



DATA SHARING

- To understand what is Data Sharing
- To discuss Data Ethics of Data Sharing
- To examine the 'Trusted Data Sharing Framework'

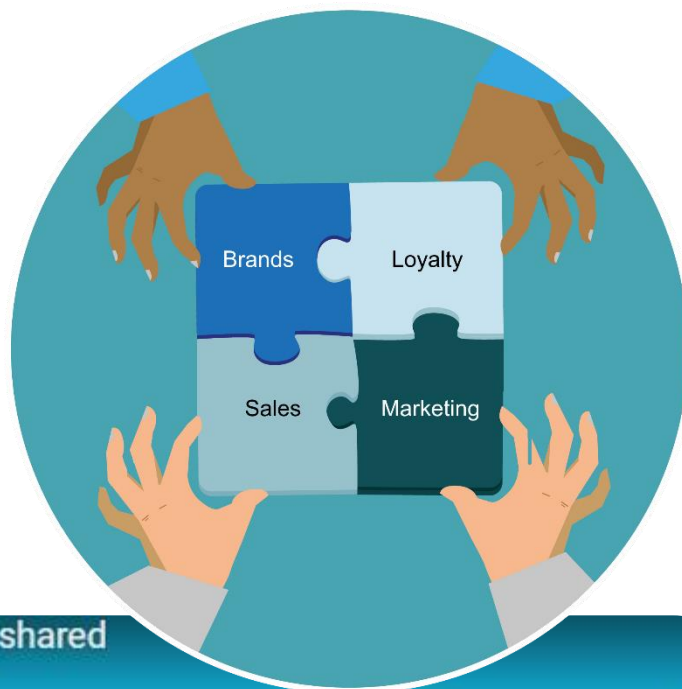
➤ **Value of Data Sharing**

- Ethics of Data Sharing
- Trusted Data Sharing Framework
- Considerations when implementing Data Sharing



Data Shared is Value Unlocked

Organisations breaking down data silos will know more about their customers' wants and needs, allowing them to offer better services and value, either by themselves or with participation of their commercial partners.



allowing your data to be shared



MINISTRY OF HEALTH SINGAPORE

Our Healthcare System | Policies and Issues | Costs and Financing | Diseases and Conditions | Medical Directory

Costs and Financing

Data Sharing

Ministry of Health > Costs and Financing > Data Sharing

You may be asked to provide consent for data sharing, on your next visit to an **Approved Healthcare Institution¹**, an **Intermediate and Long Term Care provider²**, or when you apply for the Community Health Assist Scheme (CHAS).

What is data sharing and how will it benefit me?

Data sharing enables the Ministry of Health (MOH) to facilitate the extension of government subsidies/assistance, Medisave and MediShield Life coverage when you or your family receive healthcare services.

MSF MINISTRY OF SOCIAL AND FAMILY DEVELOPMENT

HOME | ASSISTANCE | POLICIES | MEDIA ROOM | EVENTS | DIRECTORIES

Home > Policies > Social Service in Singapore > Data Management and Sharing

POLICIES

Data Management And Sharing

We will ask for your consent to manage and share your personal data across relevant organisations when you seek social services and assistance at the Social Service Offices (SSOs), the Family Service Centres (FSCs), the Divorce Support Specialist Agencies (DSSAs) and the Early Childhood Development Agency (ECDA).

What is data sharing and how will it benefit me?

By 'data sharing' we mean the disclosure of data between organisations or the sharing of data within an organisation – for example between the different departments of the Ministry of Social and Family Development (MSF).

Sharing your data with MSF allows us to facilitate the extension of social services and Government subsidies/assistance to you and your family.



Legislated Data Sharing

THE STRAITS TIMES

New law on data sharing among govt agencies

PUBLISHED JAN 9, 2018, 5:00 AM SGT

Public sector officers who share personal info without authorisation face fines, jail sentence

Joanna Seow Manpower Correspondent

Public sector officers who share the personal data of Singaporeans without authorisation can now be fined up to \$5,000, jailed for up to two years, or both.

The same applies to those who make use of data to benefit themselves or their organisations by sharing or disclosing data without authorisation.

The criminal penalties are among new rules to formalise the data-sharing rules for public sector agencies.

The Public Sector (Governance) Bill, passed by Parliament yesterday, also makes public sector officers requesting data, not just those that own it, are now responsible for protecting it.

1. to uphold and promote the values of the Singapore public sector;
2. to secure economies or efficiencies for the Singapore public sector;
3. to improve (directly or indirectly) the efficiency or effectiveness of policies, programme management or service planning and delivery by Singapore public sector agencies (whether by carrying out data analytics work or otherwise);
4. to ensure business continuity;
5. to ensure accountable and prudent stewardship of Singapore public sector finances and resources;
6. to manage risks to the financial position of the Government;
7. to support a whole-of-government approach in the discharge of the Singapore public sector agencies' functions.

The Bill lists seven specific purposes under which data can be shared between public sector agencies

Data.gov.sg

Search Singapore's Public Data

View All Datasets

Topics

1,482 datasets found

Sort by: Relevance

Economy

Education

Environment

Finance

Health

Infrastructure

Society

Technology

Transport

File format

Select one

Agency

Select one

Registered Vessels and Shipping Tonnage, Monthly

Maritime and Port Authority of Singapore / 20 Aug 2018

Dataset shows the monthly total number of registered vessels and shipping tonnage as at end of the period. (Latest month figures are preliminary estimates.)

CSV

Container Throughput, Monthly

Maritime and Port Authority of Singapore / 20 Aug 2018

Dataset shows the monthly container throughput in twenty-foot equivalent units. (Latest month figures are preliminary estimates.)

CSV

Tanker Arrivals (>75 GT), Monthly

Maritime and Port Authority of Singapore / 20 Aug 2018

Dataset shows the monthly number of tanker arrivals (>75 GT) and shipping tonnage by type. Only vessels that are more than 75 Gross Tonnes are included. (Latest month figures are preliminary estimates.)

CSV

Vessel Arrivals (>75 GT), Monthly

Maritime and Port Authority of Singapore / 20 Aug 2018

Dataset shows the monthly number of vessel arrivals (>75 GT) and shipping tonnage by type. Only vessels that are more than 75 Gross Tonnes are included. (Latest month figures are preliminary estimates.)

CSV

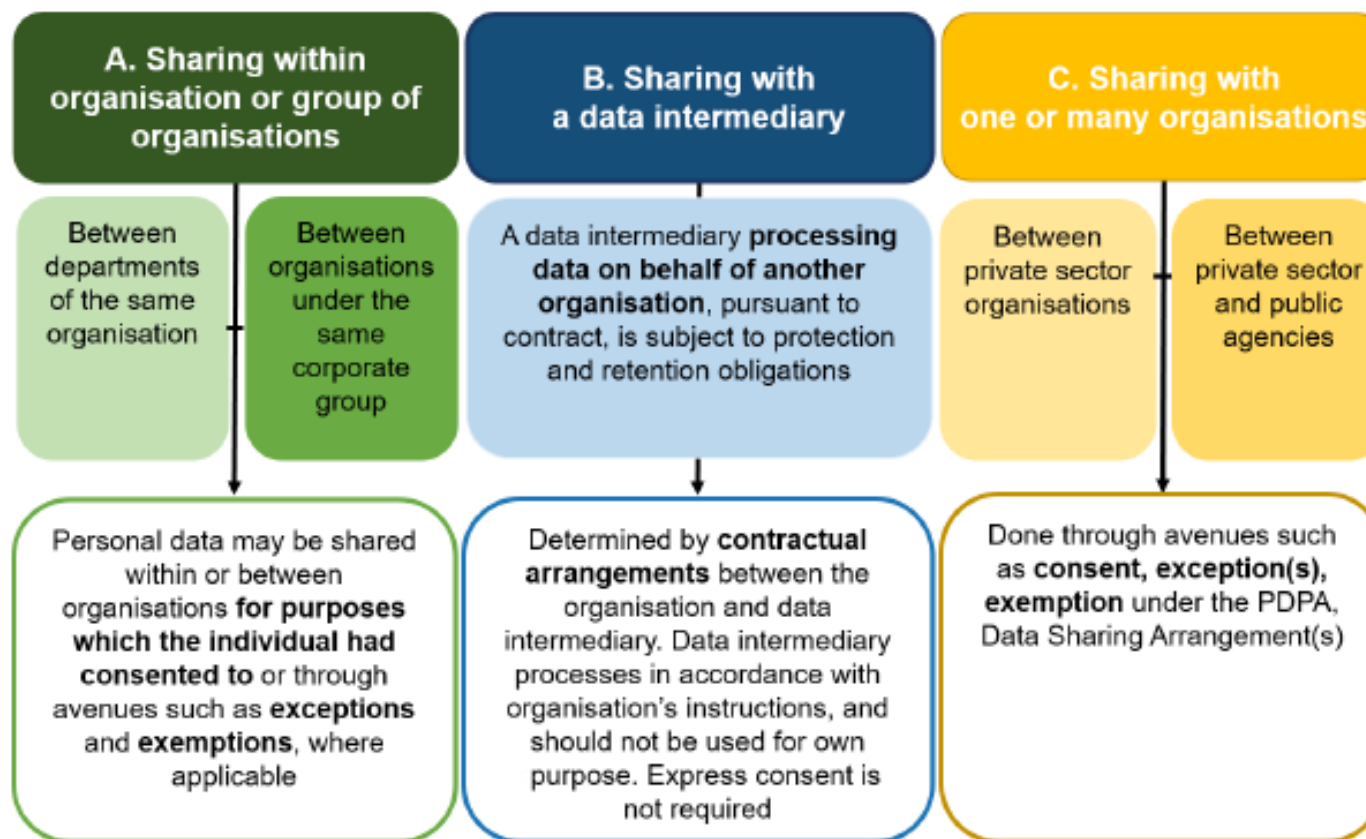
- Value of Data Sharing
- **Ethics of Data Sharing**
- Trusted Data Sharing Framework
- Considerations when implementing Data Sharing



Be Compliant

‘Data sharing’ refers to the use and/or disclosure of personal data to one or more organisation(s) and the latter’s collection of that personal data.

– *Personal Data Protection Commission*



Source: PDPC

“Ethics are principles of behaviour based on ideas of right and wrong”

– Laura Sebastian-Coleman

Ethical principles often focus on ideas such as:

- Fairness
- Respect
- Responsibility
- Integrity
- Justice
- Quality
- Reliability
- Transparency
- Trust

Data ethics are concerned with how to:

- Procure
- Store
- Use
- Dispose

of data in ways that are aligned with ethical principles.

They are concerned with doing the right things with data and prevent wrong things from being done with data, *even when no one is looking.*



Importance of Data Ethics

The ethics of data handling relate to the following core concepts:

- **Impact on people:** data often represents characteristics and behaviours of individuals. It is used to make decisions that affect people's lives. It is used to influence how people make decisions. Ethics demands that data should be used only in ways that preserve human dignity.
- **Potential for misuse:** misusing data can negatively affect people and organisations. Ethics demands preventing misuse of data, especially actions that harm the greater good.
- **Economic value of data:** data has economic value. Ethics demands that data owners determine how that value can be accessed and by whom.



The accepted tenets of bioethics, which focus on preserving human dignity, provide a good starting point:

- **Respect for persons:** the fundamental ethical requirement that people be treated in a way that respects their dignity and autonomy.
- **Beneficence:** first, do no harm; second, maximise possible benefits and minimise possible harm.
- **Justice:** fair and equitable treatment of people.

Questions that can be asked when applying these principles: Are people being treated unequally under similar circumstances? Does a certain outcome disproportionately benefit or harm a certain group of people? Is AI being trained to inadvertently reinforce cultural prejudices?



Data Ethics and Competitive Advantage

There are strong business reasons to handle data ethically:

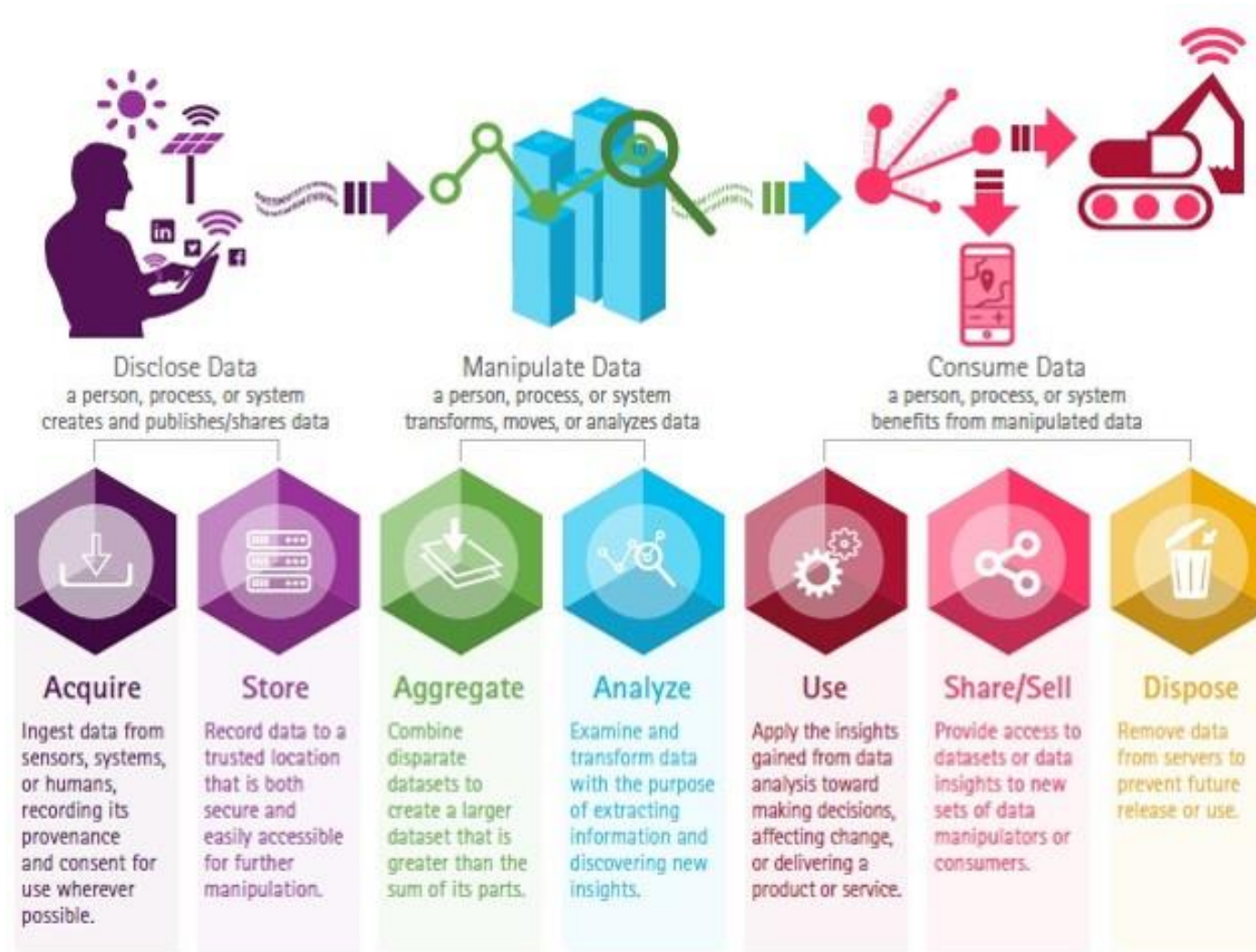
- **Stakeholder expectations:** customers and other stakeholders expect ethical behaviour and outcomes from organisations and their data processes
- **Managing risk:** reducing the risk that data will be misused by employees, customers or partners is a prime reason to cultivate data ethics
- **Preventing misuse:** there is an ethical responsibility for organisations to secure data in its care, e.g., hacking; data breaches; etc.
- **Respecting ownership:** organisations need to make ethical decisions about sharing data that does not belong to them



Beyond Personal Data

- **Research Data** – organisations share data with research organisations where experiments are conducted using anonymised and aggregated samples of datasets and other sources of data to analyse social trends.
- **Prizes and challenges** – organisations make data available to qualified applicants who compete to develop new apps or discover innovative uses for the data.
- **Trusted intermediaries** – organisations share data with a limited number of known partners for data analysis and modeling, as well as other value chain activities.
- **Application programming interfaces (APIs)** – organisations give developers access to streams of data for testing, product development and data analytics.
- **Intelligence products** – organisations share (often aggregated) data that provides general insight into market conditions, customer demographic information, or other broad trends.
- **Corporate Data cooperatives or pooling** – organisations and government agencies group together to create “collaborative databases” with shared data resources.

Data Value Chain



Source: Accenture



Data Sharing Considerations



Acquire Store



Aggregate Analyze



Use



Share/Sell



Dispose

Sample
external questions

Are data disclosers aware that they have disclosed data? Can they inspect it? Are they aware of how they disclosed this data (e.g. directly, tracking, derived)? Has intent for how the data will be used been communicated?

What are the classes of harm that a bad actor or group of actors could cause if they had access to the entire set of aggregated data sources or any related analysis?

Did the data discloser provide consent to this specific data use? Did any consent agreement make it clear that data could be used in this way?

Do data disclosers expect control, ownership, remuneration, or transparency over the data they have disclosed if it is being shared or sold? Did they provide informed consent for this action?

Are stakeholders aware of the time frame that their data will be retained? Would they be surprised to learn it still exists?

Sample
internal questions

What methods were used to collect the data? Do collection methods align with best practices? Did data disclosers provide informed consent? What are the security risks with how the data is stored?

What biases have been introduced during manipulation? Was an ethics review performed?

Are the uses of the data consistent with the intentions of the discloser? What are the potential risks to the organization if a watchdog group knew the data was used in this way?

Does the act of sharing or selling data enhance the experience for the data discloser (not including the data seller's own ability to operate)? Is there another way to share or sell this data that would increase transparency?

Should the original discloser be notified? Is metadata being retained? Are there any disaster recovery archives that have copies of the data?

Adapted: Accenture

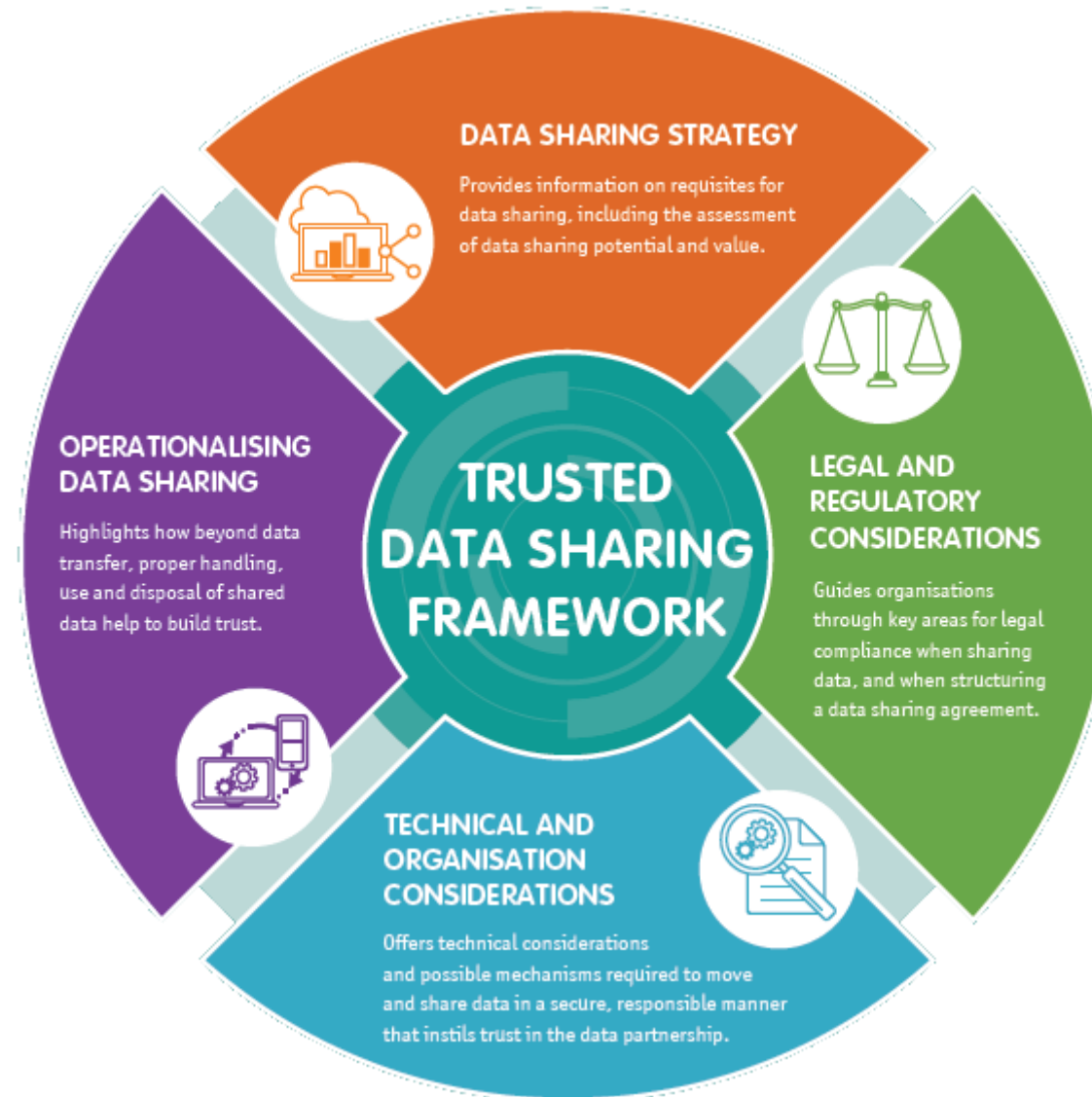
- Value of Data Sharing
- Ethics of Data Sharing
- **Trusted Data Sharing Framework**
- Considerations when implementing Data Sharing

DATA SHARING

FOR ORGANISATIONS

Businesses have recognised that pooling data together, or getting access to external sources of data, can generate greater value. This can be achieved through trusted data sharing partnerships.

The IMDA's Trusted Data Sharing Framework can help you kick-start your organisation's data sharing journey through guidance on 4 key areas.



Source: SG:D, IMDA, PDPC

Data Sharing Ecosystem

- An institution or organisation empowered to operate a supervisory function related to the ecosystem
- May refer to the regulator (or other governing bodies), or industry bodies with oversight mandates or other practical influence (e.g., industry associations, standards institutes)
- Usually not directly involved in data sharing, but can influence the data sharing activities through legislative reviews, issuance of the guidelines, standards or accreditation schemes

Authority

Data Provider

- Creators, licensees or sellers of data



Data Consumer

- Recipients collecting or buying external data for their purposes, such as to generate additional insights and supplement internal functions

Data Service Providers

- Organisations providing data services supporting the data sharing ecosystem
- Services can include, but not limited to, the following:
 - 1) Providing technical means (e.g., platform) to facilitate data exchange
 - 2) Data preparation, data management and technical/risk/governance advisory
 - 3) Acquiring data from providers (may include processing to enhance its value) and supplying data to Data Consumers or marketplaces

Data Sharing Ecosystem

- An institution or organisation empowered to operate a supervisory function related to the ecosystem
- May refer to the regulator (or other governing bodies), or industry bodies with oversight mandates or other practical influence (e.g., industry associations, standards institutes)
- Usually not directly involved in data sharing, but can influence the data sharing activities through legislative reviews, issuance of the guidelines, standards or accreditation schemes

Authority

Data Provider

- Creators, licensees or sellers of data



Data Consumer

- Recipients collecting or buying external data for their purposes, such as to generate additional insights and supplement internal functions

Data Service Providers

- Organisations providing data services supporting the data sharing ecosystem
- Services can include, but not limited to, the following:
 - 1) Providing technical means (e.g., platform) to facilitate data exchange
 - 2) Data preparation, data management and technical/risk/governance advisory
 - 3) Acquiring data from providers (may include processing to enhance its value) and supplying data to Data Consumers or marketplaces

Trusted Data Sharing Framework

PART 1: Data Sharing Strategy

1. Establish Data Sharing Potential and Value of Own Data
2. Understand Potential Data Sharing Methods
3. Consider Engaging Data Service Provider to Facilitate Data Sharing

PART 2: Legal and Regulatory Considerations

1. Determine if Data Can Be Shared
2. Establish Data Sharing Agreement

PART 3: Technical and Organisation Considerations

1. Prepare Data for Data Sharing
2. Understand technical Considerations for Data Sharing

PART 4: Operationalising Data Sharing

1. Ensure Transparency and Accountability
2. Monitor Ongoing Legal and Regulatory Obligations
3. Use of Data for Secondary Purpose
4. Understand Considerations for Retention and Disposal of Data

The Framework is organised into four parts which are not sequential. Organisations may choose to use them in any sequence, depending on their needs, but should not omit any part.

Data Sharing Strategy

PART 1: Data Sharing Strategy

1. Establish Data Sharing Potential and Value of Own Data
2. Understand Potential Data Sharing Methods
3. Consider Engaging Data Service Provider to Facilitate Data Sharing

Purpose

Organisations will identify what data can be shared, how this data can be valued, and the various arrangements or models that can be used for the sharing the data

Stakeholders

- All key decision makers, stakeholders and internal units/users involved in the data sharing process

Establish Data Sharing Potential

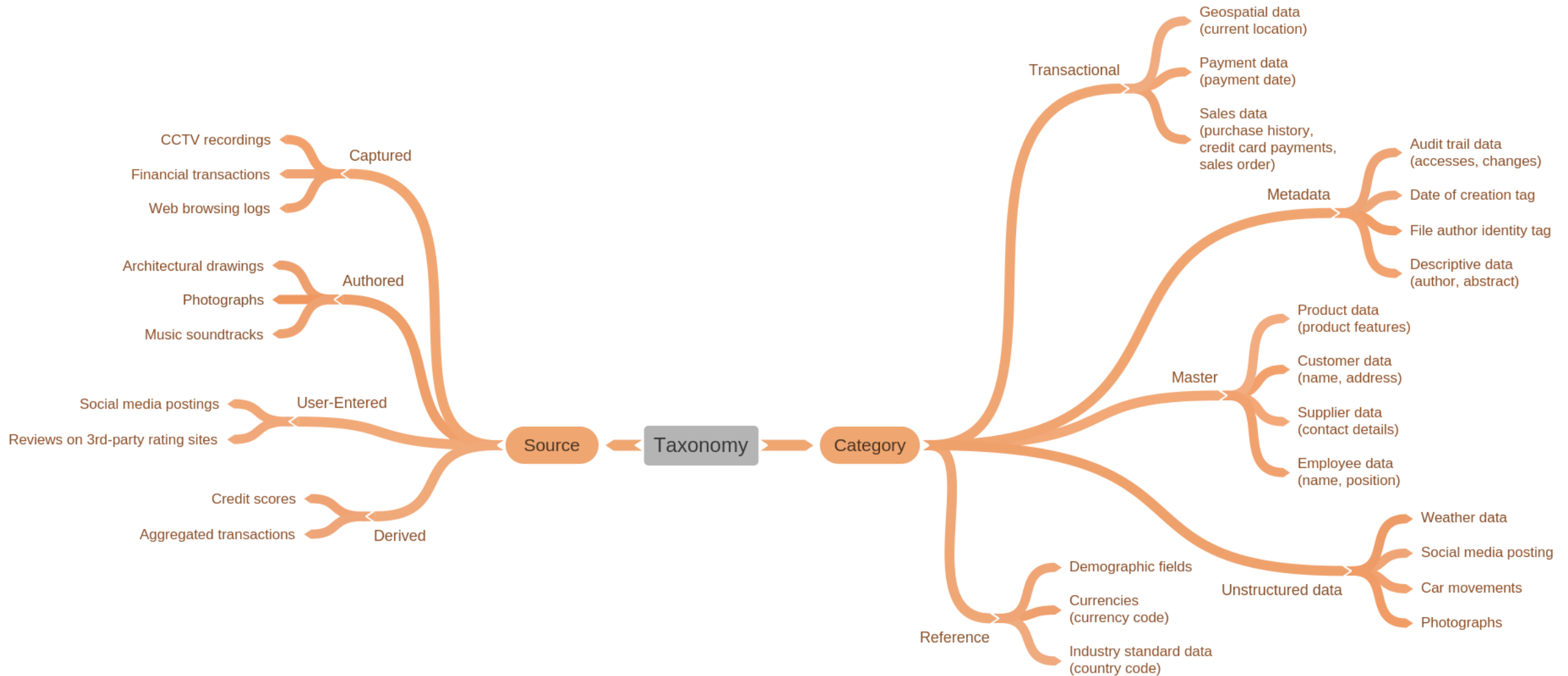
PART 1: Data Sharing Strategy

1. Establish Data Sharing Potential and Value of Own Data

Data is an intangible resource that can be used simultaneously across multiple business initiatives. Its value is dependent on the capability and capacity of the organisation to harness its use. Organisations can assess the value of data by following the key steps of:

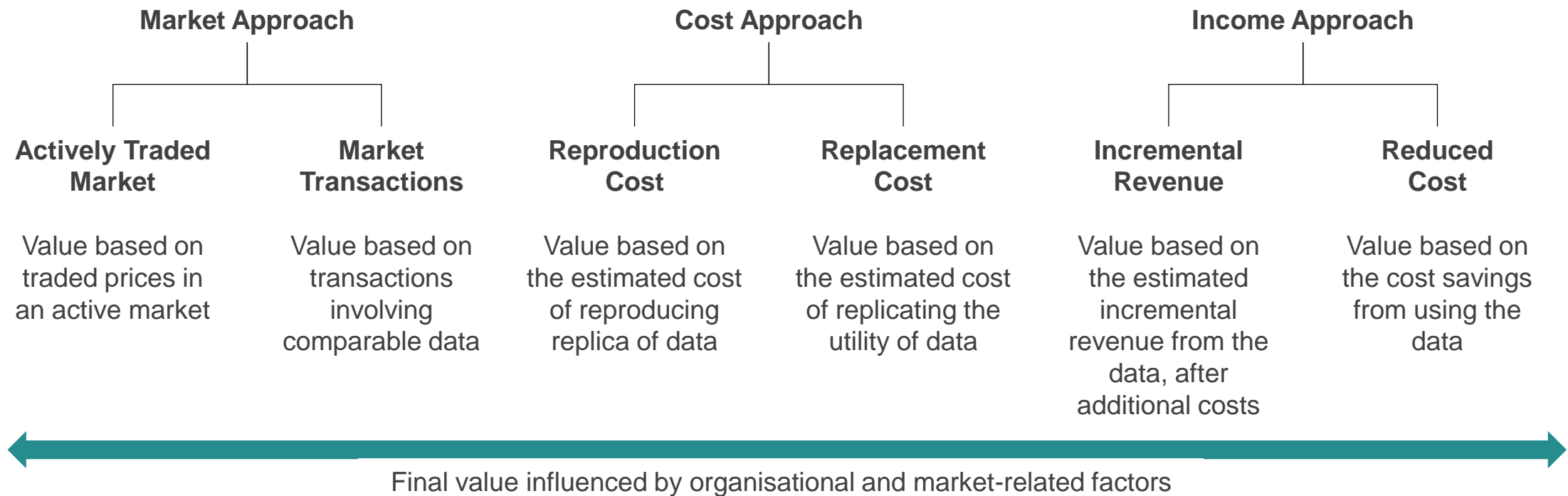
- A** Take Stock of Own Data
 - a** Identifiable and definable – may be made up of specific files or specific tables or records within a database
 - b** Promise future economic benefits – to have value, data must have a useful application. Identify productive uses for data in order to assign value to it
 - c** Under the organisation's control – the organisation must have the rights to use the data consistent with its rights, whilst also protecting the data and restricting access to it by others
- B** Assess Potential for Sharing – organisations may be approached by others to use their data, or vice versa; potential use cases could be generated from new insights derived by combining data with stakeholders across the value chain, beyond the immediate key suppliers and consumers
- C** Consider Data Valuation Approaches – data sharing partners may have differing assessments of the value of the data to be shared. Organisations may consider using common data valuation methods as yardsticks to establish agreed value with data sharing partners

What Sort of Data



Data Valuation Approaches

Market Approach	Cost Approach	Income Approach
What is the value of a similar data asset on the market?	What is the minimum value to cover costs and generate margin?	What incremental value can the data consumer generate with the data asset?
If market value for identical or similar data is available	If the data can be reproduced or replaced	If the net cash flow benefits of the data can be reasonably quantified

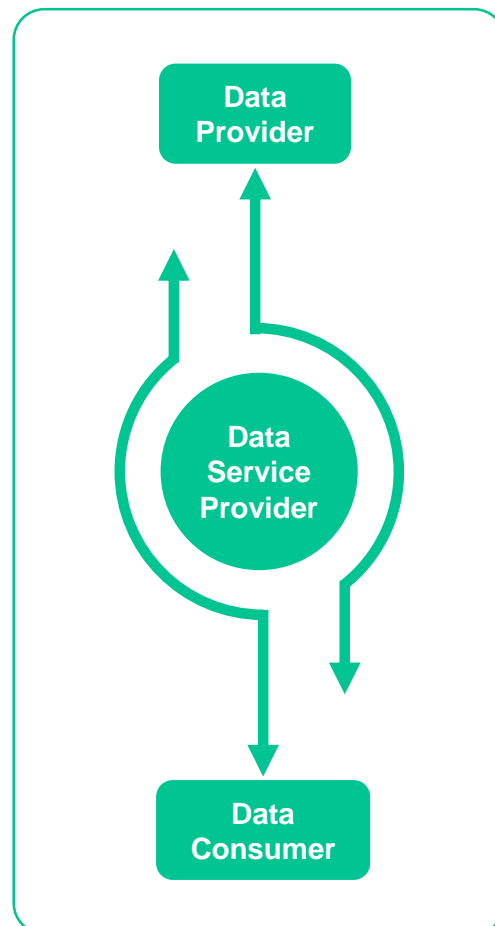


Understand Potential Data Sharing Methods

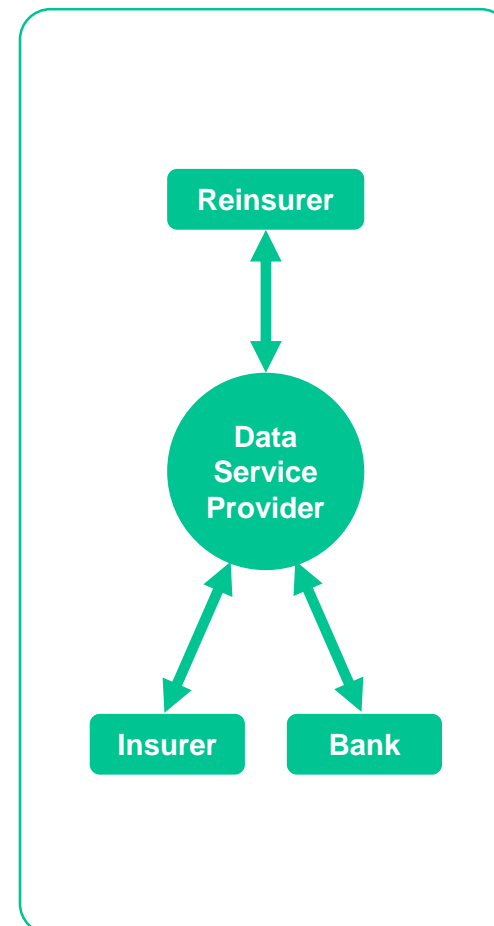
PART 1: Data Sharing Strategy

2. Understand Potential Data Sharing Methods

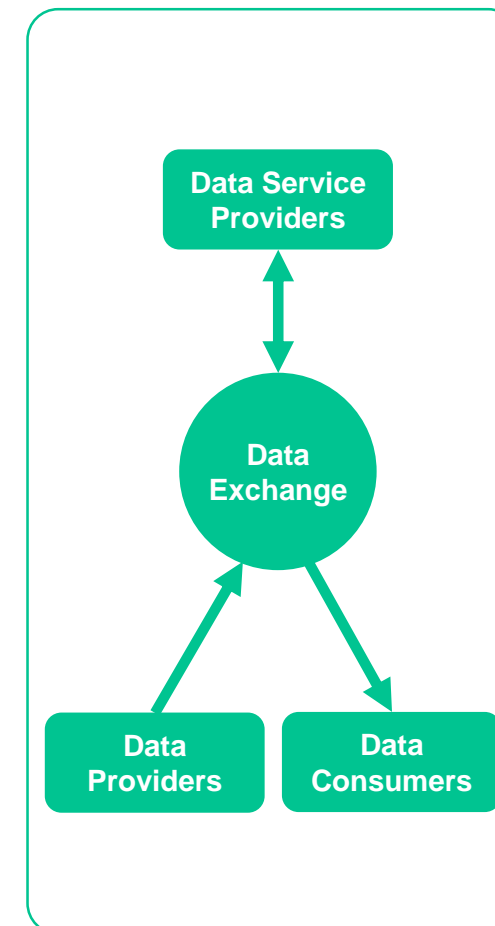
Bilateral



Multilateral



Decentralised



Consider Data Service Provider

PART 1: Data Sharing Strategy

3. Consider Engaging Data Service Provider to Facilitate Data Sharing

Data Service Providers can perform multiple data services such as data preparation, data analytics and data sharing (e.g., match Data Providers with Data Consumers, standardise data sharing agreements or place risk control mechanisms on their platforms)

When data sharing is facilitated by Data Service Providers in both multilateral model or in decentralised model, there is greater complexity; it is important for organisations to perform additional due diligence:

- a** Find out more about Data Service Providers' internal data policies and best practices (e.g., are they certified under IMDA's Data Protection Trustmark) and their track records
- b** Assess likelihood of platform-related issues (consider track record and solvency of data exchange operators as well as the technology used) and the potential costs that might be incurred if such were to happen; balance this against the expected value of participation on such a platform
- c** Check if Data Service Providers offer services that mitigate risks associated with sharing of data with a wider audience (e.g., data matching services which allow data cross-referencing between multiple participants to identify shared customers without providing access to the underlying data and/or conveying any personal data)

Legal and Regulatory Considerations

PART 2: Legal and Regulatory Considerations

1. Determine if Data Can Be Shared
2. Establish Data Sharing Agreement

Purpose

Organisations will need to ensure that the data can be shared in a legally compliant manner, as well as structure a data sharing agreement for the data sharing partnership. This should be done with an idea of the potential use case, data partners and potential data for sharing

Stakeholders

- Users in charge of driving projects
- Business units who collect, manage and use data
- Advisory teams on legal/risk and compliance matters

Consider if Data Can Be Shared

PART 2: Legal and Regulatory Considerations

1. Determine if Data Can Be Shared

- A** Consider Rules and Restrictions on Data
 - a Laws and regulations
 - b Guidelines – for certain regulated sectors, guidelines are mandatory
 - c Legal agreements
 - d Rights to share data – intellectual property rights allow Data Providers to share data for the intended purpose
- B** Data Protection Policies and Practices – they can help to engender trust by establishing that parties involved have similar data management, data protection and data standards
- C** Considerations for Sharing Personal Data

Establish Data Sharing Agreement

PART 2: Legal and Regulatory Considerations

2. Establish Data Sharing Agreement

The agreement sets out important terms that should be agreed between organisations:

- A** Grant of the licence/permission to use the data for the intended purpose(s) – the licence may include ownership of derivative data (in copyright law terms, ‘derivative work’ is copyrightable ‘work’ based on one or more pre-existing ‘works’). An example may be a dataset generated through analysis or compilation of other datasets. Where a Data Consumer can generate derivative data from data provided by a Data Provider, the licence may provide for the Data Consumer to obtain some share of ownership in the derivative work
- B** Restrictions to the permitted use of the data (e.g., territorial or time limitations, exclusivity or commercialization rights)
- C** Warranties or other assurances provided in relation to the Data Provider’s rights in the data
- D** Allocation of liability for contractual breaches and other liabilities between the parties, as well as indemnification and other remedies when breaches occur
- E** Confidentiality
- F** Term/duration of the agreement
- G** Governing law and resolving disputes – common disputes between Data Providers and Data Consumers relate to payment or breach of licence/other agreed terms. Parties should agree on simple escalation procedures to ensure that within each organisation, a dispute receives sufficiently senior attention at the appropriate time and that parties have processes in place to respond to issues quickly to limit losses. Similarly, parties should agree on how to resolve disputes where amicable resolution is not achieved after appropriate escalation

Operationalising Data Sharing

PART 4: Operationalising Data Sharing

1. Ensure Transparency and Accountability
2. Monitor Ongoing Legal and Regulatory Obligations
3. Use of Data for Secondary Purpose
4. Understand Considerations for Retention and Disposal of Data

Purpose

Organisations can choose to proceed to share data after all legal and technical modalities have been negotiated and agreed upon, or use this section to think through how they want to share data

Stakeholders

- Users in charge of driving projects
- Advisory teams on legal/technical/ risk and compliance matters

Ensure Transparency and Accountability

PART 4: Operationalising Data Sharing

1. Ensure Transparency and Accountability

During the data sharing process, organisations should seek to be transparent on how the shared data would be used. For example, both Data Provider and Data Consumer should have access to how data was processed and/or manipulated to meet the agreed objectives.

As data sharing and analysis is an iterative process, data sharing partners should refer to the Data Sharing Agreement that was established should ambiguities arise. As best practice, organisations can prepare audit logs (related to access management, monitoring and risk management) and provenance records to demonstrate accountability and transparency in the data sharing partnership. This helps organisations to be assured that the data shared has been managed in the agreed form.

Monitor Ongoing Obligations

PART 4: Operationalising Data Sharing

2. Monitor Ongoing Legal and Regulatory Obligations

As best practice, for these received data, organisations should continuously monitor for any changes that may arise on legal and regulatory obligation and the organisation should take all necessary measures to ensure they remain compliant to the revised legal and regulatory obligations (e.g., the PDPA for secondary use of personal data). Organisations should also monitor the access and use by staff to ensure that they abide by the scope as laid out in the Data Sharing Agreement or any other applicable governance policies and rules

Use for Secondary Purpose

PART 4: Operationalising Data Sharing

3. Use of Data for Secondary Purpose

Once organisations in a partnership have achieved the objectives that they set out on in the Data Sharing Agreement, they can choose to use the data received for secondary purpose (if agreed on) or retain/dispose of the data accordingly. The organisation may use the data received for secondary purposes, based on the agreed terms of use, governance structure, rules and restrictions between the data sharing partners. However, if the organisation intends to use the shared data for purposes that had not been stated upfront in the Data Sharing Agreement or beyond the restrictions on use that was agreed on, it should then engage its data sharing partners and negotiate or request for the new use of data

Considered Retention and Disposal

PART 4: Operationalising Data Sharing

For business data, organisations should retain or dispose of the data received according to the policies and procedures as agreed with the data sharing partners and/or Data Service Providers. If these were not set out in the Data Sharing Agreement, organisations should follow policies and procedures based on the applicable laws and/or internal data management policies based on classification of the received data.

For personal data, organisations should note that as soon as it is reasonable to assume that there is no longer any legal or business purpose, organisations are required to cease retention of the personal data and to dispose of these data accordingly.

Refer to PDPC's 'Guide to Disposal of Personal Data on Physical Medium' and 'How Can Your organisation Dispose of Personal Data' for details

4. Understand Considerations for Retention and Disposal of Data

Agenda

- Value of Data Sharing
- Ethics of Data Sharing
- Trusted Data Sharing Framework
- **Considerations when implementing Data Sharing**



Data Sharing Responsibilities

- Equip those responsible for data sharing with knowledge of relevant laws and regulations
- Provide understanding of available treatment of data prior to sharing, e.g.,
 - [Anonymisation](#), Aggregation & Masking
 - [Standards](#)
 - Quality
- Provide access only to relevant data





Data Sharing Agreement

Establish Data Sharing Agreement

- Purpose, or purposes, of the sharing
- Potential recipients or types of recipients
- Access control
- Data to be shared
- Data quality
- Data security
- Data retention/deletion
- Procedures for dealing with access, queries and complaints
- Review of effectiveness/termination of agreement

1. **Collaboration and mutual accountability between partners** – data may reflect the ‘basis’ on which they are collected and require collaborative interpretation
2. **Every dataset is possibly unique** – every agreement should likewise reflect the uniqueness
3. **Less is best** – the more data shared, the increased risk exposure, especially where privacy is concerned
4. **Pay special attention to re-purposed data** – data collected for one purpose when combined with other data may allow it to be used for less innocuous purpose
5. **Emphasise process, openness and trust** – especially when principles and regulations are unclear; a clearly understandable agreement is vastly able to establish a network of trust between the users, partners and public



Document the decision of each data sharing request

- Date of request
- Date of decision
- Reason(s) for sharing/not sharing the data
- Effective date of data sharing
- Decision authority
- Other relevant information



Activity Roadmap





Summary

- **Data sharing across and between organisations promotes re-use and has the potential to create value**
- **Responsible data sharing should benefit all stakeholders**
- **A clear data sharing policy is essential to facilitate data sharing**
- **Training is essential for staff who are likely to make significant decisions about data sharing or have access to shared data**

THANK YOU

nicholas_tan@nus.edu.sg