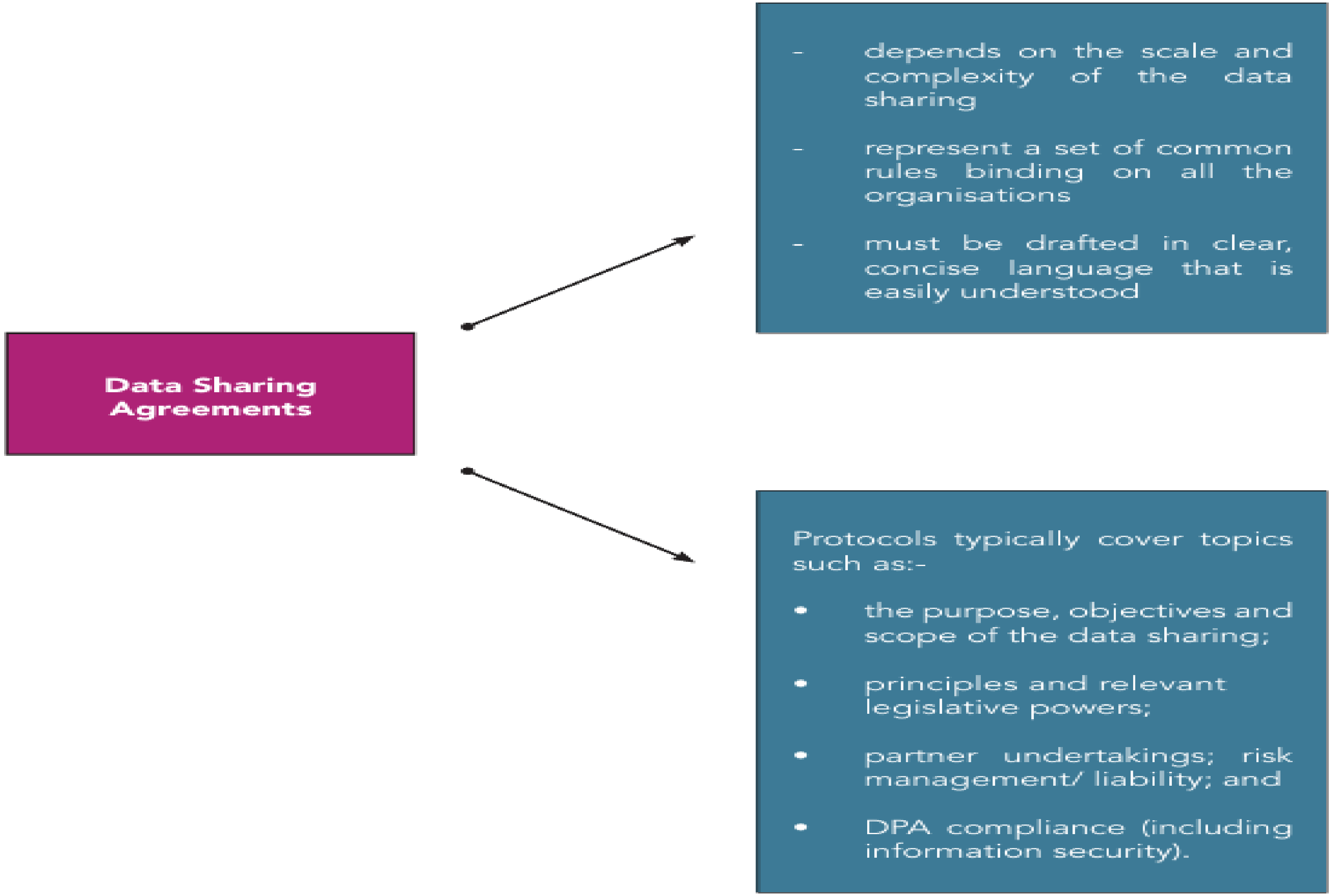
Legal Disclosures under the DPA

Section 44 of the DPA also provides for exemptions for disclosures of personal data as follows:

No exception to the DPA shall be allowed except where it constitutes a necessary and proportionate measure in a democratic society for –

- the protection of national security, defence or public security; or
- the prevention, investigation, detection or prosecution of an offence, including the execution of a penalty; or
- an objective of general public interest, including an economic or financial interest of the State; or
- the protection of judicial independence and judicial proceedings; or
- the protection of a data subject or the rights and freedoms of others;
- The processing of personal data for the purpose of historical, statistical or scientific research may be exempt from the provisions of the DPA 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

- depends on the scale and complexity of the data sharing
- represent a set of common rules binding on all the organisations
- must be drafted in clear, concise language that is easily understood

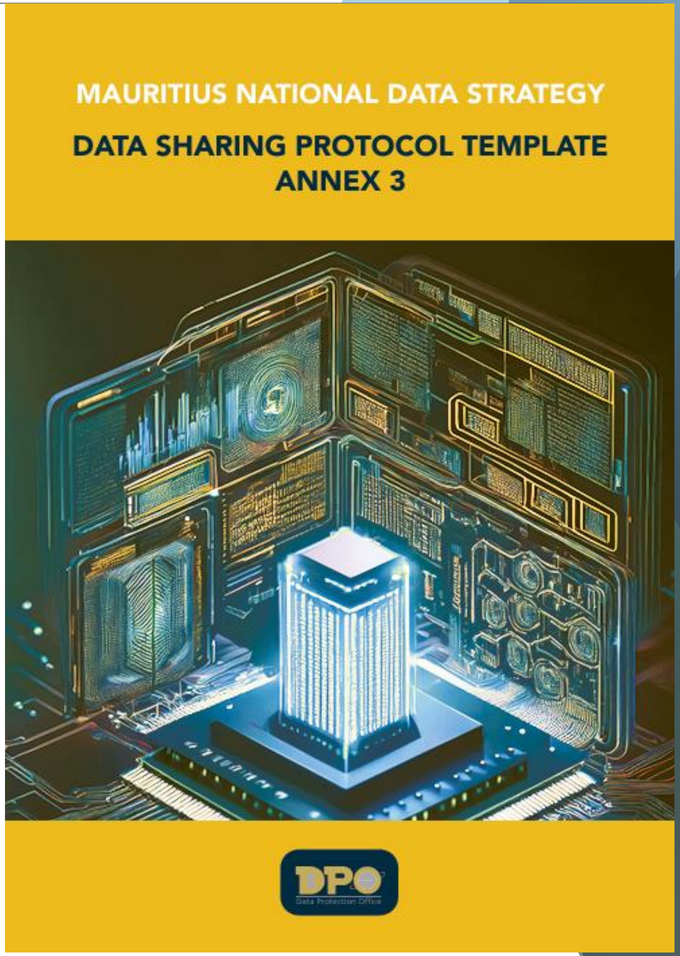
Protocols typically cover topics such as:-

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

DATA SHARING PROTOCOL TEMPLATE
Annex 3

It is designed to become an organisation’s: **internal data sharing protocol**

Annex 3 answers: “How is data sharing actually done, step by step?”



MAURITIUS NATIONAL DATA STRATEGY

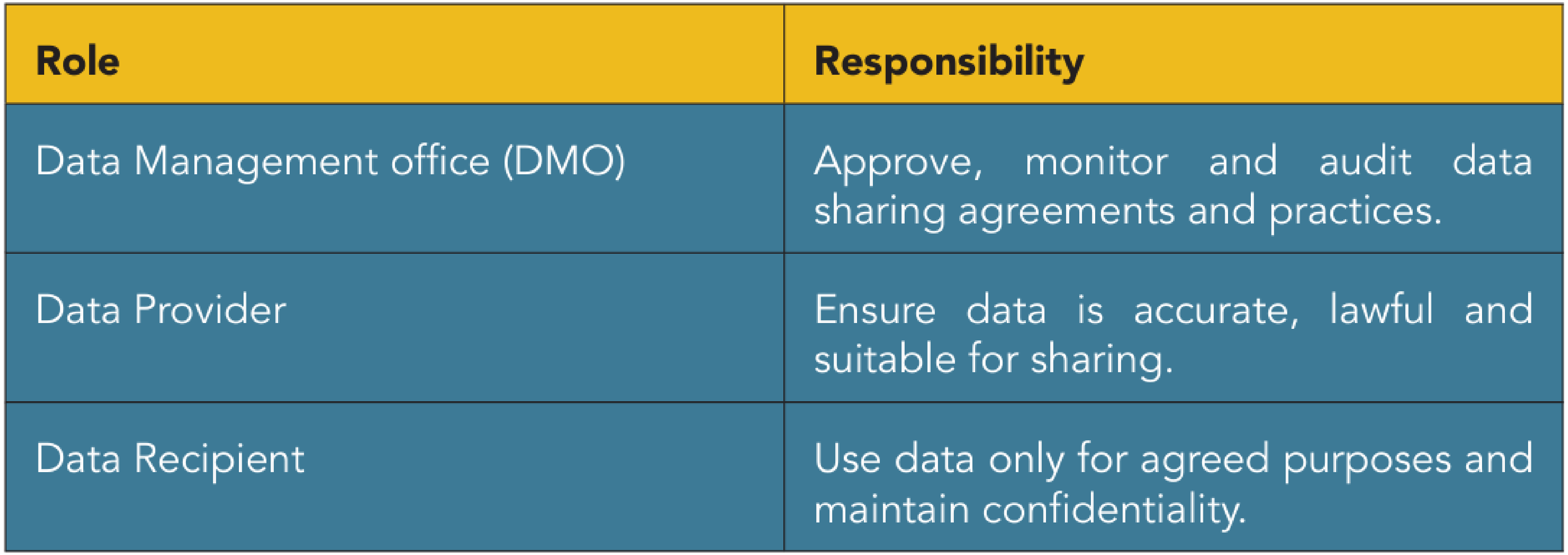
DATA SHARING PROTOCOL TEMPLATE
ANNEX 3

DPO
Data Protection Office

A full protocol template

- Scope and application
- Legal framework
- Principles for sharing
- Organisational responsibilities
- Consent and restrictions
- Liability and security
- Information quality
- Training obligations
- General principles
- Roles and responsibilities
- Formal data sharing request process
- Review and governance mechanisms

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.

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

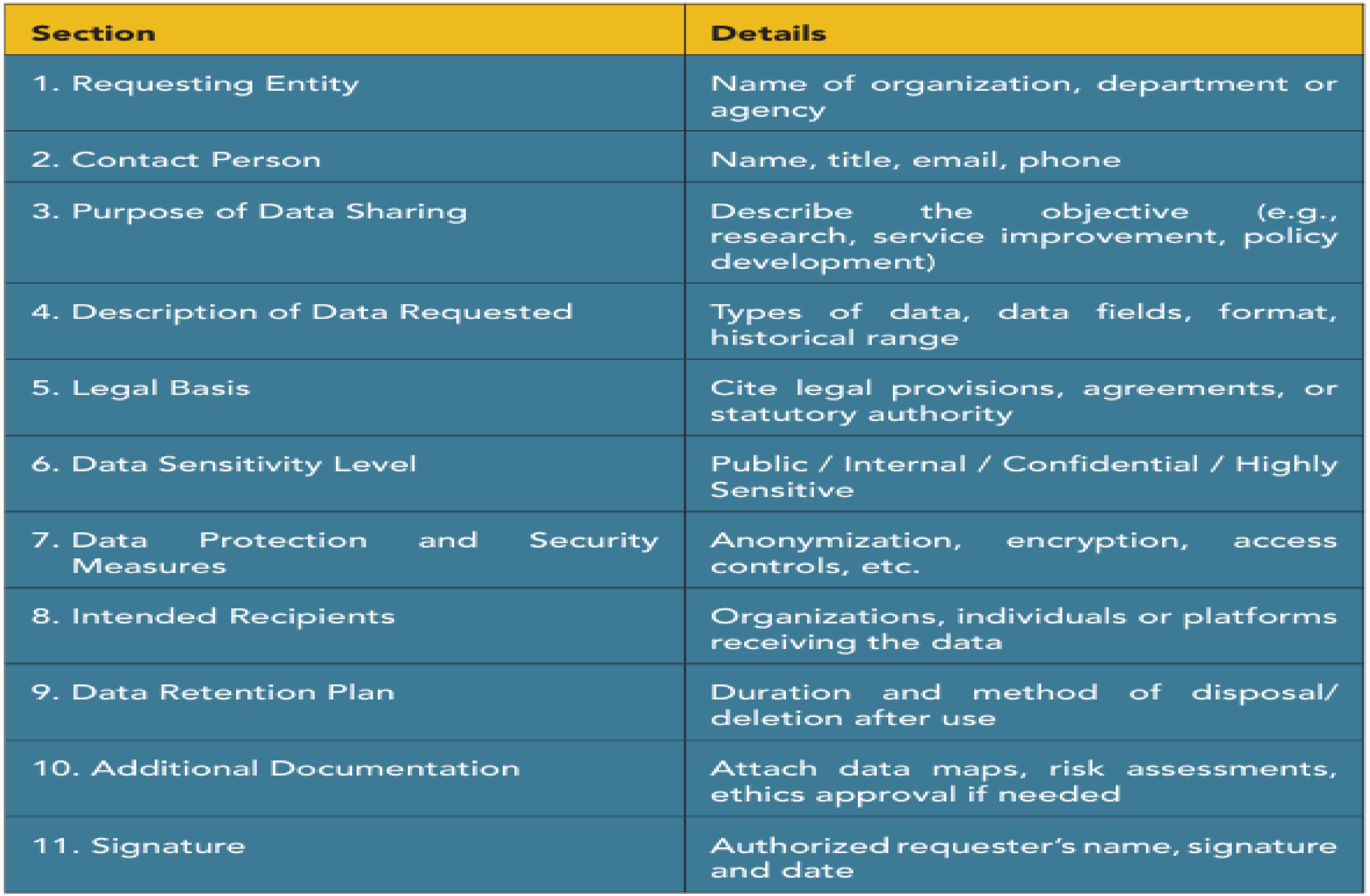
  Apply data standards, encryption and audit logs

- **Step 5: Monitoring & Review**

  Periodic reporting by DMO

  Review against performance indicators and compliance checks

Appendix A: Data Sharing Request Form

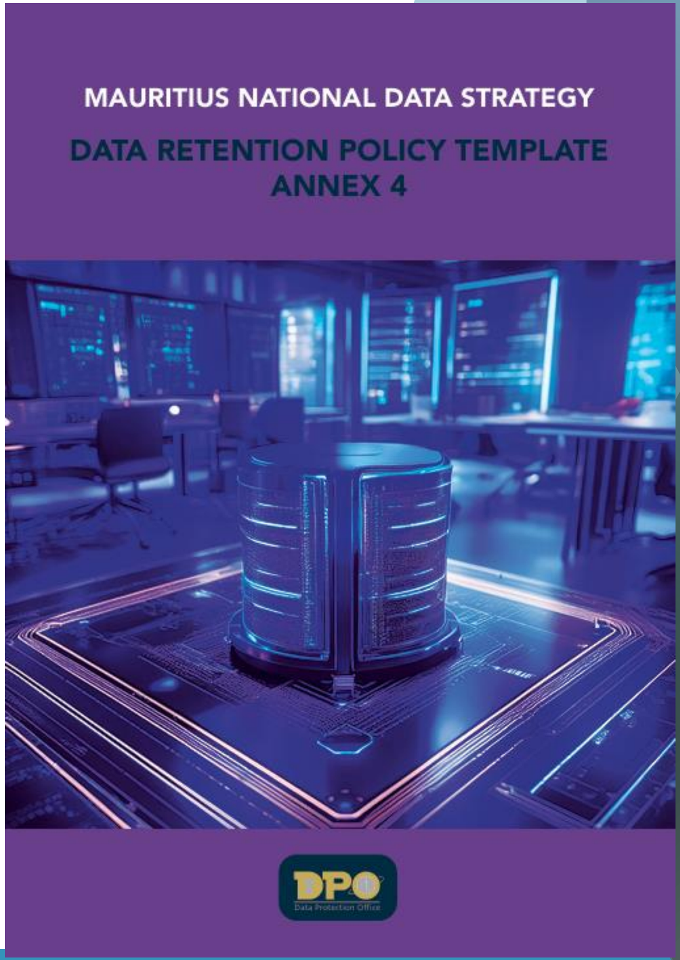


Section	Details
1. Requesting Entity	Name of organization, department or agency
2. Contact Person	Name, title, email, phone
3. Purpose of Data Sharing	Describe the objective (e.g., research, service improvement, policy development)
4. Description of Data Requested	Types of data, data fields, format, 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

DATA RETENTION POLICY TEMPLATE
Annex 4

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.



MAURITIUS NATIONAL DATA STRATEGY

DATA RETENTION POLICY TEMPLATE
ANNEX 4

DPO
Data Protection Office

DATA RETENTION POLICY TEMPLATE
Annex 4

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)

DATA RETENTION POLICY TEMPLATE
Annex 4

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)

DATA RETENTION POLICY TEMPLATE
Annex 4

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.

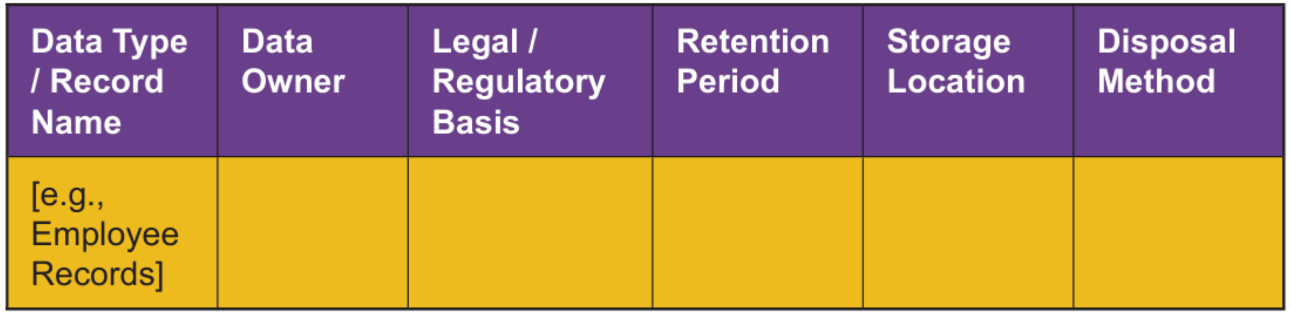
DATA RETENTION POLICY TEMPLATE
Annex 4

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]					

DATA RETENTION POLICY TEMPLATE
Annex 4

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.

DATA RETENTION POLICY TEMPLATE
Annex 4

7. Secure Data Disposal Procedures

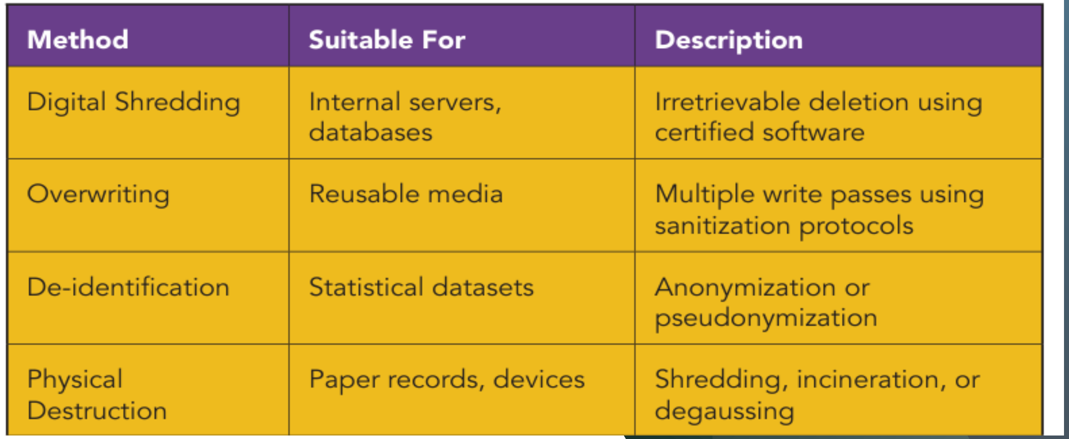
Data reaching the end of its retention period must be disposed of securely to prevent accidental leakage.

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:



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

DATA RETENTION POLICY TEMPLATE
Annex 4

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:

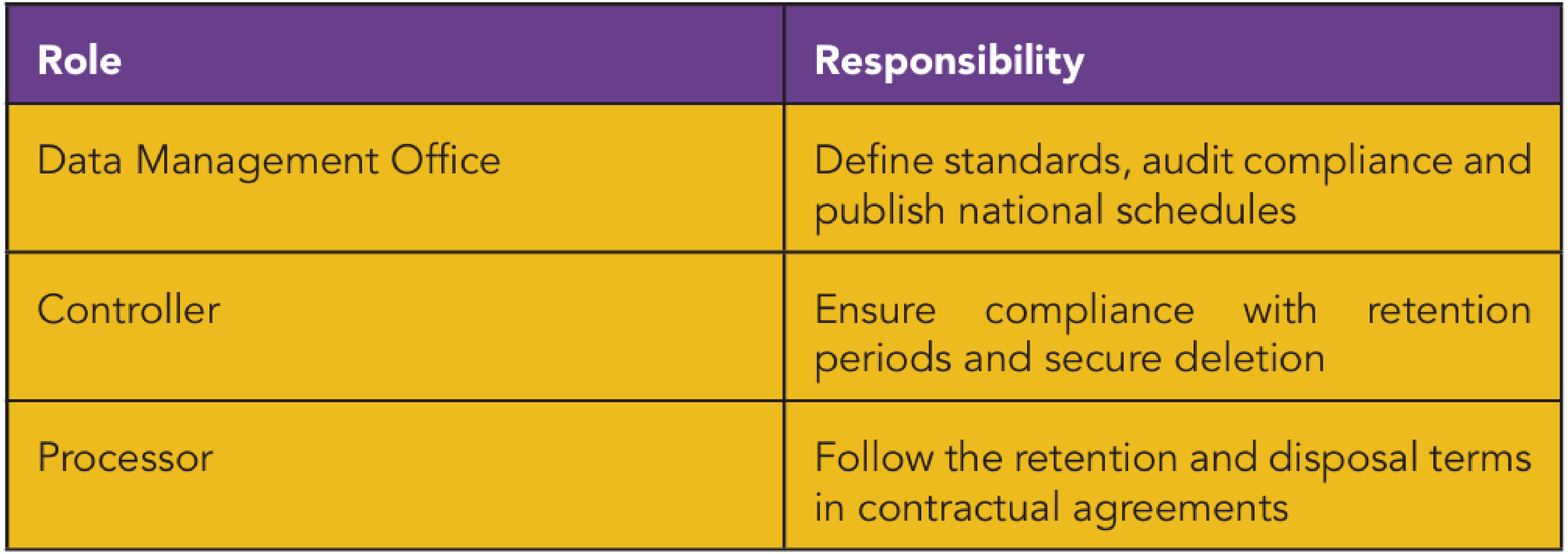
Disciplinary action against employees violating retention rules.

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.

DATA RETENTION POLICY TEMPLATE
Annex 4

10. ROLES AND RESPONSIBILITY



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

Thank
You