



TRUSTED DATA SHARING FRAMEWORK

SG:D
EMPOWERING POSSIBILITIES

IM INFOCOMM
MEDIA
DEVELOPMENT
AUTHORITY

pdpc PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

CONTENTS



PURPOSE OF TRUSTED DATA SHARING FRAMEWORK	5
INTRODUCTION	6
TRUSTED DATA SHARING FRAMEWORK	10
Key Considerations in Data Sharing	11
Key Roles in Data Sharing	13
Trust Principles	15
PART 1: DATA SHARING STRATEGY	17
1.1 Establish Data Sharing Potential and Value of Own Data	18
1.2 Understand Potential Data Sharing Models	24
1.3 Consider Engaging Data Service Provider to Facilitate Data Sharing	26
PART 2: LEGAL AND REGULATORY CONSIDERATIONS	27
2.1 Determine if Data Can Be Shared	28
2.2 Establish Data Sharing Agreement	37
PART 3: TECHNICAL AND ORGANISATION CONSIDERATIONS	39
3.1 Prepare Data for Data Sharing	40
3.2 Understand Technical Considerations for Data Sharing	41
PART 4: OPERATIONALISING DATA SHARING	49
4.1 Ensure Transparency and Accountability	50
4.2 Monitor Ongoing Legal and Regulatory Obligations	50
4.3 Use of Data for Secondary Purpose	51
4.4 Understand Considerations for Retention and Disposal of Data	51

CONTENTS

APPENDICES	52
DATA SHARING STRATEGY	53
APPENDIX I : Application of Trust Principles	54
APPENDIX II : Data Sharing Models – Example Scenarios & Case Studies	59
LEGAL AND REGULATORY CONSIDERATIONS	62
APPENDIX III : Restrictions and Rules on Data Sharing	63
APPENDIX IV : Useful Sources of Worldwide Data Rules and Guidance	65
APPENDIX V : Considerations for Data Sharing Agreement	66
SHARING PERSONAL DATA	67
APPENDIX VI : Consent, Dynamic and Iterative Consent	68
APPENDIX VII : Exemption under the PDPA	73
TECHNICAL AND ORGANISATION CONSIDERATIONS	76
APPENDIX VIII : Technical Delivery Mode for Data Sharing	77
APPENDIX IX: Security Measures to Protect Data Integrity	82
OTHERS	86
APPENDIX X : Data Sharing Checklist – Questions to Consider	87
APPENDIX XI : Common Resources Used in This Framework	89
ACKNOWLEDGEMENT	90

PURPOSE OF TRUSTED DATA SHARING FRAMEWORK

Data sharing is a multi-disciplinary process which involves not only enabling technology, but also business and legal considerations. Concerns over trust and security hinder the mass sharing of data, despite the benefits that can be gained from leveraging large volumes and variety of data for analytics, including machine learning artificial intelligence. Based on industry feedback, the data sharing ecosystem is still in a nascent stage and guidance is still very much required to help organisations, including professional data service providers, overcome the concerns of data sharing. It is with this purpose of providing guidance to the industry that this Trusted Data Sharing Framework ("**Framework**") is developed. This Framework aims to guide organisations through the data sharing journey and outline key considerations for organisations to take into account when planning data partnerships. Users of this Framework will be able to:

- a** appreciate the benefits of data sharing;
- b** gain clarity from the information and illustrations presented in this Framework;
- c** understand key areas of considerations to enable data sharing; and
- d** kick-start their data sharing journeys or possibly develop their own ideas around data sharing.

This Framework is presented from the perspectives of data providers or data consumers who are interested or have decided to embark on data sharing journeys. Data service providers may also find this Framework useful in understanding the considerations of data providers or consumers.

For the purpose of this Framework, "data" refers to both personal and business data. This Framework is intended for use in the commercial and non-governmental sectors but excludes data sharing in or with the public sector. Users should note that personal data requires additional safeguards, and that they can find information and references to specific guides or tools throughout this document.

For avoidance of doubt, this Framework is just a guide for industry and not for compliance. The content should not be read as nor constitute as legal advice, nor construed as a tool for compliance to the Personal Data Protection Act 2012 ("**PDPA**") or any law and regulations. Users of this Framework should assess the need to seek legal advice before finalising any legal agreements.

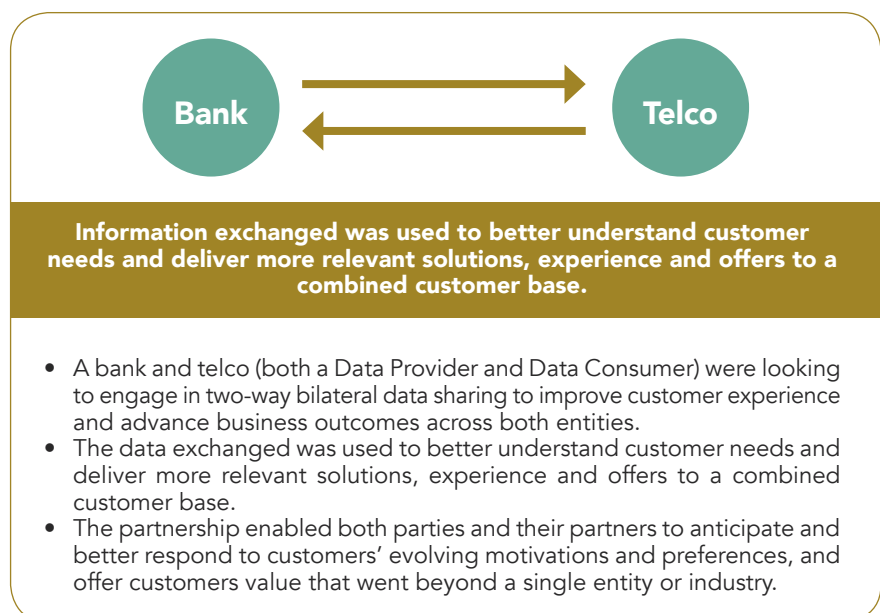


INTRODUCTION

The digital transformation of the global economy is taking place at an unprecedented speed and scale. By 2022, 60% of global GDP will be digitised,¹ with the World Economic Forum predicting that some 60 - 70% of new value will be “based on data-driven digitally enabled networks and platforms” in the coming years.² In this changing business environment, data will become an increasingly valuable asset for companies, such as an increase of 5 - 6% in output and productivity with data-driven decision-making.³

Data is also crucial to the development of Artificial Intelligence (“AI”). Businesses are using AI to enhance productivity, gain new business insights and create new products or services to drive new business models or revenue streams. As the use of AI proliferates, data that powers AI development is expected to grow in demand. In particular, businesses have recognised that pooling data together, or getting access to external sources of data, can generate greater value. In Singapore, organisations have also started to realise the shared benefits of pooling data such as generating new income, reducing costs and providing public or sectoral good. The following table highlights some real-life data sharing examples.

a Example: Improve customer experience, resulting in new income

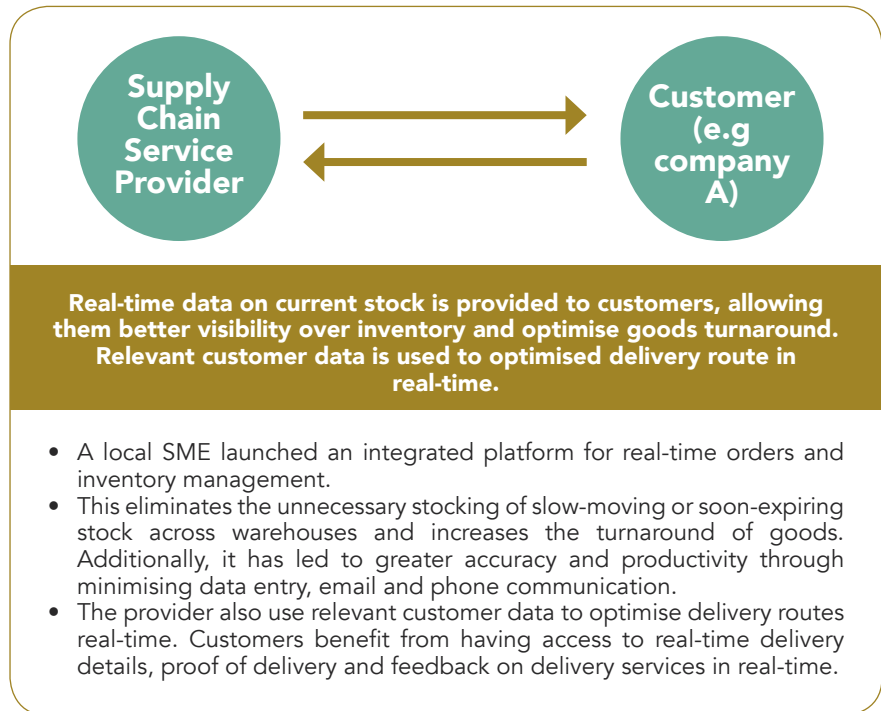


¹ International Data Corporation (30 October 2018) 'By 2023 Nearly Every Enterprise Will Be "Digital Native" in an Increasingly Digitized Global Economy'

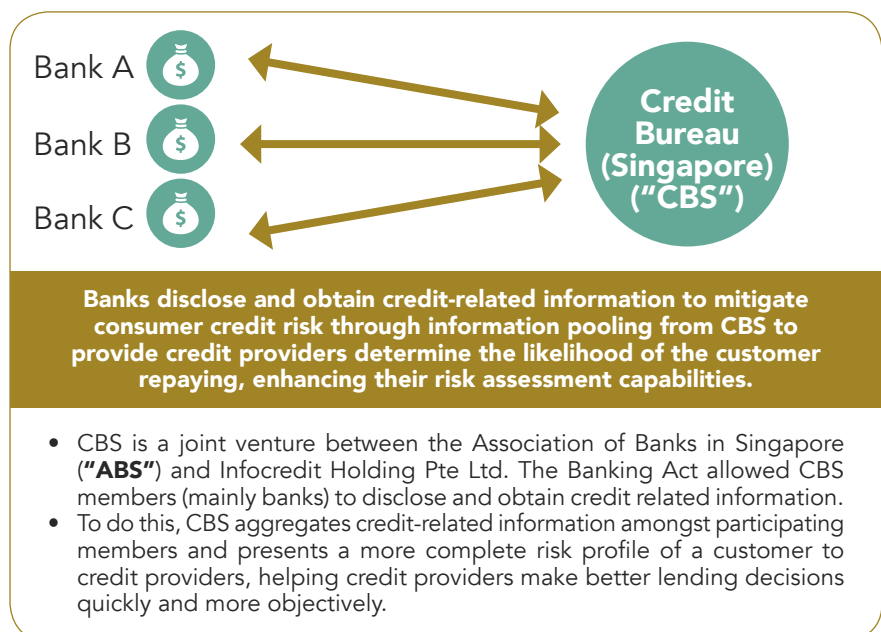
² World Economic Forum (December 2018) 'Our Shared Digital future: Building an Inclusive, Trustworthy and Sustainable Digital Society'

³ Brynjolfsson E, et al. (22 April 2011) 'Strength in numbers: How does data-driven decision making affect firm performance?'

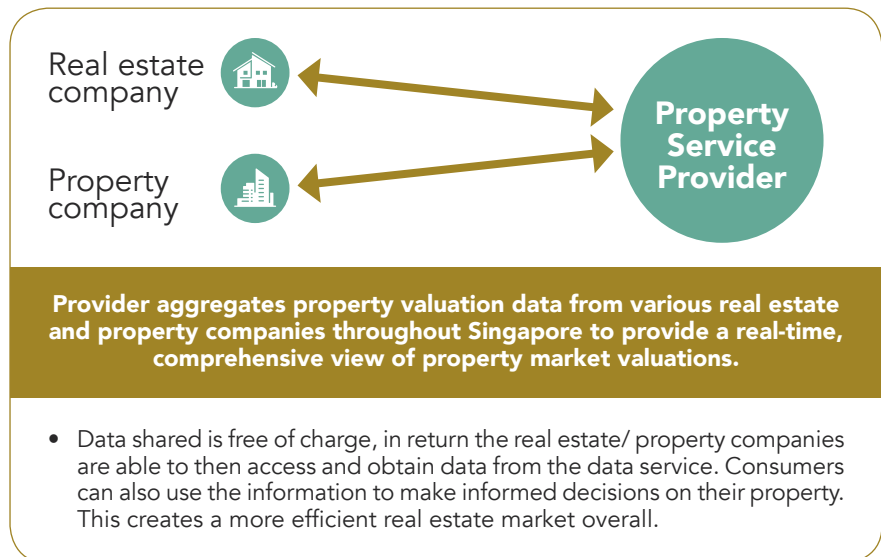
b Example: Improve overall efficiency over supply chain, resulting in cost reduction



c Example: Provide comprehensive information for overall market efficiency for the sector

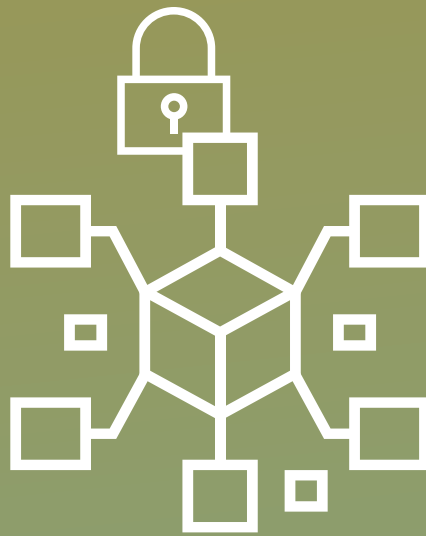


d Example: Provide comprehensive information for public good



While many companies recognise the value of data to generate useful insights and develop innovative products and services, data sharing across organisations has been slow to take off. Based on information gathered from more than 40 companies, the Infocomm Media Development Authority ("**IMDA**") understands that the barriers to data sharing include establishing mutual trust for proper handling of shared data, understanding the mechanisms for data sharing, and ensuring compliance to regulations when sharing data with other organisation(s). This Framework seeks to address these concerns through giving an overview of possible data sharing mechanisms and highlighting the key considerations when sharing data.

As technology develops and more services become digitalised, the data landscape will change. For example, new technologies that protect or reduce the need for data being exchanged (privacy-preserving technologies, distributed machine learning, etc) would mature, making it easier for businesses to leverage one another's data. The methods that are detailed in the subsequent parts of this Framework will then need to be updated to adapt to these changes, including any new policies that may be introduced.



TRUSTED DATA SHARING FRAMEWORK

The Framework (illustrated on the next page) is designed to:

- a** provide an overview of the key areas in data sharing;
- b** highlight key considerations in each area;
- c** facilitate data sharing conversations with data sharing partners and stakeholders; and
- d** help users think through the entire process to structure their data sharing arrangements.



KEY CONSIDERATIONS IN DATA SHARING

The motivation to share data typically stems from business needs such as the creation of new services, lowering business costs, detection of fraud, regulatory compliance, etc. The business motivations will, in turn, help data partners agree on the intended outcomes of their data sharing activities. Once established, organisations may consider using the Framework to kick-start their data sharing journeys. 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:

Part 1: Data Sharing Strategy

Organisations will understand what data will be useful to be shared, how this data can be valued, and the various arrangements or models that can be used for the sharing of the data.

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

Part 2: Legal and Regulatory Considerations

Organisations will understand the compliance requirements for data sharing, and how to structure the legal relationship to enable trusted data sharing between parties.

Recommended readers: Users who are driving projects, business units who collect, manage and use data, and advisory teams on technical/ risk and compliance matters

Part 3: Technical and Organisation Considerations

Organisations will understand the technical considerations and mechanisms for moving data to other organisations.

Recommended readers: Users who are driving projects, business units who collect, manage and use data, and advisory teams on technical/ risk and compliance matters

Part 4: Operationalising Data Sharing

Organisations will understand the additional considerations after data sharing has taken place.

Recommended readers: Users who are driving projects, and advisory teams on legal/technical/ risk and compliance matters

TRUSTED DATA SHARING FRAMEWORK

PART 1: Data Sharing Strategy

1.1 Establish Data Sharing Potential and Value of Own Data

1.2 Understand Potential Data Sharing Models

1.3 Consider Engaging Data Service Provider to Facilitate Data Sharing

PART 2: Legal and Regulatory Considerations

2.1 Determine if Data Can Be Shared

2.2 Establish Data Sharing Agreement

PART 3: Technical and Organisation Considerations

3.1 Prepare Data for Data Sharing

3.2 Understand Technical Considerations for Data Sharing

PART 4: Operationalising Data Sharing

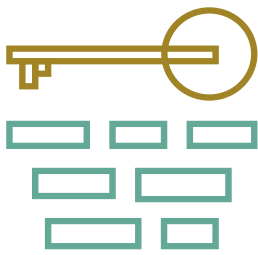
4.1 Ensure Transparency and Accountability

4.2 Monitor Ongoing Legal and Regulatory Obligations

4.3 Use of Data for Secondary Purpose

4.4 Understand Considerations for Retention and Disposal of Data

Figure 1: Trusted Data Sharing Framework and key outcomes



KEY ROLES IN DATA SHARING

Data can be said to have been “shared” when it is made available by a “Data Provider” to one or more organisations (each, a “Data Consumer”). This may not involve the physical movement of data from one location to another or access to original/raw data.

Below is an overview of the data sharing ecosystem and the key roles in the ecosystem. Roles are not mutually exclusive and activities attributed to each role may overlap, depending on the data sharing model. References to these roles would be made throughout the Framework.

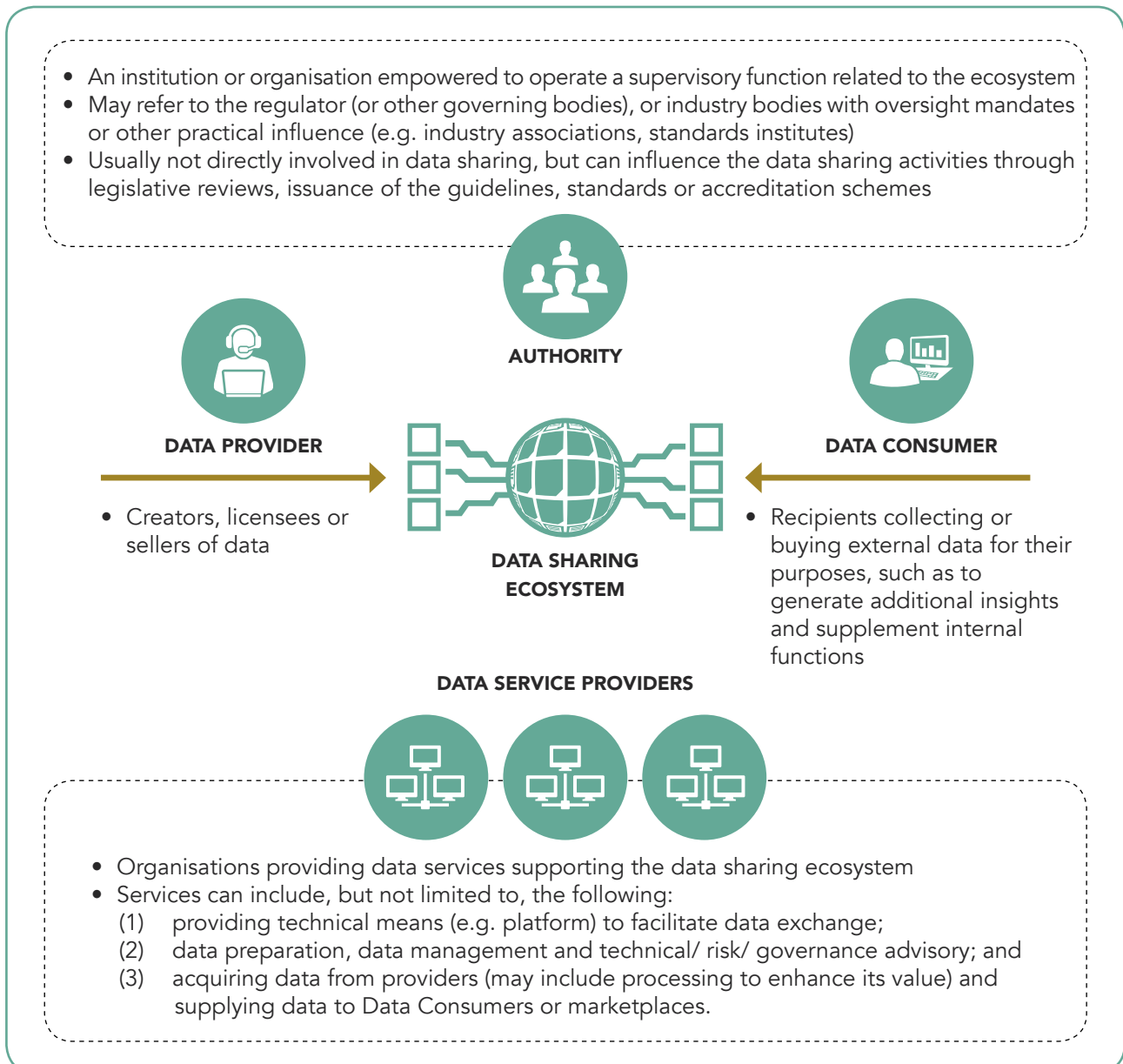


Figure 2: Data sharing ecosystem and key roles

Specifically, users considering to share personal data through a third party or data service providers may wish to note that an organisation processing personal data on behalf of another organisation is considered a “data intermediary”.⁴ They should take note of additional measures needed, as if they themselves are processing the personal data. Additional measures will be highlighted in blue boxes throughout the Framework.

⁴ Referring to an organisation that processes personal data on behalf of and for the purposes of an organisation pursuant to a written contract is subject only to the Data Protection Provisions relating to protection and retention of personal data, and not any other Data Protection Provisions. An organisation that engages a data intermediary has the same obligations under the PDPA for personal data processed on its behalf by the data intermediary as if the personal data was processed by the organisation itself.



TRUST PRINCIPLES

Embedded throughout the Framework is the concept of trust. As data sharing often involves the movement of data assets, it is important to establish that each party would be able to handle and manage the data asset responsibly. This Framework introduces 6 Trust Principles: **Transparency, Accessibility, Standardisation, Fairness and Ethics, Accountability and Security and Data Integrity** as foundations to forming a trusted data sharing partnership. How these principles can be applied at different data sharing areas are explained in the Appendix.



Transparency

Refers to the openness of all parties involved in data sharing to make available all information that is necessary for the successful delivery of the data sharing partnership.



Accessibility

Refers to the ability of parties to access the data they need, when they need it.



Standardisation

Refers to applying consistent legal, technical and other measures to data sharing partnerships.

**Fairness and Ethics**

Refers to going beyond meeting personal data protection and technical or security standards or regulatory requirements. It extends to the need to apply ethical standards to the creation and use of data sharing systems and frameworks, starting from the initial design phase.

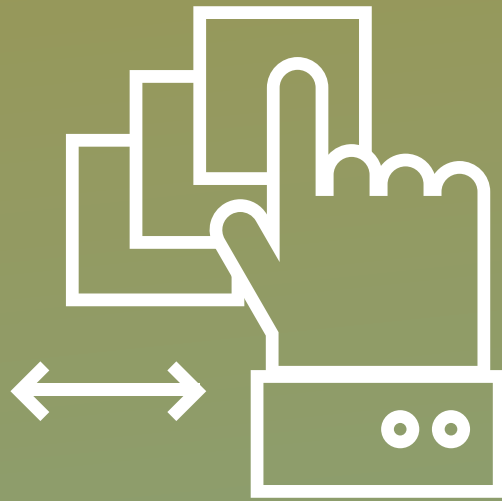
**Accountability**

Refers to demonstrating compliance with data protection laws and other rules specific to the data sharing partnership, and that each party has robust governance structures in place, and a corporate culture that encourages employees to take responsibility for the handling of data.

**Security and Data Integrity**

Refers to the implementation of measures and mechanisms designed to securely protect and safeguard information and data to enable a secure environment for data sharing.

Refer to **APPENDIX I: Application of Trust Principles** on how the principles can apply at each part of the Framework.



PART 1: DATA SHARING STRATEGY



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.

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

1.1 ESTABLISH DATA SHARING POTENTIAL AND VALUE OF OWN DATA

Data is an intangible and non-rivalrous resource. Unlike tangible resources that can only be consumed by a single process, data can be used at the same time across multiple business initiatives thereby increasing its value to organisation. At the same time, the value of data is also dependent on the capability and capacity to harness the value of data. Hence, business initiative or business motivation is usually the basis for establishing value of data that is relevant to support the initiative.

In the event where there is a need to assess the value of data on its own (e.g. when approached by business partners for data), organisations may consider the following three key actions:

- A** Take Stock of Own Data
- B** Assess Potential for Sharing
- C** Consider Data Valuation Approaches

A) Take Stock of Own Data

Many organisations generate large amounts of data in their day-to-day business, making it challenging to conduct a comprehensive stock-taking exercise. A useful starting point would be to understand what constitutes a data asset.

Data assets are intangible, and they generally:

- a are identifiable and definable** - data assets may be made up of specific files or specific tables or records within a database;
- b promise probable future economic benefits** - have value, the data asset must have a useful application. Identifying productive uses for data is often necessary to assign value to the asset; and
- c are under the organisation's control** - the organisation must also have rights to use the data in a way consistent with its rights under applicable law and any contractual licensing arrangements, while also protecting the data and restricting access to it by others.

During the process of stock-taking, it is important to categorise the data. When it comes to categorising data types, there is no 'one-size-fits-all' solution. Depending on the industry and context, organisations will have to define their own data taxonomy. While this is generally a lengthy and challenging exercise, organisations could set up their own unique taxonomy to share the data internally across business units and externally.

In defining the taxonomy, organisations could consider dimensions such as data source, data domain or even the geographical origins of the data and how strategic the data is to the organisation. Organisations could use the following examples of data taxonomy as reference to guide their stock-taking and categorisation.

Data Taxonomy Example 1:		
	Data Source	Examples
	Authored Data Typically created through some kind of creative process	• Architectural drawings • Photographs • Music soundtracks
	User-entered Data Data purposefully entered by users into a system without any expectations	• Social media posting • Reviews on third-party rating sites
	Captured Data Recorded from events occurring in the real world or digitally	• Financial transactions • Web browsing logs • CCTV recordings
	Derived Data Typically generated by combining, aggregating and otherwise processing other data	• Credit scores • Aggregated transactions

Figure 3a: Example of data taxonomy

Data Taxonomy Example 2:

	Data Category	Examples
	Master Data Describes people, places and things that are critical to a firm's operations	• Customer data (name, address) • Supplier data (contact details) • Product data (product features) • Employee data (name, position)
	Transactional Data Describes an internal or external event or transaction that takes place as part of the organisation's business	• Sales data (purchase history, credit card payments, sales order) • Payment data (payment date) • Geospatial data (current location)
	Reference Data Information that is used solely for the purpose of categorising data	• Jurisdictions (area code) • Currencies (currency code) • Industry standard data (country code) • Demographic fields
	Metadata Characterises other data, making it easier to retrieve, interpret or use the data	• Date of creation tag • File author identity tag • Audit trail data (accesses, changes) • Descriptive data (author, abstract)
	Unstructured data Data lacking a consistent format or syntax to describe objects and attributes	• Social media posting • Car movements • Weather data • Photography

Figure 3b: Example of data taxonomy

B) Assess Potential for Sharing

In some cases, organisations may be approached by potential users of their data. In other cases, organisations can also proactively assess potential for data sharing by identifying potential use cases that could leverage data from other organisations, or identifying potential uses and users for their own data.

When assessing potential use cases and data partners for the data, an organisation should consider all potential stakeholders in the whole value chain or ecosystem that the organisation operates in. This is in view that potential use cases could be generated from new insights derived from combining data with stakeholders across the value chain, beyond the immediate key suppliers and consumers. For example, credit card providers could share data on purchasing patterns with goods manufacturers and not just retailers.

C) Consider Data Valuation Approaches

Data sharing arrangement is largely driven by the commercial business case. Often, even when the commercial business case is clear, data sharing partners may have vastly differing assessments of the value of the data to be shared. With knowledge of their data assets and identification of data partners, organisations may consider using common data valuation methodologies as yardsticks to establish an agreed value for their data assets when negotiating with data sharing partners. The data valuation methodologies are provided to assist data sharing partners in overcoming impasses in negotiations.



1.2 UNDERSTAND POTENTIAL DATA SHARING MODELS

Organisations should decide on the most appropriate model that they could adopt to share data. Data sharing can take place on a bilateral, multilateral or decentralised basis:

- a Bilateral** – two parties agree to share data with each other, where sharing can be one-way (one party may act as Data Provider and the other as Data Consumer) or two-way (each party both provides and receives data). Trust is established directly between the data sharing partners.
- b Multilateral** – three or more parties agree to share data with one another, each acting as a Data Provider, a Data Consumer or both, depending on the circumstances. Trust is established either directly amongst the data sharing partners or established “institutionally” through a Data Service Provider, which is trusted independently by each of the data sharing partners. The Data Service Provider is trusted to manage the access and sharing of data.
- c Decentralised** – includes peer-to-peer (“P2P”) and other distributed systems. These are designed to grant control over data access and sharing to a community of participants. Participants in this community may share data on a bilateral or multilateral basis, using advanced platforms governed by a system of incentives and crowd consensus. This model relies on “distributed” trust amongst all participants within the decentralised ecosystem. The decentralised data sharing model will create new mechanisms for the trusted data exchange between counterparties without requiring any single third party to handle the data. New technology can also facilitate sharing without requiring the transfer of source data. However, where trust is distributed among multiple and often unknown data sharing partners, this can create challenges around ensuring that those data sharing partners are accountable to one another.

*For examples of data sharing models, refer to **APPENDIX II: Data Sharing Models – Example Scenarios & Case Studies.***

As identity is a core component of trust between organisations exploring a data sharing partnership, organisations may require that each partner is identifiable and its representatives are duly authorised by the organisation. This can be important when an organisation is new to market and may need to provide more assurance to its data partner on its credibility and legitimacy. For example, in regulated sectors such as healthcare, education, government or financial services, comprehensive due diligence on a data partner's identity may be mandatory and the form and detail of the checks may be prescribed.

Organisations should be aware of the potential risks associated with data sharing:

- a Lack of control over the use of data**

Notwithstanding the technical and due diligence measures discussed in this Framework, sharing of data with a wider audience may increase the risk of unwanted access to or unauthorised use of the data, including those by malicious actors. For example, there may be situations where a competitor may request for data belonging to a Data Provider, and the Data Provider does not wish for it to gain access to the data.
- b Lack of control over exchange or platform modifications**

As part of their terms and conditions, Data Service Providers offering data exchange platforms may seek to reserve the right to unilaterally modify the platform or exchange, either temporarily or permanently, at any time without giving prior notice to participants on the platform. This can result in additional costs and risks for participants, especially where such modifications occur at short notice.

Additionally, Data Service Providers will typically seek to exclude their liability for any data shared between participants on the platform, as well as any liability for participants' losses resulting from any modification, suspension or termination of the platform. This may severely limit or entirely exclude participants' ability to claim for losses resulting from their use of such platforms.
- c Insolvency and reputational risks**

Involving an external party would inevitably incur additional risk. For instance, in the event of a breakdown in commercial relationship with partners, some challenges in accessing or retrieving the data may be incurred. On the other hand, if the Data Service Provider runs into issues which may cause reputational damage, the reputation of its associating data sharing partner(s) may be affected.



1.3 CONSIDER ENGAGING DATA SERVICE PROVIDER TO FACILITATE DATA SHARING

Data Service Providers can perform multiple data services such as data preparation, data sharing and data analytics. Depending on the needs, Data Service Providers can do more by helping to service the myriad requirements of industry participants to utilise data effectively and build trust by facilitating data exchange among organisations. For example, Data Service Providers can help to match Data Providers with Data Consumers, and also offer other services, such as standardised data sharing agreements or placing risk control mechanisms on their platforms.

Where data sharing is facilitated by service providers in both multilateral model or in decentralised model, there is greater complexity. It is therefore important for organisations to perform additional due diligence, for example:

- a** Organisations should find out more about their Data Service Providers' internal data policies and best practices (for example, if they are certified under IMDA's Data Protection Trustmark) and their track records. They can also refer to the technical considerations in this Framework, to prepare the data appropriately (e.g. data is sufficiently aggregated) before sharing, and to establish the necessary technical modalities for data exchange. Organisations can also seek to retain control over access rights to their shared data.
- b** Organisations should assess the likelihood of platform-related issues occurring (taking into account factors such as the track record and solvency of the relevant data exchange operator, as well as the technology used) and the potential costs that might be incurred if such an event were to happen. This can then be balanced against the expected value or other benefits to be generated by participation on such a platform, to make an informed decision as to whether to proceed.
- c** Organisations can check if Data Service Providers offer services that mitigate risks associated with sharing of data with a wider audience, for example, data matching services which allow database cross-referencing between two or multiple participants to identify shared customers without providing access to the underlying data and/or without conveying any personal data. Organisations can also check if service offerings have features that allow control over data flow, such as using technology solutions like blockchain.



PART 2: LEGAL AND REGULATORY CONSIDERATIONS

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.

While this Framework takes into account Singapore's PDPA, organisations are reminded to ensure compliance with their obligations under applicable legislation in the sectors or markets in which they operate, or other requirements specific to their industry or nature of their business activities.

Recommended readers: Users in charge of driving projects, business units who collect, manage and use data, advisory teams on legal/risk and compliance matters



2.1 DETERMINE IF DATA CAN BE SHARED

A) Consider Rules and Restrictions On Data

Organisations need to consider a range of different rules and restrictions that may impact their data sharing activities. The rules and restrictions that apply will depend on the type of data being shared, how the data is being used and the parties involved.

The sources of these rules and restrictions may include:

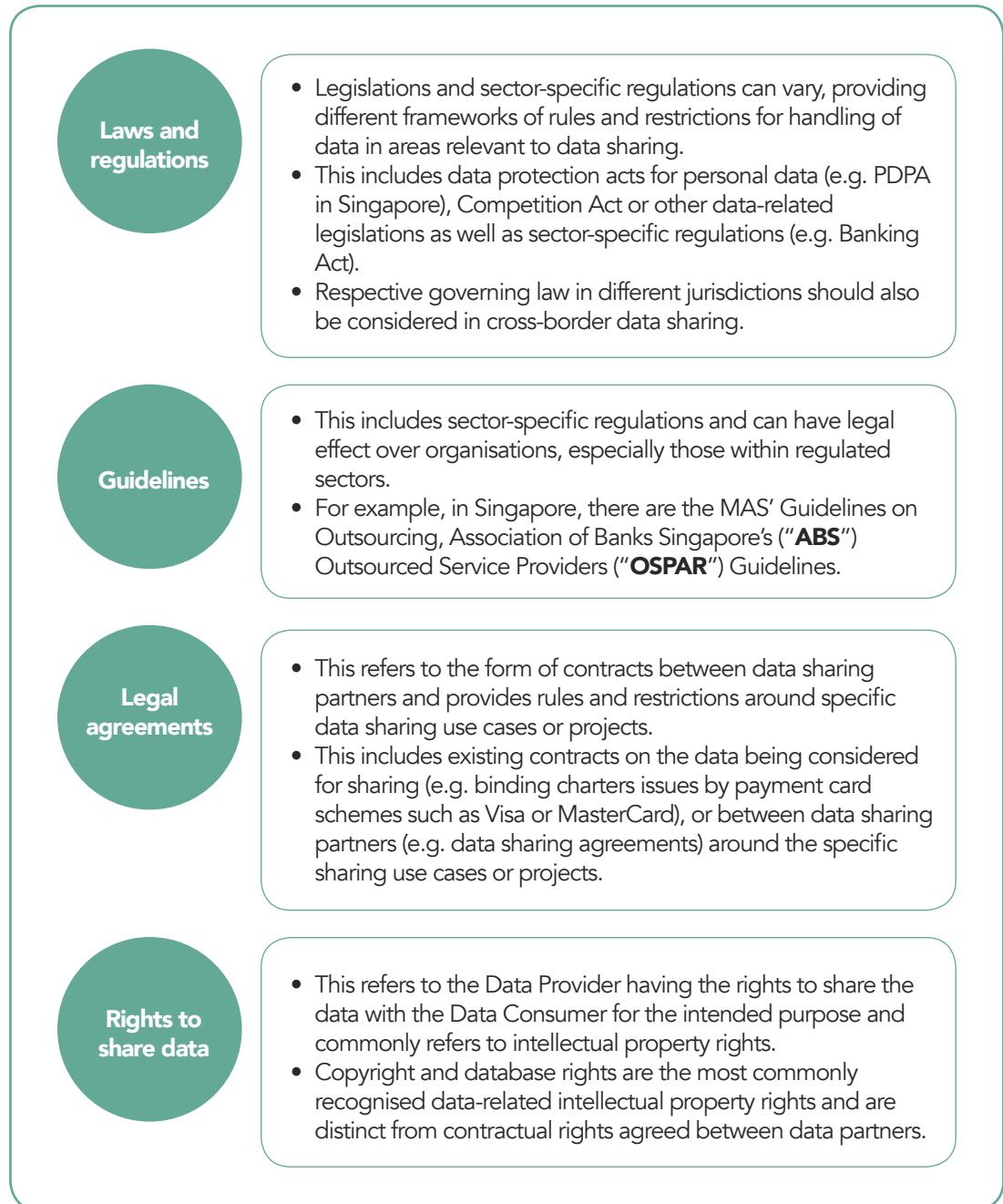


Figure 5: Sources of rules and restrictions

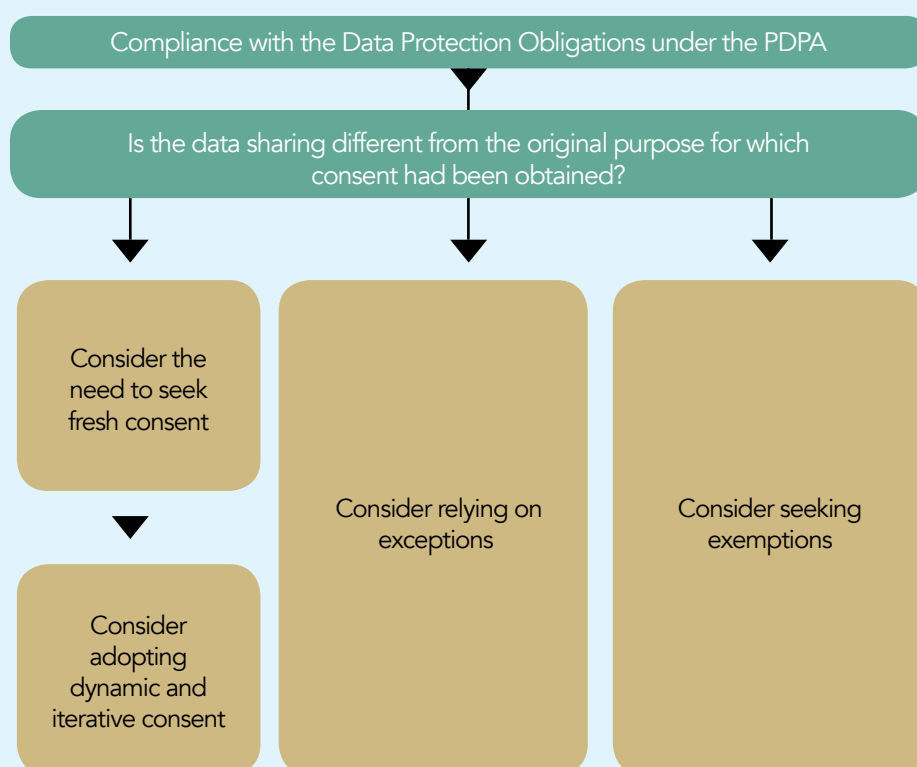
Refer to **APPENDIX III : Restrictions and Rules on Data Sharing** for details on how rules and restrictions on data sharing can apply, and **APPENDIX IV : Useful Sources of Worldwide Data Rules and Guidance** for some sources of data-related laws, regulations and guidelines.

B) Data Protection Policies and Practices

While data protection policies and practices are intended for internal use and compliance, they can help to engender trust in the data sharing partnerships by establishing that parties involved are responsible parties with similar data management, data protection and data use standards. Data protection policies and practices also help to demonstrate transparency relating to the use of data. Organisations can consider certification schemes, such as IMDA's Data Protection Trustmark, to accredit themselves on their data management schemes.

C) Considerations for Sharing Personal Data

For personal data, the PDPA sets out provisions to govern how organisations collect, use and disclose personal data. Organisations should consider the following factors:



Compliance to Data Protection Obligations under the PDPA:

An organisation should seek to understand what the obligations under the PDPA are, and how they apply to personal data. The obligations are summarised in the next few pages.

Collection, use and disclosure of personal data



Consent

- Obtain consent to collect, use or disclose individuals' personal data.
- Allow individuals to withdraw consent.



Purpose

- Do not make customers consent to the collections, use or disclosure of their personal data beyond what is reasonable to provide the product or service.
- Collect, use or disclose personal data only for the purposes for which consent was obtained.



Notification

- Notify individuals of the purposes for the collection, use or disclosure of their personal data.

Accountability to individuals



Access and Correction

- Upon request, provide individuals with their personal data and the ways in which their personal data were collected, used or disclosed in the past year.
- Correct any error or omission in individuals' personal data upon their request.



Openness

- Appoint a Data Protection Officer and make his/her business contact information readily available to the public.
- Publish information on the organisation's data protection policies, practices and complaint-handling process.

Care of personal data



Protection

- Put in place reasonable security arrangements to protect personal data from unauthorised access, collection, use, disclosure and similar risks.
- Make reasonable effort to ensure that the personal data collected is accurate and complete.



Accuracy

- Make reasonable effort to ensure that the personal data collected is accurate and complete.



Retention

- Cease retention or anonymise personal data when it is no longer necessary for any business or legal purposes.



Transfers

- Ensure that the standard of protection accorded to personal data is comparable to the PDPA when it is transferred overseas.

Figure 6: Summary of 9 data obligations under PDPA

Consider the Need to Seek Fresh Consent: Organisations must notify the individual of the purposes of the collection, use and disclosure of his personal data and obtain consent, on or before collecting the personal data. If an organisation intends to share the personal data for a different purpose from the original purpose for which consent had been obtained, it must inform the individual of the new purpose and obtain fresh consent, unless an exception applies.

Dynamic and Iterative Consent: In the context of data sharing, especially for activities like big data analytics, it can sometimes be challenging for organisations to determine the future purposes for sharing data at the outset, and whether fresh consent is required for the sharing. Organisations should consider adopting innovative processes and methods, such as dynamic and iterative consent, to comply with the consent requirement under PDPA. Organisations should set the default as “not-to-share”, and allow individuals to opt in to the data sharing and inform about the possible risks and implications for the individual as a result of sharing the personal data.

Examples of dynamic approaches to consent via a mobile application platform include just-in-time notifications and data protection dashboards.

Just-in-time notifications

Pop-up notifications pushed to individuals right before personal data is collected, used or disclosed.

Example:

An organisation that collects personal data via a mobile app could cater for just-in-time notifications, thereby enabling for multiple touch-points with individuals, and iterative means to obtain fresh consent where necessary.

Data protection dashboards

Personal data protection dashboards provide an interactive interface for individuals to modify real-time data protection preferences.

Example:

An organisation can provide a personalised dashboard allowing individuals to view the personal data that an organisation has collected about them, and how the personal data is being used or disclosed. Individuals can also easily opt in or out of any purposes or any further collection, use or disclosure of their personal data at any time.

Figure 7: Examples of dynamic approaches to consent

For details, refer to **APPENDIX VI : Consent, Dynamic and Iterative Consent.**

Consider Relying on Exceptions: The PDPA sets out exceptions⁵ where organisations may collect, use or disclose personal data without consent. Organisations relying on exceptions from the consent requirement must still comply with other Data Protection Obligations (e.g. transfers/ protection of personal data) when sharing the personal data. The following figure illustrates how exceptions may apply to the sharing of personal data:

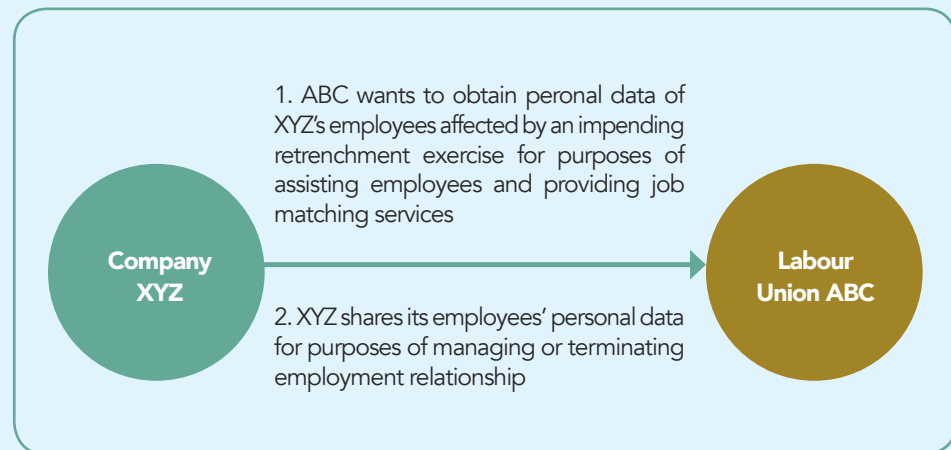


Figure 8: Example of how exceptions can apply

- Where Company XYZ had relied on the exception to collect personal data from its employees without consent for the purposes of managing or terminating their employment relationships, the personal data may be shared with Labour Union ABC for consistent purposes without consent.
- However, Company XYZ must still notify its employees of the purposes of sharing the personal data, and may determine the most appropriate manner of doing so. For example, it may provide the information in the employee handbook or human resource policies, and update employees through emails.

⁵ The exceptions from the consent requirement can be found in the Second Schedule (collection of personal data without consent), Third Schedule (use of personal data without consent), and Fourth Schedule (disclosure of personal data without consent) of the PDPA. Examples of how some of these exceptions apply can be found in the Key Concepts Guidelines, Advisory Guidelines for Healthcare Sector and Advisory Guidelines for the Social Service Sector.

Consider Seeking Exemptions under the PDPA: Where organisations are exploring data sharing arrangements (“**DSAs**”) to share personal data, organisations may consider applying for an exemption from all or any of the provisions of the PDPA, subject to specified terms and conditions, as follows:

1. Notification and Opt-Out

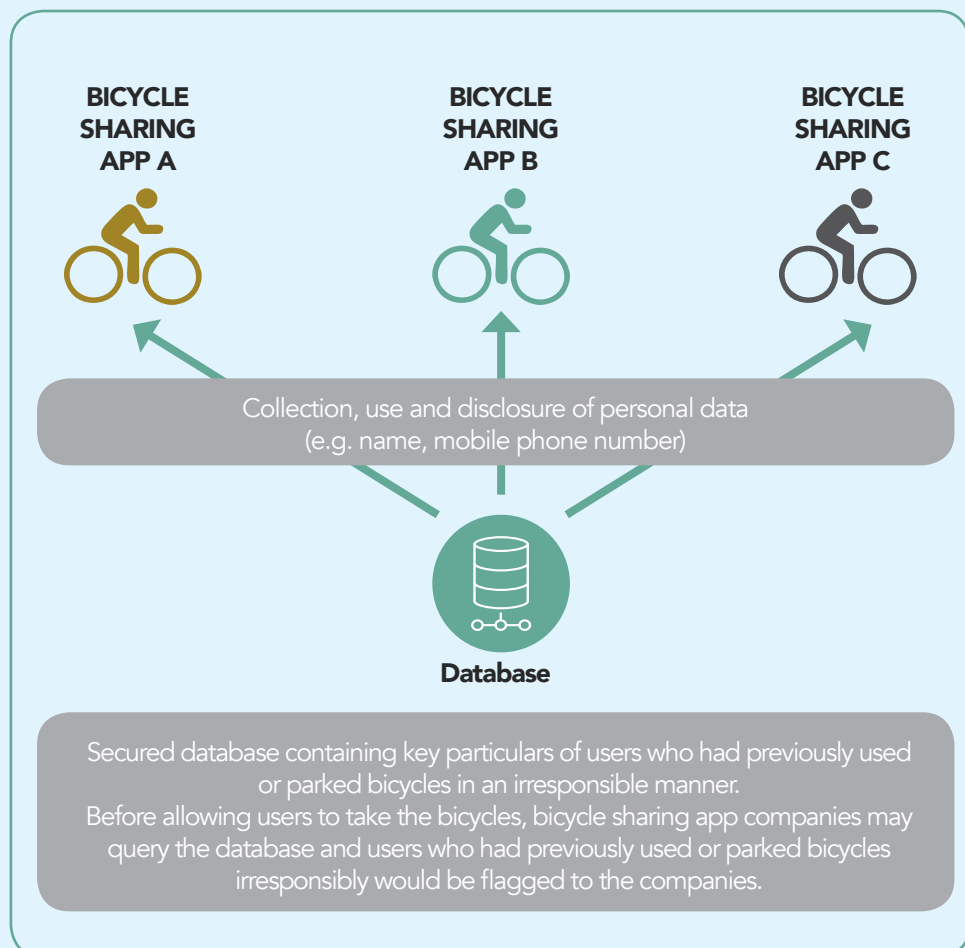
- Sharing for such purposes is **not likely to have any adverse impact on the individuals**
- Sharing is not for the purpose of direct marketing

2. Legitimate Interests

- Obtaining consent for the purposes may not be desirable or appropriate
- **Benefits** to the public (or section thereof) from the sharing **clearly outweigh any adverse impact or risks to the individuals**

Figure 9: Circumstances that may allow for exemptions

This is permitted, with approval of the Minister, by order published in the Gazette, to exempt any person or organisation, or any class of persons or organisations, from all or any of the provisions of the PDPA, subject to specified terms and conditions.



- Bicycle Sharing Applications A, B and C established that there is a need to protect legitimate interests that will have benefits for the public, and such processing should not be subject to consent since individuals may not provide consent in such circumstances (i.e., customers who intend to misuse, damage or irresponsibly park bicycles would be unlikely to provide consent and would likely withdraw consent for this purpose).
- Bicycle Sharing Applications A, B and C may submit a proposed DSA to the Personal Data Protection Commission ("**PDPC**") for an exemption from specific provisions of the PDPA to share personal data of identified customers with a track record of misusing, damaging or irresponsibly parking the bicycles used. This will help to reduce incidences of public nuisance and hazard to the public caused by irresponsible users.
- Bicycle Sharing Applications A, B and C must conduct data protection impact assessments to assess the risks and impact of sharing the personal data, and implement safeguards and measures to mitigate such risks.
- Bicycle Sharing Applications A, B and C must still comply with the other Data Protection Provisions which the DSA is not exempted from (e.g. taking reasonable steps to protect the personal data, including implementing controls to limit access to the database). Any data inaccuracies should be corrected as soon as reasonably possible.
- For transparency, Bicycle Sharing Applications A, B and C should disclose their reliance on legitimate interests and make available a document justifying their reliance on legitimate interests for sharing the personal data. Customers should also be informed that any failure to return their bicycles could result in their inclusion on a shared database, and that they may be prevented from renting bicycles in the future.

Figure 10: Example of exemption under the PDPA

For details, refer to **APPENDIX VII: Exemption under the PDPA**.



2.2 ESTABLISH DATA SHARING AGREEMENT

A data sharing agreement sets out the important terms that should be agreed between organisations to govern the data sharing partnership. While there is no prescribed format for a data sharing agreement, some of the important terms include:

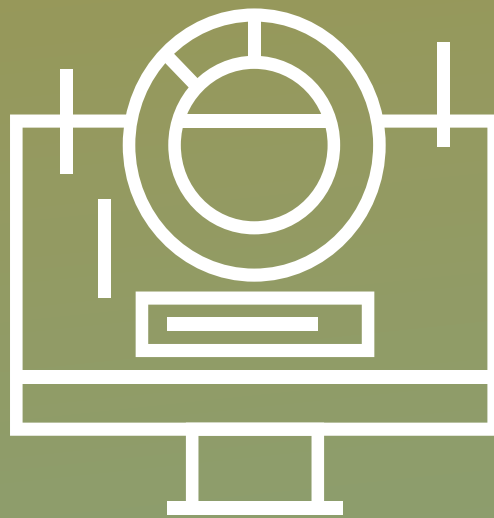
- a** the grant of the licence/permissions to use the data for the intended purpose;
- b** restrictions to the permitted use of the data (if any), such as territorial or time limitations, exclusivity or commercialisation rights;
- c** warranties or other assurances provided in relation to the Data Provider's rights in the data;
- d** allocation of liability for contract 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; and
- g** governing law and resolving disputes.

In the context of data sharing, organisations should be aware of two terms – grant of license and resolving disputes – which form the basic considerations to data sharing activities.

Grant of License: The permission to use the data for the intended purpose provided by the Data Provider to the Data Consumer is typically granted in the form of a license and 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 which was 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 data.

Resolving Disputes: Disputes may arise between Data Providers and Data Recipients. Common disputes between Data Providers and Data Recipients are related to payment, breach of licence terms (e.g. unauthorised sharing or use) or breach of other agreed terms. Within a data sharing agreement, it is recommended for the parties to agree on simple escalation procedures to ensure that within each organisation a dispute receives sufficiently senior attention at the appropriate time and that the parties have processes in place to respond to issues quickly to limit losses. Similarly, the parties should agree on how to resolve disputes where amicable resolution is not achieved after appropriate escalation.

*For a start, organisations can refer to the template clauses provided in **APPENDIX V: Considerations for Data Sharing Agreement.***



PART 3: TECHNICAL AND ORGANISATION CONSIDERATIONS



With an idea of a data sharing partnership in mind, organisations need to consider and put in the technical mechanisms for data sharing to take place.

Recommended readers: Users in charge of driving projects, business units who collect, manage and use data, advisory teams on technical/ risk and compliance matters

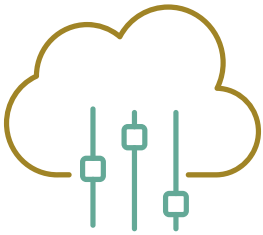
3.1 PREPARE DATA FOR DATA SHARING

Depending on the type of data and its potential utility, organisations preparing to enter into a partnership may seek to compile, refine or in some other way, optimise the data before sharing, to ensure it is able to be used for the intended purpose.

For example, during data extraction, organisations should identify the correct and required amount of data that can meet the data sharing objectives. When transforming data, where personal data is involved, organisations should use anonymisation by default and ensure that the data sharing does not require identifiable information. Organisations should also ensure that during data loading, data was transmitted in a secure manner and check for data corruption.

When sharing personal data, Data Providers should first consider if using anonymised data can meet the data sharing objectives. Anonymisation or other techniques can prevent unauthorised dissemination of data and mitigate risks such as those posed by malicious third parties seeking to reverse-engineer data from anonymised datasets. For data to be considered anonymised, organisations have to ensure that there is no serious possibility that an individual can be re-identified. If there is a need to share identifiable data, PDPA compliance becomes relevant and Data Providers should consider if the data sharing purpose is different from the original purpose for which consent had been obtained, and consider the need to seek fresh consent, rely on or seek exemptions.

*For details, refer to the PDPC's **"Guide to Basic Data Anonymisation Techniques"** and **"Chapter 3 (Anonymisation) of the Advisory Guidelines on the PDPA for Selected Topics"**.*



3.2 UNDERSTAND TECHNICAL CONSIDERATIONS FOR DATA SHARING

A) Recommended Practices for Securing Data Sharing Activities

For securing data sharing activities, the recommended practices are drawn from existing risk assurance standards, guidelines and certifications. The extent of adoption or application to data sharing activities should be scaled according to organisations' requirements and the data sharing use case.

Governance: Governance refers to the policies, procedures and operational processes put in place to guide personnel through the maintenance of security over information, data and systems. It supplements the technical mechanisms implemented on the infrastructure. These procedures facilitate the oversight and efficient execution of tasks to make changes or the timely maintenance of technological competencies.

Some recommended practices are as follows:

- a** Establishing, documenting, communicating and implementing policies and procedures around data, information and system management, which include:
 - setting up regular meetings amongst stakeholders to monitor data sharing issues;
 - labelling data assets and objects containing data including data aggregation containers;
 - classifying data and objects containing data based on data type, value, sensitivity, and criticality to the organisation;
 - (where data is highly sensitive) developing a comprehensive data loss prevention strategy, taking into consideration the following specifications:
 - Data at endpoint – data which resides in notebooks, personal computers, portable storage devices and mobile devices
 - Data in motion – data that traverses a network or that is transported between sites
 - Data at rest – data in computer storage which includes files stored on servers, databases, backup media and storage platforms
 - establishing clearly defined and understood roles and responsibilities (ownership, stewardship) across datasets and systems before data is transferred out of controlled environments; and
 - retaining and destroying data and information. Policies and procedures should clearly state guidelines based on the classification of information/data and applicable laws and as agreed with the third party.

- b** Deploying and maintaining policies and procedures around the maintenance of industry-accepted cryptography/encryption protocols for sensitive data in storage (e.g. file servers, databases and end-user workstations), data in use (memory), and data in transmission (e.g. system interfaces, over public networks and electronic messaging) as per applicable legal, statutory and regulatory compliance obligations.
- c** Establishing and maintaining policies and procedures around a minimal Know-Your-Customer ("**KYC**") for various types of user access across systems.

Infrastructure Security: Infrastructure security refers to the necessary security controls and mechanisms to the network and physical facilities to prevent security breaches or attacks compromising business-as-usual ("**BAU**") capabilities. Examples of network type attacks include Man-In-The-Middle ("**MITM**") attacks and Distributed Denial-of-Service ("**DDoS**") attacks.

The following are some recommended practices:

- a** Implementing and testing the robustness of defensive mechanisms such as defence-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns. These mechanisms may also include network intrusion detection/prevention systems ("**NIDPS**"), web application firewalls ("**WAFs**"), DDoS mitigation mechanisms and data leakage prevention systems.
- b** Protecting data endpoints by blueprinting all network infrastructure before implementing and/or maintaining secure standardised network protocols (e.g., TCP/IP, FTP, HTTPS) that involve communication between two or more devices. Protect confidential information stored in all types of endpoint devices with strong encryption.
- c** Developing and implementing redundancy plans for single points of failure that can bring down the entire system or network.
- d** Isolating or segregating unencrypted data in online or offline backups for replication and storage.

- e Establishing and maintaining procedures and mechanisms for access into physical facilities (e.g. via card access, biometric systems, ISO standard locks) – by authorised personnel on a need-to-have basis only. These include:
 - reviewing at a frequency agreed with the third party, the access rights to data centre/controlled areas, and monitoring, following up and reporting access violations in accordance with the contract agreement;
 - promptly revoking or disabling physical access credentials when not required, and managing the inventory of security access cards and promptly invalidating or revoking the damaged or lost cards in the access control system; and
 - knowing where data is physically stored and establishing physical entry controls (e.g., card-controlled entry points and surveillance cameras) to be followed by authorised employees with access to data centre.
- f Conducting regular enforcement checks against security controls and ensuring that baseline standards (i.e. system security baseline settings and configuration rules) are carried out to monitor compliance.

Access Management: Access management refers to the technical and operational security measures to ensure that each user has only the minimum privileges for access to the right resources (data, information, systems) at the right time to perform their functions. Non-authorised parties should not be granted access.

Some recommended practices are as follows:

- a Establishing and maintaining user access policies and procedures for appropriate identity, entitlement, and access management for all users relating to data and application interfaces as well as infrastructure network and systems components, including:
 - performing screening procedures (e.g. by KYC), for all users prior to granting any level of access granting access to IT systems software only where based on a documented and approved request, and on a need-to-use basis;
 - periodically reviewing in accordance with a frequency agreed all users' access to IT systems;
 - restricting access to data proportional to its classification to be accessed, business requirement and acceptable risk;
 - establishing a network architecture blueprint to observe the criticality of system components to subsequently define the logical access requirements to all IT systems (i.e., programmes, data and operating system software, which includes defining from the 'least privileged' user group to the 'most privileged' user group); and

- implementing and maintaining technical mechanisms and controls (e.g., two-factor authentication, IP address filtering and TLS encapsulated communications) to restrict access on single sign-on to servers or devices.

- b** Monitoring the use of privileged access and log access in accordance with internal and independent third-party audits of compliance.

Incident Management and Backup: Incident management and backup refers to the operational procedures that provide assurance around recovery and continuity of systems and infrastructure achieved through these means: proper storage and documentation of data, information and system recovery processes in an accurate, timely and secured manner, as well as the authorisation of appropriate personnel to execute immediate action in response to an incident.

Some recommended practices are as follows:

- a** Documenting formal incident management and disaster recovery processes as guided by regulatory standards, internal compliance and contractual agreement between parties. The processes should be reviewed periodically, and include:
 - timely review of the document at least every 12 months, or where there have been changes to processes that would affect the service provided;
 - roles and responsibilities of authorised staff involved in the incident management process, including recording, analysing, remediating and monitoring of problems and incidents;
 - escalation and resolution protocols and timelines; and
 - preparation for diverse scenarios including but not limited to major system outages, hardware malfunction, operating errors, security incidents and total incapacitation of the primary processing centre.
- b** Documenting formal restoration and data disposal processes as guided by regulatory standards, internal compliance and contractual agreement between parties. The processes include:
 - backup and restoration of technical and business processes such that data can be recovered where necessary during the data sharing timeframe; and
 - secure disposal processes from all concerned storage media objects, ensuring that data is not recoverable by any computer forensic means.
- c** Establishing and implementing data input and output integrity routines (i.e. reconciliation and edit checks) for application interfaces and databases to prevent manual or systematic processing errors, corruption of data or misuse.
- d** Securely storing system level backups at off-site storage facilities.

Monitoring and Risk Management: Monitoring and risk management refers to any structures, ongoing assessments, risk management and responsibility allocation mechanisms relevant to measuring and managing data, information and system risks. Critical to risk management is the categorisation of data based on type, value, sensitivity and criticality to the organisation – this categorisation will determine the level of associated risk and therefore appropriate security measures. Different data types will attract different legal, regulatory, contractual and jurisdictional requirements, which must be reviewed, managed and checked.

The following are some recommended practices:

- a** Establishing, maintaining and periodically reviewing a risk register which facilitates the monitoring and reporting of risks. This includes:
 - analysis and documentation of the risks presented by existing and new third-party arrangements, including but not limited to cybersecurity risks, fraud and corruption risks, operational risks, and reputational risks;
 - risk assessment of the identified risk factors which may include changes in the operating environment, new or revamped systems, rapid growth, new technology, new business models, products, or activities, or expanded foreign operations;
 - risk prioritisation based on susceptibility to risks, followed by a process around risk monitoring and reporting on mitigation efforts and actions; and
 - risk remediation plans to resolve vulnerabilities including status updates and a roadmap.
- b** Developing and conducting change management processes where the operating environment, including technology components, are due for change. The materiality of changes should also be evaluated, especially in situations such as:
 - assimilating new functions into its systems or implementing new systems that could affect the third-party arrangements;
 - gaining a substantial number of new users; and
 - diversion of resources to new activities from existing activities.

- c** Establishing and implementing policies and procedures, business processes and technical measures to inventorise, document, and monitor and maintain data flows for data residing either permanently or temporarily within the service's geographically distributed applications and infrastructure network and systems components. The same applies to data shared with third parties to ascertain any regulatory, statutory, or service level agreement ("**SLA**") compliance impact, and to address any other business risks associated with the data.
- d** Implementing an endpoint monitoring system to monitor the endpoint's status, activities, software, authorisation and authentication. Threats, risks, breaches and violations should be identified and addressed in a timely manner.
- e** Implementing an appropriate monitoring infrastructure such as a Security Incident and Event Monitoring ("**SIEM**") system to provide automatic analysis, correlation and triage of security logs from the various monitoring systems. Internal audit may be employed to evaluate the effectiveness of controls over time, either by ongoing activities, periodic evaluations, or combinations of the two. The risks presented by third-party arrangements, including but not limited to cybersecurity risks, fraud and corruption risks, operational risks, and reputational risks, should be understood, and relevant end-to-end processes be reviewed to identify any risks. Third-party risks tend to be unique to each engagement, and thus may require multiple robust plans for different scenarios.

*For personal data, companies may wish to consider referring to PDPC's "**Guide To Securing Personal Data In Electronic Medium**".*

B) Possible Technical Delivery Modes for Data Sharing

Data exchange, whether physical or virtual, can occur either directly between a Data Provider and a Data Consumer, or through a Data Service Provider who might provide platform accessible by both the Data Provider and Data Consumer. Regardless, it usually involves the migration of data from one source to another and organisations can consider protecting the data using cryptographic measures.

However, some organisations have recently explored the possibility of sharing data without transferring ownership (i.e., data stays in place with the original data provided but is allowed to be securely computed by its intended beneficiary). In such cases, data security can be provided by secure computation measures and distributed ledger technology.

The most common delivery modes for data exchange, along with their key characteristics, benefits, and challenges are summarised in the table below.

	Wire	Removable Storage Media	Wi-Fi	Remote Access/ VPN	Object Storage URL / SFTP	API	Distributed Ledger
Continuous Access	✓		✓	✓	✓	✓	✓
High Volume of Data	✓			✓	✓	✓	
High Speed of Transfer	✓		✓	✓	✓	✓	
Highly Sensitive Data	✓					✓	✓
Affordability		✓	✓		✓	✓	
Secure by Design	✓						✓

Figure 11: Common delivery modes for data exchange

C) Possible Security Measures to Protect Data Integrity

Organisations can also explore other ways to protect data integrity. There are various methods to secure data, cryptographic or otherwise. Cryptography refers to a range of techniques used to scramble or disguise data such that it is only available to an authorised person to restore the data to its original form.

- a** Where data sharing requires data to transit, cryptography presents an economical method of ensuring data security and offers different degrees of sophistication. Cryptographic measures can include: encryption, hashing, salting and tokenisation.
- b** Where data must stay in place, various methods of secure computation can be used to enable a highly secure data transaction. Secure computation techniques include homomorphic encryption and multi-party computation.

*For details, refer to **APPENDIX IX: Security Measures to Protect Data Integrity**.*



PART 4: OPERATIONALISING DATA SHARING

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.

Recommended readers: Users in charge of driving projects, advisory teams on legal/technical/ risk and compliance matters



4.1 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.

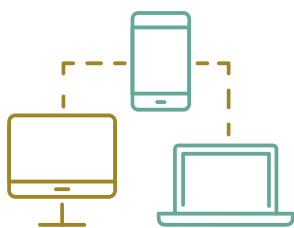
As data sharing and analysis is an iterative process, data sharing partners should refer to the Data Sharing Agreement that was established should ambiguities arise.

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.



4.2 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.



4.3 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 their data sharing partners and negotiate or request for the new use of data.



4.4 UNDERSTAND CONSIDERATIONS FOR RETENTION AND DISPOSAL OF DATA

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.



APPENDICES



DATA SHARING STRATEGY



APPENDIX I : APPLICATION OF TRUST PRINCIPLES

This Appendix explains how the 6 Trust Principles **Transparency, Accessibility, Standardisation, Fairness and Ethics, Accountability and Security & Data Integrity** can be applied in different parts of the Framework.

Each Trust Principle would be first explained, followed by how it can help engender trust in the partnership and lastly, examples of how it can be applied at different parts of the Framework.

Transparency

Transparency refers to the openness of all parties involved in data sharing to make available all information that is necessary for the successful delivery of the data sharing partnership.

The principle of Transparency is continuous and can be applied at any part of the Framework, reflecting the ongoing relationship between the organisations which are sharing data. Transparency and trust can be built by sharing relevant information, such as those relating to each organisation's business practices and policies, the data being shared and its components, and how the data being shared will be used.

For example, it is important for Data Consumers to clearly state, for example, how they will be using the data provided to them by the Data Provider. This can help data sharing partners build trust, and establish their integrity at the outset of their data sharing journey.

Accessibility

Accessibility refers to the ability of ecosystem participants to access the data they need, when they need it.

This is typically related to technical accessibility but can also refer to accessing other information such as metadata to find and identify data sets initially, to assess their quality and fitness for purpose before the data sharing partnership itself. This can help partners agree on the appropriate data sharing mechanisms and restrictions based on the data type and their data sharing model, establishing mutual trust and understanding that the data shared will be accessed by the right people at the right time.

For example, at the outset of the data sharing partnership, partners can decide what data sets (including metadata) should be accessible throughout the life cycle of that data partnership. For technical accessibility, organisations can consider the frequency of access, volume of data, exclusivity of access; and sensitivity of the data. Organisations can also ensure that each data partner's obligations relating to data access are clearly set out in the legal agreements for the data sharing partnership.

Accountability

Accountability refers to demonstrating compliance with data protection laws and other rules specific to the data sharing partnership, and also ensuring that the organisation has robust governance structures in place and a corporate culture that encourages employees to take responsibility for the handling of data.

With each organisation taking responsibility for the shared data, the Data Provider is assured that the data shared would continue to be compliant with the relevant laws and regulations. Within an organisation, a robust culture of accountability within the organisation across business units, departments and territories, can also help to build trusted data sharing partnerships with other organisations as it provides a sense of confidence that the data would be handled by individual(s) who are familiar with responsible data management practices.

For example, a written legal agreement can help to ensure accountability with external data partners. The agreement should clearly state the purpose of the partnership, describe the data being shared and allocate responsibilities between the parties relating to the use of the data. Accountability can also be demonstrated through keeping data trails and audit logs.

In a personal data context, if a data partner in Singapore has been awarded a Data Protection ("**DP**") Trustmark, this may also provide evidence of its accountability in responsible data protection practices.

Standardisation

Standardisation refers to applying consistent legal standards, technical standards and other measures to your data sharing partnerships.

In instances where organisations are from different industries and countries, relevant technical, legal and other standards may vary. Trust can be built more easily by harmonising and agreeing on the standards that will apply to the data sharing activity that is being put in place and ensuring these are included in the legal agreements for the data partnership.

For example, during the project planning phase, organisations can discuss relevant rules and restrictions that apply to each data partner and then assess how these impact the partnership, with the goal of seeking to harmonise and agree on common standards where possible. Once the methods are agreed upon, appropriate standards can be set out in writing and referenced in the relevant data sharing legal agreements.

Organisations should be aware that there are ongoing efforts being made towards strengthening the data ecosystem by aligning legislation and governance frameworks across the region such as the ASEAN Economic Community Blueprint 2025, the Master Plan on ASEAN Connectivity 2025 – both aim to harmonise international data laws, as well as the endorsement of the ASEAN Framework on Digital Data Governance by 10 Southeast Asian countries.

How legal standards, technical standards and other measures can be applied to engender trust are elaborated in the succeeding paragraphs.

Legal standards

Organisations operating internationally must comply with a range of data protection laws and other rules and restrictions at a country or industry level. Data sharing partners should therefore agree on the appropriate legal standards that apply to their partnership and refer to this in their data sharing agreements, as there may be less commonality in the legal standards, especially where they are from different industry sectors or jurisdictions.

For example, when entering into data sharing agreements, data sharing partners from different jurisdictions may manage the risks associated with the application of different laws and regulations by agreeing upon a governing law that they are both comfortable with, in the context of the planned partnership.

Technical standards

Similarly, from a technical standards perspective, terms used to describe the data and services have to be universally understood. This involves references to industry glossaries. Some examples are applicable International Organisation for Standards ("**ISO**") standards, the FIBO standard in the finance sector, or Preservation Metadata Implementation Strategies ("**PREMIS**") for metadata profiling.

Other measures

Beyond technical and legal standards, data sharing partners may discuss their preferred data quality standards, to ensure that data offerings meet a minimum level of quality assurance. While these standards may not have the force of law, for example, if they are specific to a particular industry or group of companies, they may be included in data sharing agreements to help build trust between the data sharing partners by ensuring that the data being shared is suitable for the project.

Fairness and Ethics

Fairness and Ethics refers to going beyond meeting personal data protection and technical or security standards or regulatory requirements. It extends to the need to apply ethical standards to the creation and use of data sharing systems and frameworks, starting from the project planning & strategy phase to the data retention & destruction phase.

By seeking to understand the data partner's approach to ethics in its data sharing and other activities, and consider referring to these in your data sharing agreements, as an important component of trust as this assures that the data will be used solely for the purposes that it is required, securely and in a manner consistent with the rights and consents obtained from individuals or other organisations.

For example, organisations' own commercial data and their counterparties' commercial data should be kept confidential, as a matter of good ethical practice as well as under any applicable legal agreements. Organisations are also not permitted to engage in discriminatory or anti-competitive behaviour in most countries, a principle that also applies to their use of data and data sharing. As data and accompanying analytic tools involve human decision-making, while it is not necessarily possible to remove bias from data sets entirely, it would help if there is greater transparency as to the nature and sources of that data, along with greater accountability from data service providers as to the basis on which such data has been gathered and processed. Organisations can also refer to IMDA's **Model AI Governance Framework** for more information.

Security and Data Integrity

Security and Data Integrity refers to the implementation of measures and mechanisms designed to securely protect and safeguard information and data to enable a secure environment for data sharing.

By seeking to identify and agree on relevant security protocols in the context of the proposed data sharing partnership with the data partners and making security integral to the design of devices, applications and systems (by reference to recognised security standards), this can provide assurance that the data shared is secured and protected adequately.

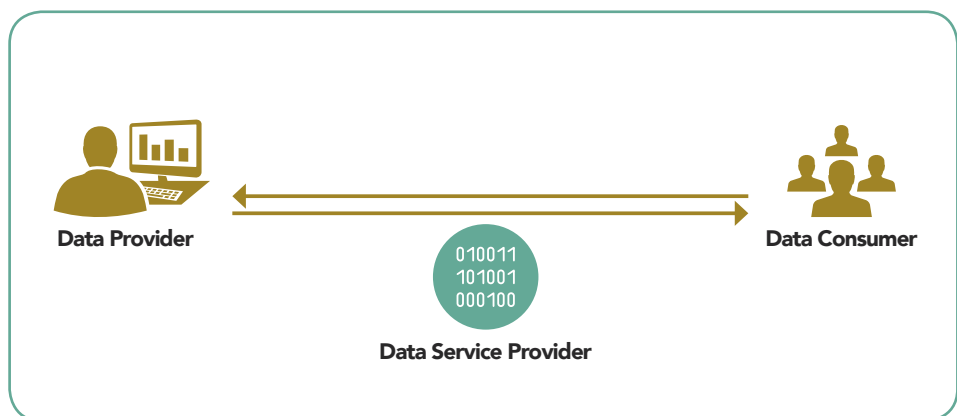
For example, the requirement for security requirements will vary according to the type of data that is being shared, and the way in which the system and programme operates. The security requirements for a blockchain-based programme will differ substantially from those applicable to server-based architectures. The key considerations are:

- a** metrics to determine risk and mitigation protocols;
- b** best practice encryption methods on communication channels, data transfer pipelines, data and storage spaces;
- c** best practice access control and management mechanisms to administer rights and privileges given to privileged users, marketplaces and consumers; and
- d** tools to monitor in real-time the integrity of the network, systems and end-user devices.

APPENDIX II: DATA SHARING MODELS – EXAMPLE SCENARIOS & CASE STUDIES

Bilateral

The simplest form of direct data sharing between a Data Provider and Data Consumer is illustrated in the figure below. The parties may engage directly with Data Service Providers throughout the lifecycle of the data, for example, to manipulate, cleanse or organise the data. However, the data sharing partnership remains directly between Data Provider and Data Consumer as the Data Service Provider is not contributing data.

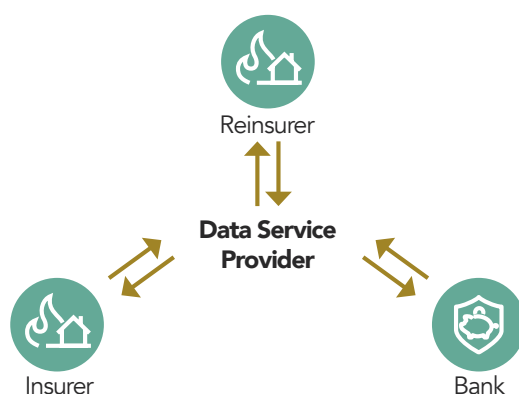


A bilateral data sharing model is also possible in the scenario where the Data Service Provider facilitates the data sharing by matching the Data Provider and Data Consumer's data sharing requirements. In this scenario, this is considered bilateral data sharing as the Data Service Provider does not contribute data for sharing.

Multilateral

When three or more parties make data available to an access-managed data pool for a common objective, each can act as a Data Provider and/or Data Consumer, depending on the circumstances. An agreed governed data exchange workflow and common legal contract can be implemented to facilitate the data exchange and help build trust between data sharing partners.

Case Study: Multilateral data partnership facilitated by Data Service Provider, providing a platform



Using a hybrid cloud-based data governance platform, the Data Service Provider facilitates the sharing of data between three participants for the purpose of fraud prevention.

The parties each take on the role of Data Provider and Data Consumer to share data for the purpose of fraud prevention.

To ensure that the parties are able to share data in a secure and legally-compliant manner, the Data Service Provider facilitates the exchange by:

- defining the scope of data partnership and collaboration between the parties;
- implementing a common legal framework for the data exchange which defines the data licence terms, including the type/category of data that may be extracted, the permitted use and commercialisation of the data, and the enforceability of the licence; and
- implementing a governed exchange workflow to facilitate data sharing and analysis, utilising risk assessment and control mechanisms to manage risk and a flexible data asset licensing framework to provide access to agreed subsets of data and algorithms.

Other ancillary services related to the data sharing include:

- conducting due diligence to ascertain whether each party has sufficient data quality, appropriate risk mitigations and safeguards have been put in place;
- preparing, cataloguing, cleansing and curating the data; and
- providing data governance and risk education and training.

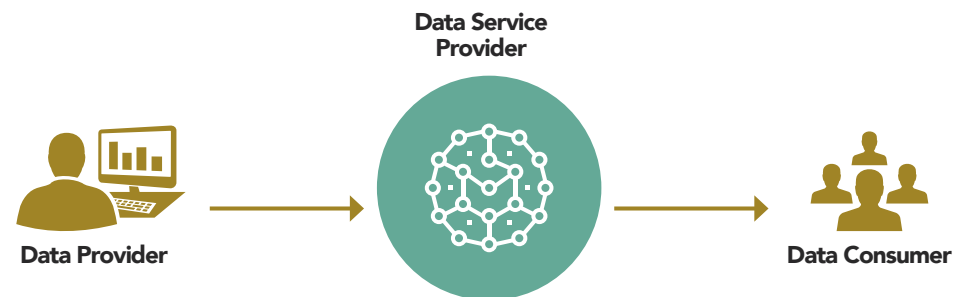
The sharing of data in this example does not always require data to be exchanged, as it may also be accessed virtually without any movement of data taking place.

In this example, the Data Service Provider continues to use audit features and egress checks to monitor the conditions under which data is being shared to ensure that the insight and output is consistent with the agreed data license. At no point is a copy of the data created, nor retained. Data collaboration is enabled with no loss of control, under a flexible framework of control.

Decentralised

New technologies have enabled more sophisticated data sharing strategies and models. “Decentralised” solutions such as distributed ledger technology are enabling new data exchange models, marketplaces, as well as services such as counterparty due diligence, data verification, security and certification, contracting and governance.

Case Study: A decentralised marketplace model that illustrates how the collective computing and consensus/incentives mechanisms of a blockchain community



Decentralised marketplaces have the capability to incorporate broad functionality, and the ecosystem continues to grow. To engender trust, such marketplaces aim to offer the following:

- To operate as a decentralised marketplace and provide a marketplace for other Data Service Providers to provide services to Data Providers and Data Consumers
- To use incentivisation built-into the network and protocols to provide better services and tools
- To use the community to provide the framework for data validation, storage, network, Graphical User Interface (“**GUI**”), discovery, compliance and pricing
- To leverage open source development to facilitate the sharing of data
- To operate without taking control of the data or storing the data
- To use decentralised technology to allow for technically verifiable, transparent data exchange among participants
- To provide traceability and transaction history



LEGAL AND REGULATORY CONSIDERATIONS



APPENDIX III: RESTRICTIONS AND RULES ON DATA SHARING

Laws and Regulations

For business data, other legislations may also contain provisions which impact organisations' data sharing activities.

Organisations exploring data sharing with cross-border or regional elements should take a dynamic approach to monitoring local, regional and global data protection and other data-related legislation.

For personal data, legislation (such as Singapore's PDPA) provides a framework of rules and restrictions for the handling of personal data in areas relevant to data sharing such as the storage, transfer and processing of data. Legislation often delegates authority to institutions with responsibility for supervising a particular sector, industry or category of data, such as the PDPC in Singapore.

Organisations exploring data sharing involving processing personal data in Europe, targeting European goods and services, or monitoring the activities of European citizens online, should also note compliance with Europe's General Data Protection Regulation ("**GDPR**"). They may wish to refer to the UK's Guide to the GDPR, which was created by a public and private sector working group for the National Health Service, social care and partner organisations on how healthcare organisations should prepare for changes to data protection law.

Guidelines

Guidelines can also have legal effect over a particular category of organisations, particularly those within regulated sectors. For example, outsourcing regulations typically impose restrictions on the ability of organisations to subcontract their responsibilities to third parties. An example of this is the MAS' Guidelines on Outsourcing as well as the ABS' OSPAR Guidelines.

Legal Agreements

Legal agreements, usually in the form of contracts put in place between data sharing partners, also provide a binding framework of rules and restrictions around specific data sharing use cases or projects. These help to build trust by clearly setting out in writing the purposes of the data sharing arrangement, while also helping to ensure accountability for the obligations of each data partner.

In a multilateral or decentralised data sharing context involving Service Providers, they can build trust by implementing a legal framework for data sharing which defines the data licence terms, including the type/category of data that may be extracted, the permitted use and commercialisation of the data, and the obligations of the participants.

Rights to Share Data

Data Providers should clearly state their rights in the data that is being shared along with any related materials and to consider including intellectual property ownership and licensing clauses in their data sharing agreements. For example, a Data Provider may have the right to share data as a result of having developed that data itself (e.g. in the creation of a database) or obtained a licence from a third-party owner to re-distribute the data to the Data Consumer.

For Data Consumers, where any materials such as hardware, software or other documents are being supplied by the Data Provider along with the data, Data Consumers should be aware that a Data Provider may seek to reserve their intellectual property rights in those materials also. Data Consumers may consider including contractual safeguards in the form of warranties provided by the Data Provider, that the data does not infringe the intellectual property rights of any third parties.



APPENDIX IV: USEFUL SOURCES OF WORLDWIDE DATA RULES AND GUIDANCE

The following sets out some useful worldwide rules and guidance in relation to data. These include legislation, principles, frameworks and sector-specific guidance, each with varying application and legal status.

1.	Singapore Personal Data Protection Act 2012 (Act No. 26 of 2012)	Singapore
2.	Singapore Cybersecurity Act 2018 (Act No. 9 of 2018)	Singapore
3.	IMDA Data Protection Certification Trustmark Certification Criteria	Singapore
4.	Personal Data Protection Commission Guide to Anonymisation	Singapore
5.	Monetary Authority of Singapore Guidelines on Outsourcing Risk Management	Singapore
6.	Monetary Authority of Singapore Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector	Singapore
7.	Association of Banks Singapore's Outsourced Service Providers Guidelines	Singapore
8.	Bank Negara Malaysia Policy Document on Outsourcing	Malaysia
9.	Malaysia Personal Data Protection Act 2010 (Act 709)	Malaysia
10.	Vietnam Law on Cybersecurity 2019 (No. 24/2018/QH14)	Vietnam
11.	Thailand Cybersecurity Act 2019	Thailand
12.	Government Regulation No. 82 of 2012 Concerning the Electronic System and Transaction Operation	Indonesia
13.	Hong Kong Monetary Authority SA-2 Supervisory Policy Manual on Outsourcing	HongKong
14.	California Consumer Privacy Act of 2018	USA
15.	Australian Computer Society Data Sharing Frameworks Technical White Paper	Australia
16.	Australia Privacy Act 1988 (Act No.119, 1988)	Australia
17.	EU General Data Protection Regulation (Regulation (EU) 2016/679)	EU
18.	European Commission Study on Data Sharing Between Companies in Europe	EU
19.	National Health Service General Data Protection Regulation Guidance	UK
20.	EU-U.S. Privacy Shield (2016)	EU and USA
21.	Asia-Pacific Economic Cooperation Privacy Framework (2005)	APEC
22.	Organisation for Economic Co-Operation and Development Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013)	OECD
23.	The FAIR Guiding Principles for Scientific Data Management and Stewardship	NA



APPENDIX V: CONSIDERATIONS FOR DATA SHARING AGREEMENT

The following are some legal templates for reference. The templates may not be all-inclusive and there are other alternatives to these templates which the organisations may explore to adapt for their own use.

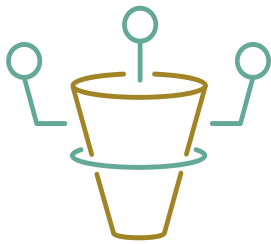
- Data Sharing Agreement
- Confidentiality Agreement
- Data Subject Consent (applicable to personal data)

The templates may be found at

www2.imda.gov.sg/programme-listing/ai-data-innovation.



SHARING PERSONAL DATA



APPENDIX VI: CONSENT, DYNAMIC AND ITERATIVE CONSENT

Consent

Under the PDPA, organisations must notify the individual of the purposes of the collection, use and disclosure of his personal data, during or before collecting the personal data, and obtain his or her consent. If an organisation intends to share the personal data for a different purpose from the original purpose for which consent had been obtained, the organisation must inform the individual of the new purpose and obtain fresh consent from the individual, unless an exception applies.

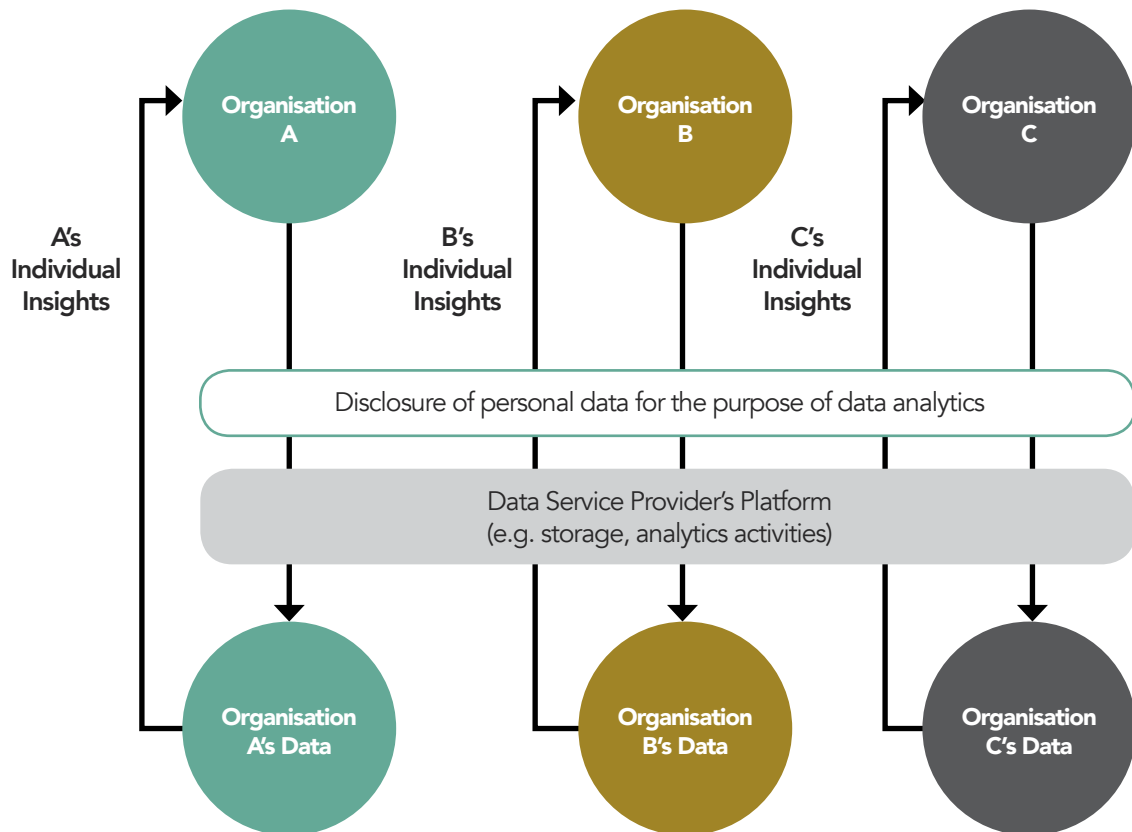
Example 1



- As Organisation ABC wants to share the data with Organisation XYZ for a new purpose, ABC must notify the individuals of the new purpose and obtain their consent.⁶
- If there are any potential risks to the individuals as a result of sharing the personal data, Organisation ABC should highlight these risks to the individuals when obtaining their consent.
- Organisation ABC must allow the individuals to withdraw their consent if they no longer want their personal data to be shared for this purpose.

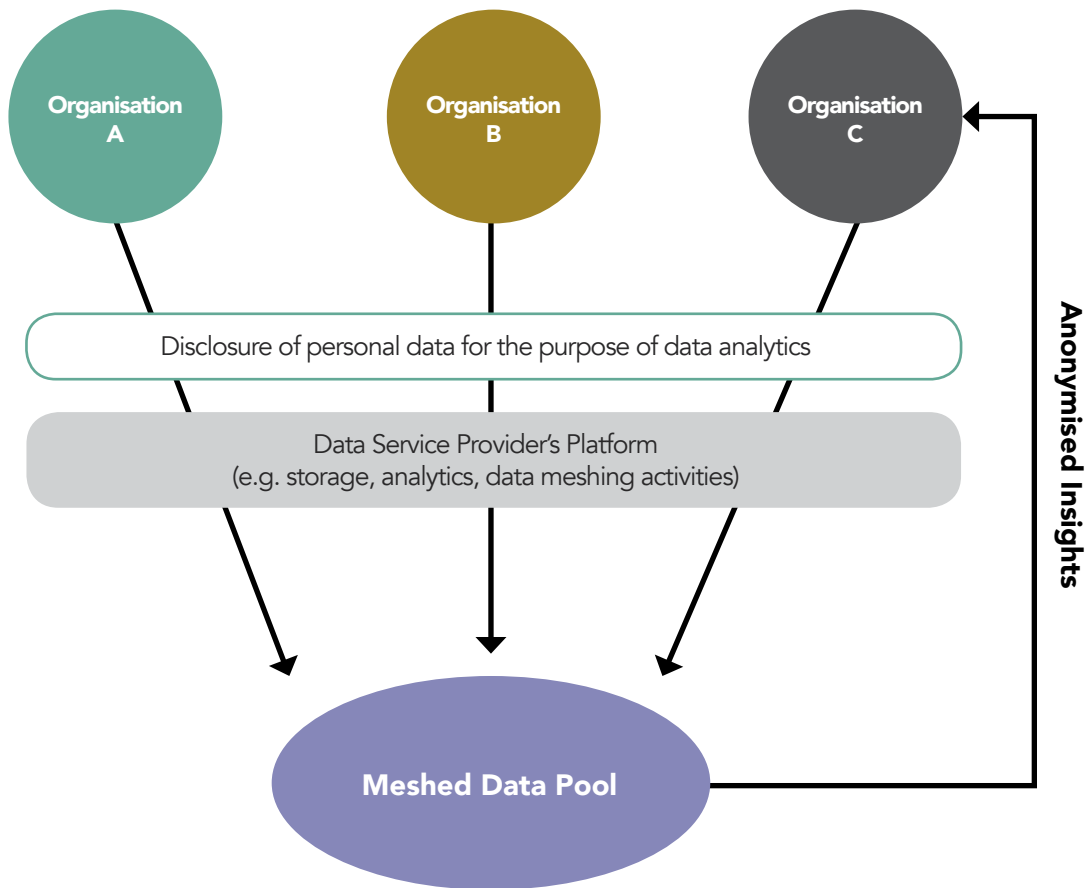
In the context of data sharing, especially for activities like big data analytics, it can sometimes be challenging for organisations to determine the purposes for sharing data at the outset, and whether fresh consent is required for the sharing. The following examples provide an illustration of when fresh consent should be obtained.

⁶ If the organisation intends to send a message to a Singapore telephone number to obtain consent for marketing purpose, this would constitute a specified message and the organisation must also ensure compliance with the Do Not Call Provisions of the PDPA.

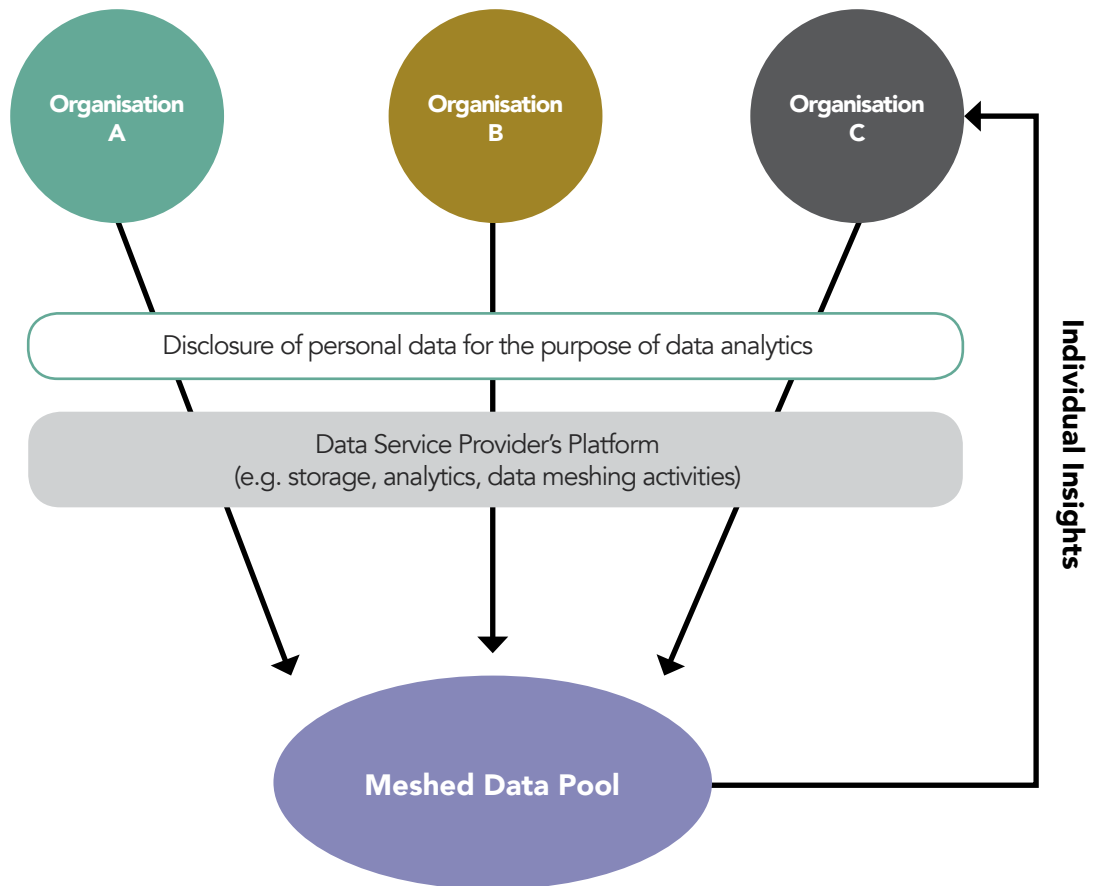
Example 2

- Organisations A, B and C each wants to carry out its own data analytics on personal data in its possession. Each organisation has obtained its customers' consent to use the personal data for its own data analytics.
- Activities such as storage and analytics of each organisation's own data performed in the Data Service Provider's platform would likely fall within the purpose of data analytics, and no additional consent is required for such activities.

Example 3



- In addition, Data Service Provider, which is acting on behalf of A, B and C, conducts analytics on datasets provided by A, B and C. Anonymised insights are then derived from the meshed data pool and can be extracted by any organisation using the platform.
- In this example, only anonymised insights will be shared with C. A's and B's personal data stored on Data Service Provider's platform will not be disclosed to C.
- Since insights generated are anonymised, it is no longer personal data. Hence, additional consent is not required for the sharing of anonymised datasets or insights with other organisations.
- For data to be considered anonymised, organisations have to ensure that there is no serious possibility that an individual can be re-identified. For more information, please refer to the **Advisory Guidelines on Selected Topics, Chapter 3 on Anonymisation**.

Example 4

- In contrast, if A wants to share personal data with C for C's data analytics purposes, A will have to obtain fresh consent.
- This scenario is similar to the preceding scenario, except that individually identifiable insights and analysis (instead of anonymised insights) would be derived.
- By extracting insights in identifiable form, data from Organisation A is being disclosed to Organisation C, albeit indirectly via Data Service Provider.
- Consent obtained by Organisation A for the purposes of its own "data analytics" cannot extend to the analytics activities of Organisation C. As such, initial consent obtained by Organisation A would only apply to its own data analytics activities, and fresh consent must be obtained for Organisation A to share the data in identifiable form to Organisation C.

Dynamic and Iterative Consent

Clear and specific consent obtained at the start of a relationship with the individual may not always be able to cater for all future purposes, especially in the current landscape where changing business models and new technologies influence the way organisations collect, use or disclose personal data.

If organisations need to obtain fresh consent for new purposes from time to time, they should consider adopting innovative processes and methods to comply with the consent requirement under the PDPA.

For instance, a dynamic approach to obtaining consent could be implemented. Instead of a one-time compliance tick-box, consent-taking can be an ongoing and actively managed choice, with granular options offered to the individuals at various “touch-points”. Such processes could be applicable whether the collection is taking place via an online platform, or offline in-person. This allows the same set of personal data to be used (or reused) with the knowledge and consent of the individuals whenever the purposes of collecting, using or disclosing the personal data change. Individuals, in turn, will have more control over their consent preferences (i.e. individuals can choose to give or withdraw their consent), and are more likely to make better-informed choices as their consent is being obtained at appropriate junctures.

If there are any risks or implications for the individual as a result of sharing the personal data (e.g. if the personal data contains sensitive information or the sharing could adversely impact the individual), the individual should be informed about the possible risks and implications. In general, organisations should set the default as “not-to-share”, and allow individuals to opt in to the data sharing.

Example: Dynamic Consent

Objective:

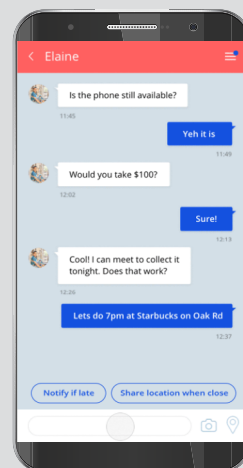
Enable individuals to share personal data (in this instance, location data) intuitively in social apps (e.g. chat groups) when meeting up, depending on strength of relationship.

Design Features:

For close friends: **Automatic sharing** of location information via mini-map, pin-pointing an individual's location.

For acquaintances: **Consent is sought** to either disclose ETA and location only when in close proximity or to send a simple notification to the other party.

Extracted from Singapore Design Jam (Nov 2018), co-hosted by IMDA and TTC Labs





APPENDIX VII: EXEMPTION UNDER THE PDPA

The PDPC is permitted, with approval of the Minister, by order published in the Gazette, to exempt any person or organisation, or any class of persons or organisations, from all or any of the provisions of the PDPA, subject to specified terms and conditions. Organisations that wish to apply for exemption from any provision of the PDPA should visit the PDPC's website for more information.

Exempted DSAs

When sharing personal data, organisations should generally rely on consent, or one of the applicable exceptions to share the data without consent. Nonetheless, there may be circumstances where the sharing of data is not likely to have any adverse impact on the individuals, or where there is a need to protect legitimate interests and the benefits for the public (or a section thereof) outweigh any adverse impact to the individuals.

This section sets out the considerations and criteria for applications to the PDPC for organisations' DSAs to be exempted from one or more obligations under the PDPA on a case-by-case basis. The criteria for the PDPC to consider a DSA exemption application are explained in the following paragraphs.

Criteria for DSA application

Sharing with a specified group for a specified period of time;

For defined and specific purposes; and

Not likely to have adverse impact to the individual, or the benefits to the public outweigh and adverse impact to the individual.

Firstly, personal data shared under the DSA must be with a specified group of organisations for a specified period of time. A specific group of entities or individual entities which the DSA will apply to must be specified in the application. After an exemption is granted, if additional organisations need to be added to the DSA, approval must be sought from the PDPC.

Secondly, the purposes of the DSA must be defined and specific. The data shared under the DSA has to be for well-defined purposes that are specific. For example, the sharing of data under a DSA for the purposes of social research would likely be too broad a scope.

Thirdly, the sharing must not be likely to have any adverse impact on the individuals, or there are legitimate interests and the benefits to the public (or a section thereof) that outweigh any foreseeable adverse impact to the individuals. The PDPC may consider exempting the DSA if the arrangement falls under any of the following two circumstances:

1. Notification and Opt-Out

- Sharing for such purposes is not likely to have any adverse impact on the individuals
- Sharing is not for the purpose of direct marketing

2. Legitimate Interests

- Obtaining consent for the purposes may not be desirable or appropriate
- Benefits to the public (or section thereof) from the sharing clearly outweigh any adverse impact or risks to the individuals

DSAs that are exempted from any PDPA obligation will be published in the Gazette, as required under the PDPA.

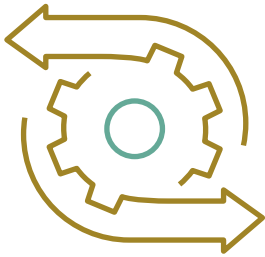
Terms and conditions will be imposed on the organisations under the DSA, including the requirement to conduct a data protection impact assessment to assess the risks and impact to individuals of the intended sharing, and implement the necessary measures to mitigate and address these risks. Depending on the specific circumstances, the following terms and conditions may be imposed:

- a** notify individuals of the purposes of the intended sharing and provide a reasonable time period for the individuals to opt out prior to the proposed sharing;
- b** give effect to any requests to opt out within the time period or any withdrawals of consent for the sharing of personal data under the DSA; and/or
- c** disclose reliance on legitimate interests (e.g. through data protection policy) and make available a document justifying the reliance on legitimate interests for the sharing of the personal data.

Organisations that meet the aforementioned criteria can submit an application for exemption of a proposed DSA to the PDPC. In general, it would be unlikely for the PDPC to grant an exemption for a proposed DSA if the organisations can rely on other alternatives to share personal data without consent (e.g. exceptions under the Second, Third, or Fourth Schedules to the PDPA, or provisions under any other written law).



TECHNICAL AND ORGANISATION CONSIDERATIONS



APPENDIX VIII: TECHNICAL DELIVERY MODE FOR DATA SHARING

Wire Transfer

This mode of data transfer typically involves a fibre-optic hardware cable – for instance a LAN cable or Ethernet cable – directly connecting two data storage sites. A key advantage of this transfer method is its ability to transfer large amounts of data at high speeds in a secure, efficient and continuous manner. This method is therefore suitable for Data Providers sharing large volumes of data, for example, the continuous sharing of real-time traffic data in Singapore over a period of six months. However, the installation of physical cable wires can be tedious and cost ineffective if the data transfer is short-term or over a singular occurrence.

Removable Storage Media

Data can be stored and retrieved either permanently or temporarily through a device such as an external hard disk drive or universal serial bus (“**USB**”) flash drive. This presents an appropriate mode of transfer for relatively small data packages. This can be a viable data transfer method for non-sensitive data especially since these devices are cost-effective and portable.

Storage media devices also allow security to be managed separately at the data endpoints and on the media device, making it more challenging for hackers to gain access to the information unless the device is physically stolen or accessed from the data endpoints. However, these devices are unable to carry large volumes of data and may have compatibility issues with systems. They may also carry viruses that can take down systems that expose themselves to them. An example of a suitable use of storage media for data exchange would involve a one-time transfer of shopper basket details.

Wireless

This data delivery model typically involves setting up a wireless network and connecting devices to that network without any hardware cable material. Wireless transfer technologies include Bluetooth, UWB, Wireless LAN, Wi-Fi and ZigBee, which all provide an easy way to set up a connection and sync two devices quickly. The differences between these protocols lie in the range, power consumption and intended use.

Relative to many other delivery models, Wi-Fi transfers can offer a higher transfer speed and better security. A key advantage of Wi-Fi networks is that the user can move around freely within the area of network access as opposed to a device that is connected via wires. Additionally, a Data Provider or Data Consumer who wishes to send or retrieve information across multiple devices can connect all devices to the network simultaneously. That said, the transfer speed and volume of Wi-Fi networks are not comparable to wire transfers and are generally less secure against the threat of external parties stealing bandwidth.

Remote Access/ VPN

A Virtual Private Network ("**VPN**") uses a network connection to enable users to remotely access data on devices or servers that are connected to the network at the time. A VPN is a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed through some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis.

Remote access VPNs are used to connect individual users to private networks with each user employing a VPN client and therefore are a much safer alternative than less secure networks such as the Internet. Once a user is connected, a software encrypts the traffic before delivering it over the Internet. The VPN server located at the edge of the targeted network then decrypts the data and sends it to the appropriate host inside the private network.

Since a server connected to a VPN network can be remotely accessed from any location around the world, this method of data transfer is suitable for cross-border instances of data exchange. A VPN network is also ideal in transferring files over multiple instances incurring only a one-time configuration cost. However, VPN data transfer speeds are very slow given that information has to be first encrypted before being transferred and subsequently decrypted. An illustrative example would be the Singapore and Malaysian governments exchanging road traffic images on the Causeway in order for both parties to manage traffic congestion.

Object Storage Accessible by URL/ SFTP

An object storage mechanism refers to a computer data storage architecture which manages data as objects, unlike a block storage architecture which structures data as blocks with a maximum length. Typically, each object includes the data itself, metadata and a globally unique identifier. Object storage services offer Internet-scale, high-performance storage platforms which are reliable and cost-efficient; they also preserve data durability.

An object storage architecture can store an unlimited amount of unstructured data of any type, including analytic data and rich content such as videos and images. For its capabilities in consistency, durability, customisable metadata and encryption, it has been greatly adopted and used by popular cloud storage vendors such as AWS, Azure, Dropbox, IBM and Oracle.

Object storage allows their users to store and retrieve data directly from the Internet or from within a cloud platform, and access data over an Internet connection and object storage endpoints. These storage platforms are also typically elastic, allowing users to first start small and then scale seamlessly. Vendors typically offer customers a range of options to access data based on preferences and suitability to certain tasks.

Data Providers may share their data with a Data Consumer through Secure FTP ("**SFTP**") or a customised URL using an object storage platform. Alternatively, a cloud infrastructure may include a tool to create a temporary long, difficult-to-guess URL that can be used for a specified period to download objects without requiring further authentication or giving full access to the storage account. A Data Provider can share such a URL to a Data Consumer who can use the URL to download data with any compatible HTTP clients such as Firefox, or download the data via SFTP. Data sharing via object storage enables transfer of large volume of data and usually includes access control such as read-only access, Access Control List ("**ACL**") defined access and temporary access.

Data Service Providers which are able to secure the data pipeline from the Data Provider to the Data Consumer can provide a cloud-supported data exchange platform which enables the transfer of high volume data at high speeds. For example, AWS and Azure are well-established collaborative platforms where information is often shared between data partners.

Database Accessible by API

Application Programming Interface ("**API**") is a set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other services. It is not a remote server, but a part of the server that receives the requests and sends responses.

Depending on the nature of the sharing, in particular, whether the Data Consumer or Data Service Provider has administrative or aggregation type of access as opposed to viewing access, Data Providers can choose between an open or partner API structure. Public APIs (also known as open APIs) are interfaces designed to be easily accessible by external parties and the wider population across the Internet. Partner APIs, on the other hand, are a hybrid of open and private APIs that grant access to the backend functionalities of an application, typically not fit-for-purpose to users who want to merely view the application.

APIs are particularly useful for exchanges between smaller firms with limited technical capabilities which are unable to invest in comprehensive data management systems. Preliminary research by the EU Commission has also certified the vastly interoperable nature of APIs, allowing unrelated software applications to seamlessly exchange datasets and data streams.

In a notable instance of API use, Dutch navigation company TomTom derives most revenue from sharing data in the forms of maps and online services licensed to other companies via APIs. TomTom monitors the use of data, verifies any breaches of contracts, and takes rapid actions on cases of data misuse.

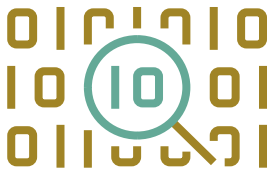
Email

Data Providers and Data Consumers can exchange data quickly, easily, and at no additional cost in the form of email attachments using third-party email providers such as Gmail, Outlook, and Apple Mail. In addition to built-in security measures, Data Providers, as email platform users, may choose to adopt further protection measures such as password protecting files and adding public key cryptography mechanisms. Apart from security considerations around email theft, a critical limitation of email exchange is its inability to support large files.

Distributed Ledger Technology

A distributed ledger is a consensus of replicated, shared, and synchronised digital data spread across multiple sites and users. It is an alternative to the typical centralised ledger-type architecture where a central authority has control over the shared information. Especially in situations where all partners are equal contributors to the shared information, a distributed ledger architecture eliminates a central authority and relies instead on each party's validation.

The blockchain is a typical example of this type of technology. The nature of the blockchain ensures that it is secure by design. Data sharing partners can therefore consider private blockchains as a supporting architecture to store, process, validate and authenticate information. However, blockchains cannot at the moment support large data files and data sharing partners requiring transfers of large datasets would require other forms of distributed ledgers. An example of this would be where a group of banks come together in a multilateral data sharing partnership and contribute to a singular ledger with each party's validation required for transactions.



APPENDIX IX: SECURITY MEASURES TO PROTECT DATA INTEGRITY

For Data Requiring Transit: Consider Cryptographic Measures

Encryption

Encryption refers to the process of encoding information to prevent unauthorised access. Encryption can be used in data sharing activities to protect stored or exchanged data from being accessed by an unauthorised party. There are two primary types of encryption – symmetric key encryption and public key encryption. Standards applicable to both forms of encryption are:

- a encrypted files should not be indexed;
- b certificates and private keys for recovery agents should be stored on separately secured media objects;
- c Federated Information Processing Standards Publication 140 ("**FIPS-140**") compliant encryption algorithms should be used;
- d secure channel traffic should be encrypted and signed; and
- e two forms of key recoveries should be available to users of the system.

In recent times, encryption has enabled the creation of useful applicators such as digital cryptographic signatures and cryptographic keys. Cryptographic keys designed with the public key encryption architecture gives each user two keys: one public key and one private. An example of how this might be used in a data sharing exchange would be: The Data Provider requests the public key of the Data Consumer, encrypts the intended data to be provided with the given public key, and sends the output to the Data Consumer. When the output reaches the Data Consumer, only the intended and authorised Data Consumer's private key will be able to decode the output – therefore that theft of information cannot occur without possession of the Data Consumer's private key.

Hashing

Hashing is a one-way digest function: it generates a string of a fixed length from a text using algorithms such as the MD5, SHA and SHA-2. These vary in sophistication with the SHA-2 as the current industry favourite as both an algorithm and a standard. A hash generated from a body of text varies widely with small variations in input and ideally makes it impossible to turn the hash back into the original text.

Unlike encryption, the reliability of hashing algorithms does not depend on access to an encryption key, and therefore eliminates the risks incurred when a key is stolen. Hashing is useful to store data items without necessarily reading them again, such as passwords and email addresses.

While hashing does not apply directly to data sharing activities per se, it is highly relevant in the secure storage of data. A worked example of a hash would be the secure storage of customers' email addresses. Once these email addresses have been hashed, the resulting unreadable hashes can be stored securely until they are "accessed" by running the hash again using the same email addresses to check that the same hash is generated.

Salting

On top of conventional hashing, salting can be applied for an additional layer of security. Salting refers to an environment where the output hash value is a combination of the intended stored value and an additional salt value. Salting is more relevant when the intended stored value is a common value such that guesswork can enable a computer to decode the hash. Salt values can be randomised and added to increase security around the hashed value.

Tokenisation

Tokenisation refers to the cryptographic process of substituting a sensitive data element with a non-sensitive element referred to as a token. This token has no exploitable or extrinsic value and simply serves as an identifying reference to map the original data to the token. This form of cryptography secures data in transit over the Internet as well as data at rest, and like encryption, is a form of data obfuscation technology.

While similar to encryption, tokenisation also features different strengths and weaknesses and depending on the particular security instance should be employed either instead of or in addition to encryption. For instance, since tokenisation is difficult to scale securely, it is less appropriate as a means of securing large databases. However, unlike encryption, it can preserve the integrity of different data formats without diminishing the strength of the security. Most significantly, given the reversibility of encryption, tokenisation does not allow reversal into original data. Additionally, tokenisation can be more appropriate than encryption where compliance requirements dictate that the original data must not leave the organisation, since encryption involves data leaving in an encrypted form.

For Data Required to Stay in Place: Consider Secure Computation Techniques

Homomorphic Encryption

While encryption and other cryptography methods can nevertheless expose data to leaking and misuse once decrypted, recent developments in homomorphic encryption and distributed ledger technology have allowed data to be completely secured against misuse, leakage or theft.

For example, homomorphic encryption enables algorithms to perform analytics or train AI models on unrevealed data – this unrevealed data will have its privacy intact throughout the computation process, with only the outputs from the computation revealed. This allows sensitive information such as personal data to be processed without being viewed or transferred, and is therefore a viable option for cases where data cannot be transferred from one party to another for regulatory reasons.

Given that data can therefore be encrypted throughout its lifecycle, it is safeguarded from malicious insider and outsider threats while in use, and by definition, avoid the risks associated with third-party Data Service Providers. In the context of data sharing, homomorphic encryption allows data to stay in place, and instead works by the Data Consumer sending its algorithms – which can themselves be encrypted – to a trusted execution environment or servers controlled by the Data Provider.

Multi-party Computation (“MPC”)

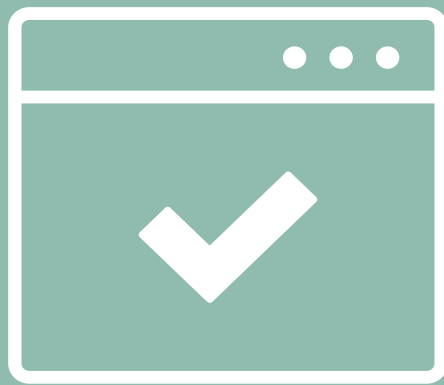
MPC is another secure computation technique growing in popularity. It enables multiple parties – each with private datasets and pre-determined queries – to jointly compute a function over their inputs while keeping those inputs private. While conventional cryptography seeks to conceal content, MPC involves concealing partial information about data while computing this data from many sources. Inputs – that is, shared or stored data assets – can therefore be used or analysed without being revealed to any of the parties involved in its use or analysis. MPC therefore allows organisation to collect data from each other for the joint benefit of larger data analytics, but without being able to access others’ inputs or reveal their own. In the context of data sharing, this allows parties to derive insights from larger, shared datasets without compromising the privacy of such data. For example, MPC was used by two Estonian government departments and a research agency to share and analyse over 10 million data points from university students in a way which passed vetting by the local Data Protection Agency.

For example, Microsoft Azure is an MPC service which protects the privacy and integrity of customer data and code when it is being processed in the cloud. This allows parties to confidently use cloud storage and processing as a means for data sharing, since their data and code remain opaque to the cloud platform. The principle behind this technology – that data can be securely and simultaneously computed – has led to the popularity of centralised databases being replaced by temporary links of data for analysis purposes. This distributed architecture model is discussed below.

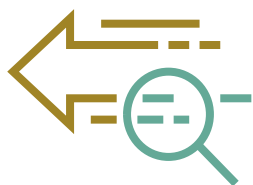
Security and Distributed Ledger Technology

When combined with secure computation, blockchain technology can open up a new realm of possibilities for data sharing by facilitating trusted data transactions. The elemental features of the blockchain – distributed consensus, a tamper-resistant ledger requiring digital signatures, and enforceable contracts – allow increased transparency and traceability and therefore foster trust amongst data sharing partners. For instance, a Data Provider may decide to sell or share sensitive data on the blockchain by stipulating through a smart contract various requirements regarding the identities of the Data Consumer and the approved use of the data.

Once a Data Consumer authenticates himself cryptographically and sends any required inputs to the smart contract, this smart contract will automatically execute by providing access to the data – or, where secure computation is used, to the Data Consumer's algorithm. Traceability through an audit trail in this transaction is provided by its being logged on the blockchain – in the case of a public protocol, this transaction and contract would be available for anyone (including competitors) to see. Where confidentiality is required, a permissioned ledger can be used with access given only to regulators and approved auditors.



OTHERS



APPENDIX X: DATA SHARING CHECKLIST – QUESTIONS TO CONSIDER

The following list of questions can be used to guide organisations in planning their data sharing activities:

Data Sharing Strategy

Establish Data Sharing Potential Of Own Data

1. What are the data assets and who are the potential stakeholders in the whole value chain or ecosystem that the organisation operates in?

Understand Potential Data Sharing Models

2. Is the organisation looking to obtain access to data from another (Data Consumer) or provide access to data to another (Data Provider)?
3. Is the sharing model bilateral, multilateral or decentralised?
4. How can one verify the identity of the participants (including Data Providers, Data Consumers and any Data Service Providers)?
5. Will Data Service Providers be engaged to facilitate the data sharing?

Legal and Regulatory Considerations

Determine If Data Can Be Shared

6. Will the data transfer be cross-border?
If so, are there any data-related laws or guidelines that may have impact on the data sharing?
7. Is the data within a special category of data subject to additional rules and restrictions on its transfer? Are there any other restrictions that apply to the data or its transfer or access? Does the nature of the transfer create legal, regulatory or other obligations on the Data Consumer?
8. How can one ensure that the Data Provider has the right to license the data and has not contravened any existing obligations or rights by providing the data?
9. Who owns any intellectual property rights relating to the data being shared or the results from the data sharing project?

Company Policies

10. Are there any rules of participation for data sharing groups or consortiums that include onerous terms or which operate contrary to your corporate practice or policy?

Considerations for Sharing Personal Data

11. Where personal data is involved, are the permissions, notices and consents provided sufficient for the intended purpose?

Establishing Data Sharing Agreement

12. If the Data Service Provider is involved, do the applicable terms sufficiently protect the exposure of the Data Provider and Data Consumer to losses arising from participant breaches, general enforcement of contract and intellectual property rights?

Legal and Regulatory Considerations

Determine If Data Can Be Shared

13. Do the terms sufficiently describe the warranties attaching to the data, for example, whether the data is provided 'as-is' or whether there are warranties relating to fitness for purpose, accuracy or viruses?

Grant of License

14. How can data partners ensure that the data is being used in accordance with the licence terms?
15. Where a Data Service Provider facilitates a direct contractual relationship with a data partner, how can the Data Provider ensure that the risks arising from the indirect relationship are effectively mitigated and any losses arising are recoverable?

Resolving Disputes

16. Is the jurisdiction and governing law of the applicable terms clear and have appropriate dispute resolution methods been considered to ensure effective resolution of disputes and enforcement in any relevant jurisdictions?

Technical and Organisation Considerations

Prepare Data For Data Sharing

17. Will the original data be accessible (or only derivative data)? Is the data the minimum for the required purpose? Who requires access to the data?
18. What techniques are required to prepare or process the specific type of data identified?

Understand Technical Considerations for Data Sharing

19. What will be the technical model for data transfer/access and will it require any additional security?
20. How will the data be tracked and are there any procedures in place to monitor the use of the data from the date of the initial transfer?
21. How can you ensure that your organisation is protected against any unilateral changes/suspensions/upgrades made by Data Service Providers?

Operationalising Data Sharing

22. What additional data analysis is required after sharing has occurred?
23. What measures may be implemented to allow a Data Provider to monitor the use and disclosure of its data after exchange?
24. How can a Data Provider ensure a Data Consumer complies with its ongoing legal and regulatory obligations after the data exchange?
25. If the data sharing partnership is an ongoing relationship, is there any commitment to ongoing improvement of technology safeguarding the data and access to it?
26. Are there measures in place to implement the retention and disposal of data according to what is set out in the Data Sharing Agreement?



APPENDIX XI: COMMON RESOURCES USED IN THIS FRAMEWORK

Resources for Sharing Business Data		
Guide to Data Valuation for Data Sharing	Information on how organisations can determine the value of their data for sharing.	www2.imda.gov.sg/programme-listing/ai-data-innovation
Resources for Sharing Personal Data		
Guide to Basic Data Anonymisation Techniques	Information and examples on anonymisation concepts and techniques for personal data.	www.pdpc.gov.sg/og
Guide to Disposal of Personal Data on Physical Medium	Information on the disposal of physical medium (largely paper) containing personal data and examples of the different ways of disposal which organisations may consider adopting.	www.pdpc.gov.sg/og
How Can Your Organisation Dispose of Personal Data	Summary of good practices in both physical and electronic destruction of personal data.	www2.imda.gov.sg/programme-listing/ai-data-innovation
Guide To Securing Personal Data In Electronic Medium	Information and examples on good practices which organisations may adopt to further secure electronic personal data.	www.pdpc.gov.sg/og
Chapter 3 (Anonymisation) of the PDPC's Advisory Guidelines on the PDPA for Selected Topics	Information on how the PDPA applies to issues pertaining to anonymisation.	www.pdpc.gov.sg/ag



ACKNOWLEDGEMENT

We would like to thank the members and companies of the following organisations and workgroup who provided valuable inputs for the development of this Trusted Data Sharing Framework:

- Business Innovation Rights (BIR) Workgroup
- Business Software Alliance (BSA)
- SGTech

#SGDIGITAL

Singapore Digital (SG:D) gives Singapore's digitalisation efforts a face, identifying our digital programmes and initiatives with one set of visuals, and speaking to our local and international audiences in the same language.

The SG:D logo is made up of rounded fonts that evolve from the expressive dot that is red. SG stands for Singapore and :D refers to our digital economy. The :D smiley face icon also signifies the optimism of Singaporeans moving into a digital economy. As we progress into the digital economy, it's all about the people - empathy and assurance will be at the heart of all that we do.

BROUGHT TO YOU BY



Copyright 2019 – Infocomm Media Development Authority of Singapore (IMDA) and Personal Data Protection Commission (PDPC)

This publication gives a framework for considerations related to data sharing. The contents herein are not intended to be an authoritative statement of the law or a substitute for legal or other professional advice. The IMDA, PDPC and their members, officers and employees shall not be responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind as a result of any use or reliance on this publication.

The contents of this publications are protected by copyright, trademark or other forms of proprietary rights and may not be reproduced, republished or transmitted in any form or by any means, in whole or in part, without written permission.