GUIDE TO DATA SHARING

Revised 1 February 2018

TABLE OF CONTENTS

PART 1: INTRODUCTION

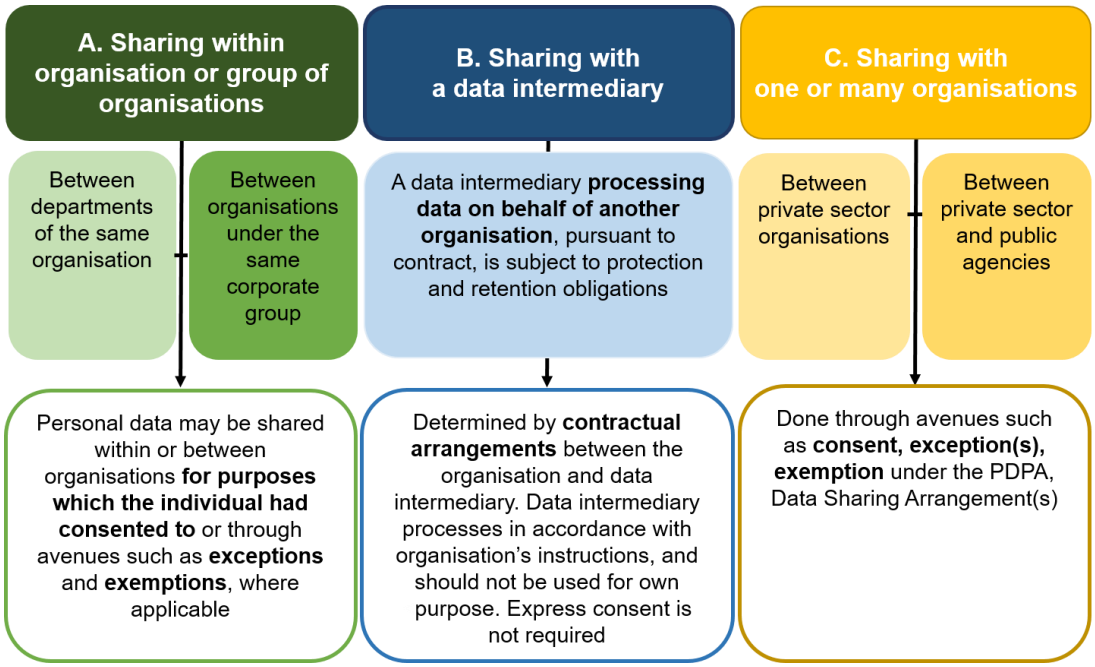
1.1 This guide explains how the Personal Data Protection Act 2012 ("**PDPA**") applies to the sharing of personal data within and between organisations.

1.2 As a Data Protection Officer, you may be asked to determine whether your organisation may share personal data and how it should do so. This guide aims to help you identify the appropriate approach for sharing personal data in compliance with the PDPA. The scenarios provided highlight certain aspects of the PDPA, but do not address every PDPA provision that may apply.

1.3 This guide is intended to be read together with the Advisory Guidelines on Key Concepts in the PDPA ("Key Concepts Guidelines"). Organisations are also reminded to ensure compliance with their obligations under other written laws.

WHAT IS 'DATA SHARING'

1.4 'Data sharing' refers to the use and/or disclosure of personal data[1] to one or more organisation(s) and the latter's collection of that personal data. Briefly, data sharing can occur in the various forms illustrated below.



[1] Under the PDPA, "personal data" means data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.

A. Sharing within the organisation or group of organisations

1.5 An organisation may share personal data within the organisation for purposes which the individual has consented to, or is deemed to have consented to (see section on "Consent" below for information on consistent purposes). For instance, an organisation's customer relations department may share personal data with its finance department for the purpose of administering customer requests for refunds of purchases. The organisation should also have internal policies to prevent misuse of the data, for example access controls to prevent unauthorised access, use and disclosure.

1.6 Likewise, organisations within the same corporate group may share personal data for purposes which the individual has consented to. Given that the organisations within the same corporate group are separate legal entities, the organisation sharing the personal data will have to ensure that the consent it obtained would cover the purposes of the disclosure. For example, hotels under the same hotel group may want to share personal data (e.g. the guest's special preferences) of guests who are members of the hotel group for the purpose of providing personalised hospitality services to their members. When one of the hotels in the group obtains consent from a guest who signs up to share such personal data with other hotels in the group for the purposes of providing personalised hospitality services, all the other hotels in the group can rely on that consent to collect, use and disclose the guest's personal data for those purposes.

1.7 Organisations should consider, among other things, the intended purposes of the sharing, as well as the potential benefits and risks to the individuals that may arise from the sharing. If organisations intend to share personal data without consent, they must ensure that a relevant exception or exemption under the PDPA applies. Exceptions to the requirement to obtain consent to share personal data may apply in certain circumstances (see section on "Exceptions" below). For example, there is an exception to allow for the disclosure of personal data without consent where it is necessary for any investigation or proceedings.

B. Sharing with a data intermediary

1.8 An organisation may share personal data with its data intermediary to process personal data on its behalf. The organisation should put in place a written contract for the data intermediary to process the personal data in accordance with the organisation's instructions. To ease business decisions on the outsourcing of operations, express consent is not necessary for an organisation to disclose personal data to its data intermediaries. However, the personal data should not be used by the data intermediary for other purposes without the consent of the individual. For more information on data intermediaries, please refer to the Key Concepts Guidelines.

1.9 A data intermediary 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. [2]

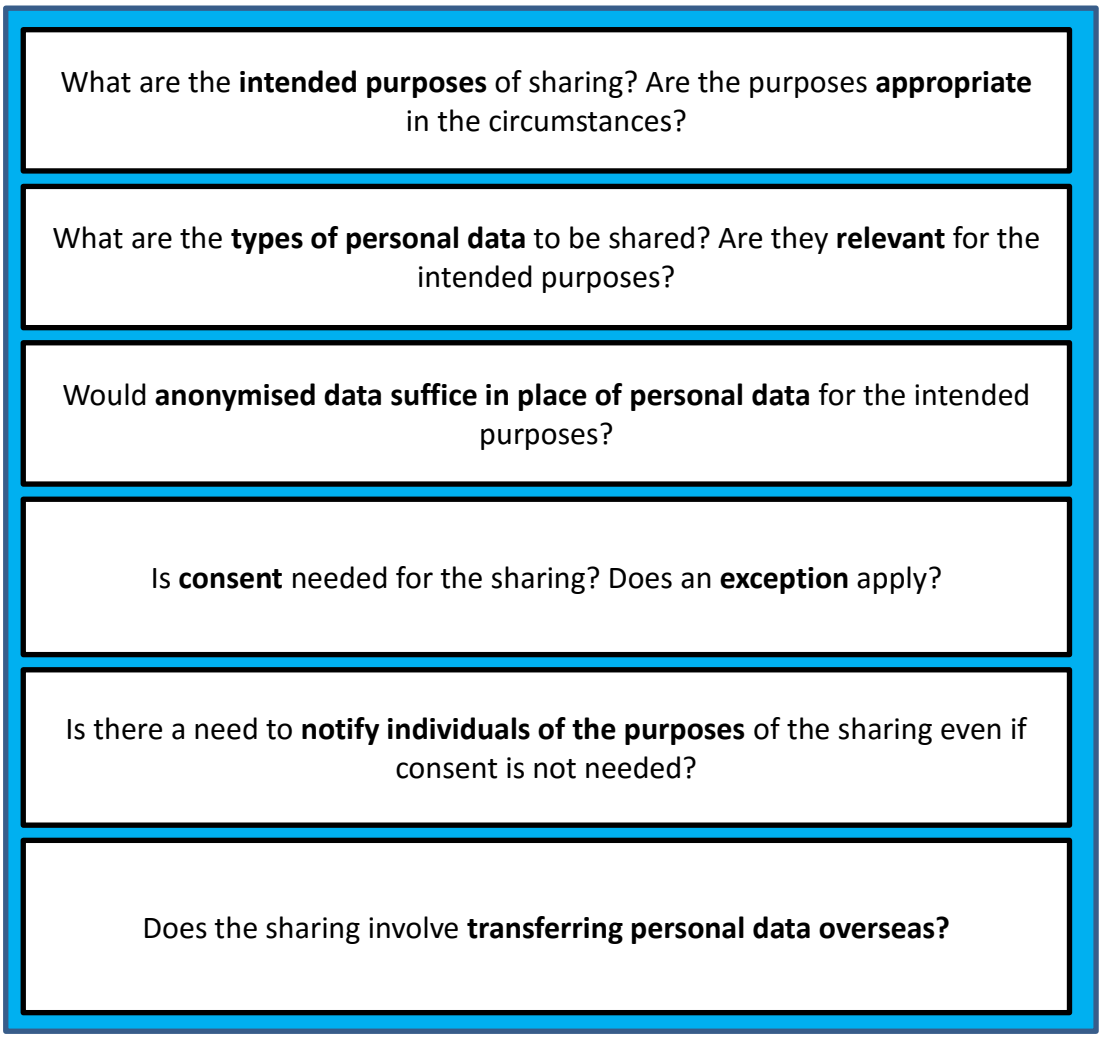
C. Sharing with one or many organisations

1.10 When deciding whether to share personal data with other organisations, the organisation should consider, among other things, the intended purposes of the sharing, as well as the potential benefits and risks to the individuals that may arise from the sharing. The following sections outline the key considerations and approaches for sharing personal data with other organisations in compliance with the PDPA.

[2] This is regardless whether the engagement of the data intermediary is set out in a written contract (or contract evidenced in writing).

PART 2: FACTORS TO CONSIDER BEFORE SHARING

2.1 Before deciding whether to share personal data, organisations should consider the following:



A sample list of questions, considerations for organisations intending to share personal data is provided in **Annex A**

A workflow process template is provided in **Annex B** which organisations can consider adapting

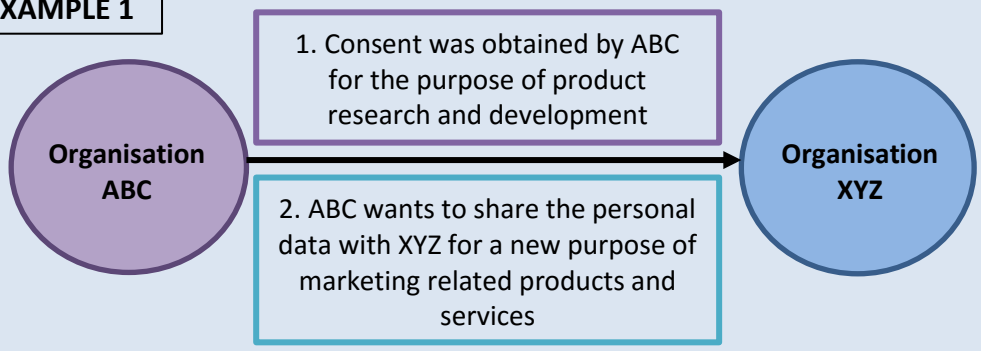
PART 3: THE "HOW" OF PERSONAL DATA SHARING

3.1 This section discusses the various approaches to sharing personal data under the PDPA.

CONSENT

3.2 Under the PDPA, the organisation must notify the individual of the purposes of the collection, use and disclosure of his personal data, on or before collecting the personal data, and obtain his 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. Organisations may wish to refer to the Key Concepts Guidelines for more information on the Consent Obligation.

EXAMPLE 1

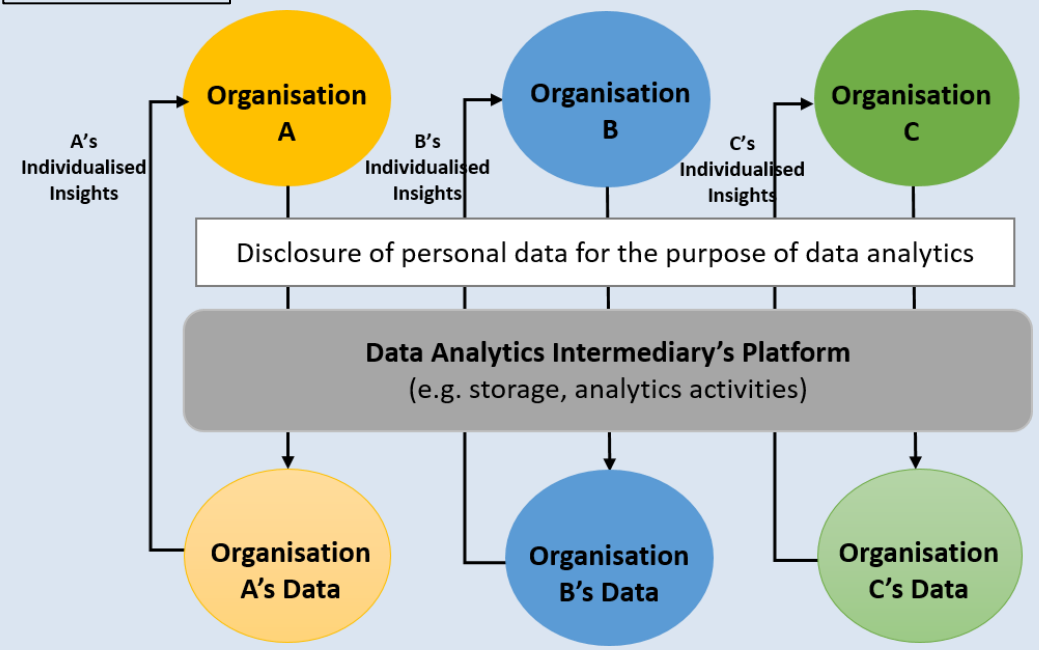


- As Organisation ABC wants to share the data with Organisation XYZ for a new purpose, ABC must notify the individuals of the new purpose and obtain their consent[3].
- If there are any potential risks to the individuals as a result of sharing the personal data, Organisation ABC should highlight these 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.

[3] 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. Please refer to the Advisory Guidelines On The Do Not Call Provisions at for more information: https://www.pdpc.gov.sg/legislation-and-guidelines/advisory-guidelines/main-advisory-guidelines#AG3

3.3 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.

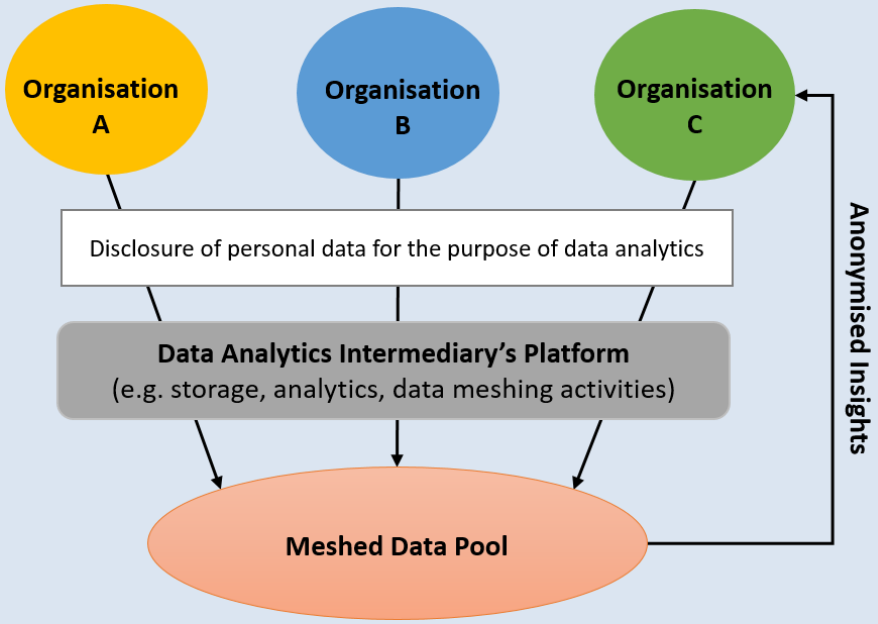
EXAMPLE 2



- 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 Analytics Intermediary's platform would likely fall within the purpose of data analytics, and no additional consent is required for such activities.

EXAMPLE 3



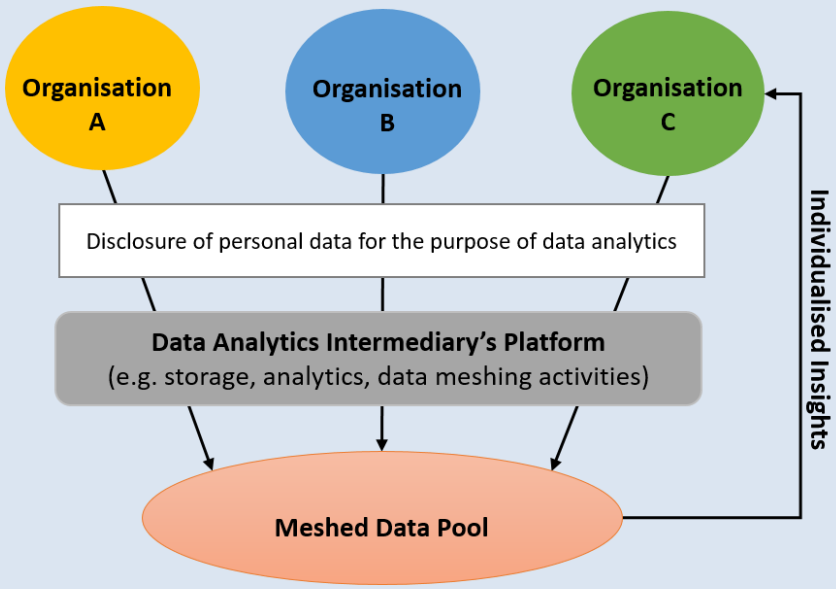
- In addition, Data Analytics Intermediary, which is acting on behalf of A, B and C, conducts analytics on datasets provided by A, B and C. ***Anonymised insights*** are then derived from the meshed data pool and can be extracted by *any* organisation using the platform.

- In this example, only anonymised insights will be shared with C. A's and B's personal data stored on Data Analytics Intermediary'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** for C's data analytics purposes.
- This scenario is similar to that illustrated in Example 3, 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 Analytics Intermediary.
- 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: methods and approaches

3.4 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.

3.5 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.

3.6 For instance, a dynamic approach to obtaining consent[4] could be implemented. Instead of a one-off compliance tick-box, consent-taking can be an on-going 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.

3.7 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 opt-out of any purposes or any further collection, use or disclosure of their personal data at any time.

3.8 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.

[4] "Dynamic consent…could be adapted to allow data subjects to be notified and review how their data is being used, whether for new purposes or shared with new actors", *See* L. Hutton and T. Henderson, *Beyond the EULA: Improving Consent for Data Mining*, in T. CERQUITELLI, D. QUERCIA, F. PASQUALE (EDS.), TRANSPARENT DATA MINING FOR BIG AND SMALL DATA (Volume 11) at 164.

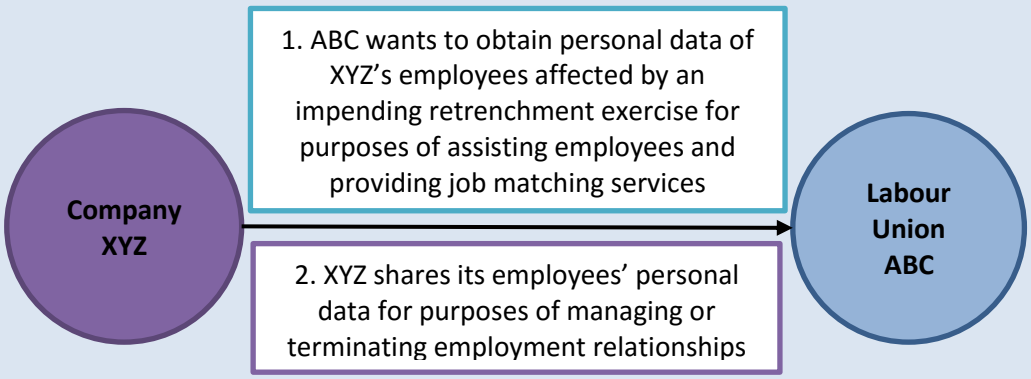
EXCEPTIONS

3.9 The PDPA sets out exceptions where organisations may collect, use or disclose personal data without consent.

3.10 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.

3.11 Organisations relying on exceptions from the consent requirement must still comply with other Data Protection Provisions (e.g. protection of personal data) when sharing the personal data. The following examples illustrate how exceptions may apply to the sharing of personal data.

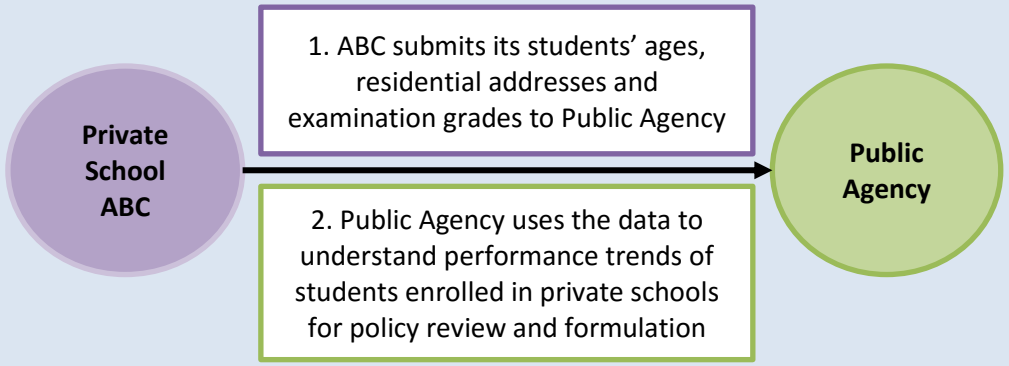
EXAMPLE 5



- 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.

EXAMPLE 6



- Private School ABC may share the personal data of its students to Public Agency for the purposes of policy review and formulation as there is an applicable exception under the Fourth Schedule of the PDPA.[5]

EXEMPTION UNDER THE PDPA

3.12 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[6] for more information.

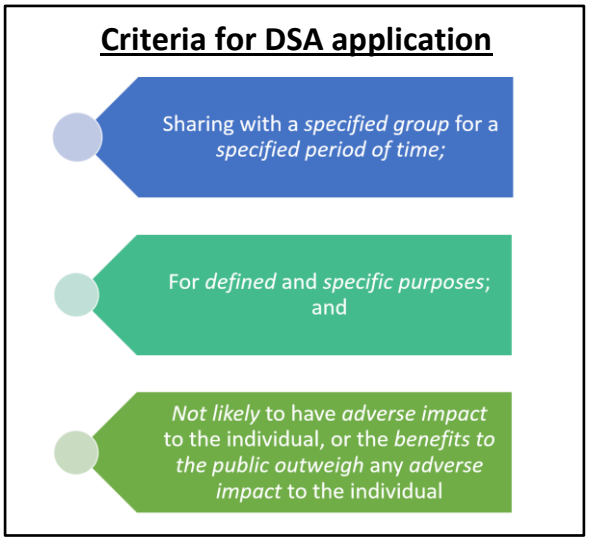
Exempted Data Sharing Arrangements (DSAs)

3.13 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.

[5] Paragraph 1(l) of the Fourth Schedule to the PDPA provides that an education institution may disclose without consent personal data about its current or former students to a public agency for the purposes of policy formulation or review.

[6] https://www.pdpc.gov.sg/legislation-and-guidelines/exemption-requests

3.14 This section sets out the considerations and criteria for applications to the PDPC for organisations' data sharing arrangements (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.



3.15 **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.

3.16 **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.

3.17 **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) 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 the 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**.

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

3.19 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:

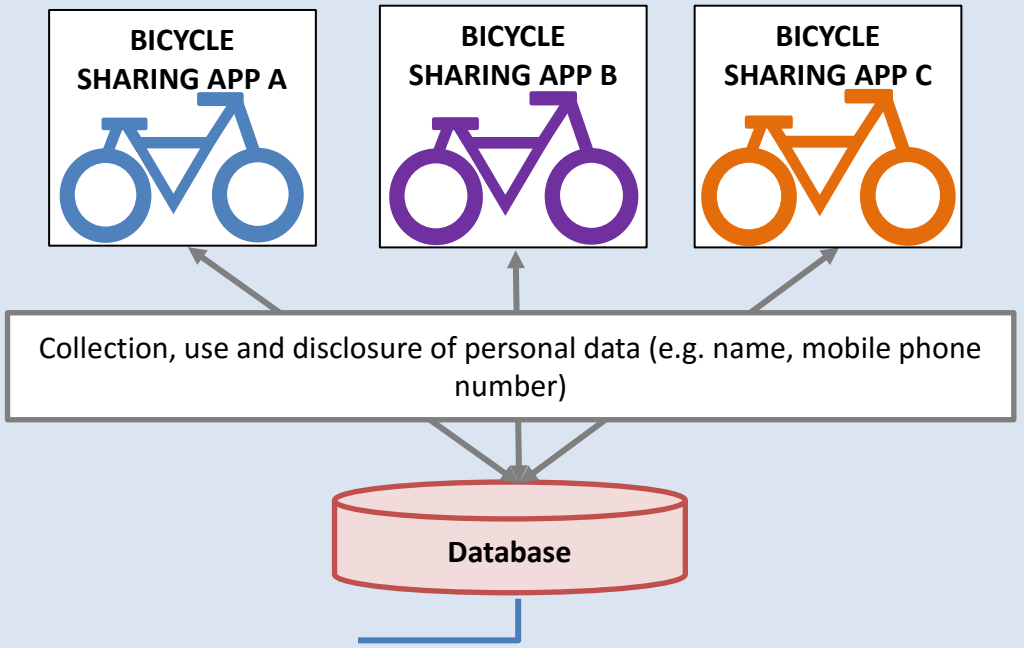
(a) To notify individuals of the purposes of the intended sharing and provide a reasonable time period for the individuals to opt-out prior to the proposed sharing;

(b) To 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) To 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.

3.20 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). Some examples of possible DSAs are illustrated below.

EXAMPLE 7



Secured database containing key particulars of users who had previously used or parked bicycles in an irresponsible manner.
Before allowing users to take the bicycles, bicycle sharing app companies may query the database and users who had previously used or parked bicycles irresponsibly would be flagged to the companies.

- 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 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.

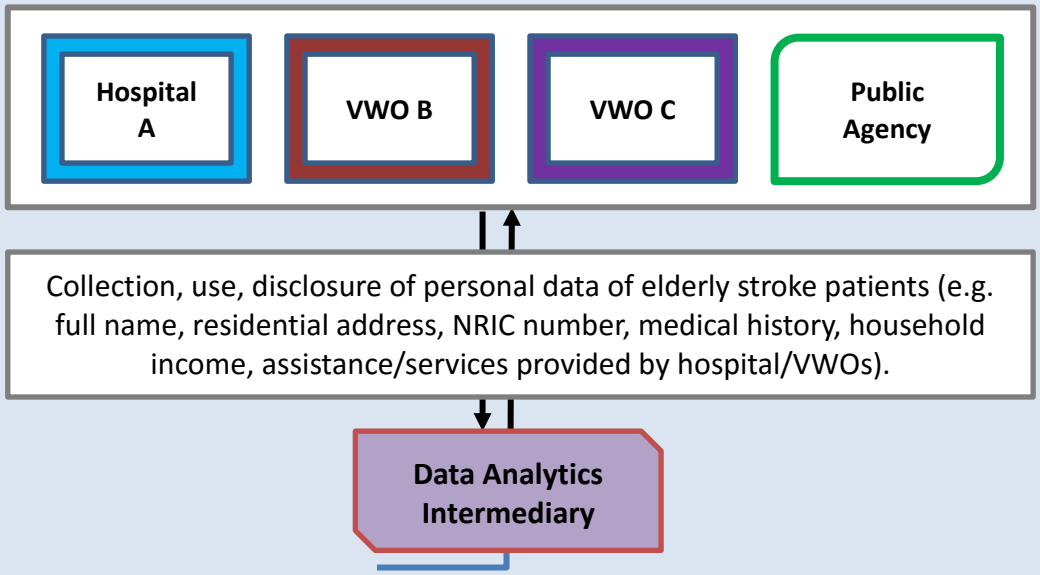
- Bicycle Sharing Applications A, B and C must conduct data protection impact assessments to assess the risks and impact of sharing the personal data, and implement safeguards and measures to mitigate such risks.

- 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.

EXAMPLE 8



Data Analytics Intermediary conducts analytics on behalf of the hospital/VWOs and public agency. Pooled data is used to deliver better personalised services, better individual assistance matching, and to gain general insights for policy making.

- A group of organisations consisting of a Hospital, two VWOs and a Public Agency decides to collaborate to share and pool data for the purposes of conducting data analytics to improve service delivery and ensure effective matching of assistance and outreach to elderly stroke patients. The VWOs intend to pro-actively reach out to the Hospital's patients to offer income assistance or social support, and the Public Agency would like to use the information to improve policy making and decide if these patients are suitable participants for smart wearables trials. These activities will ensure that services can be delivered more conveniently and expediently to potential beneficiaries. It was also assessed that the sharing is not likely to have any adverse impact on the individuals.

- The organisations may submit a proposed DSA to PDPC for an exemption from specific provisions of the PDPA to share the personal data. The organisations would be required to 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. They must also notify the individuals of the purposes of the sharing, and allow them to opt-out within a reasonable time period. Where possible, they should also give effect to any requests for withdrawal of consent at any time after the data sharing scheme has commenced.

END OF DOCUMENT

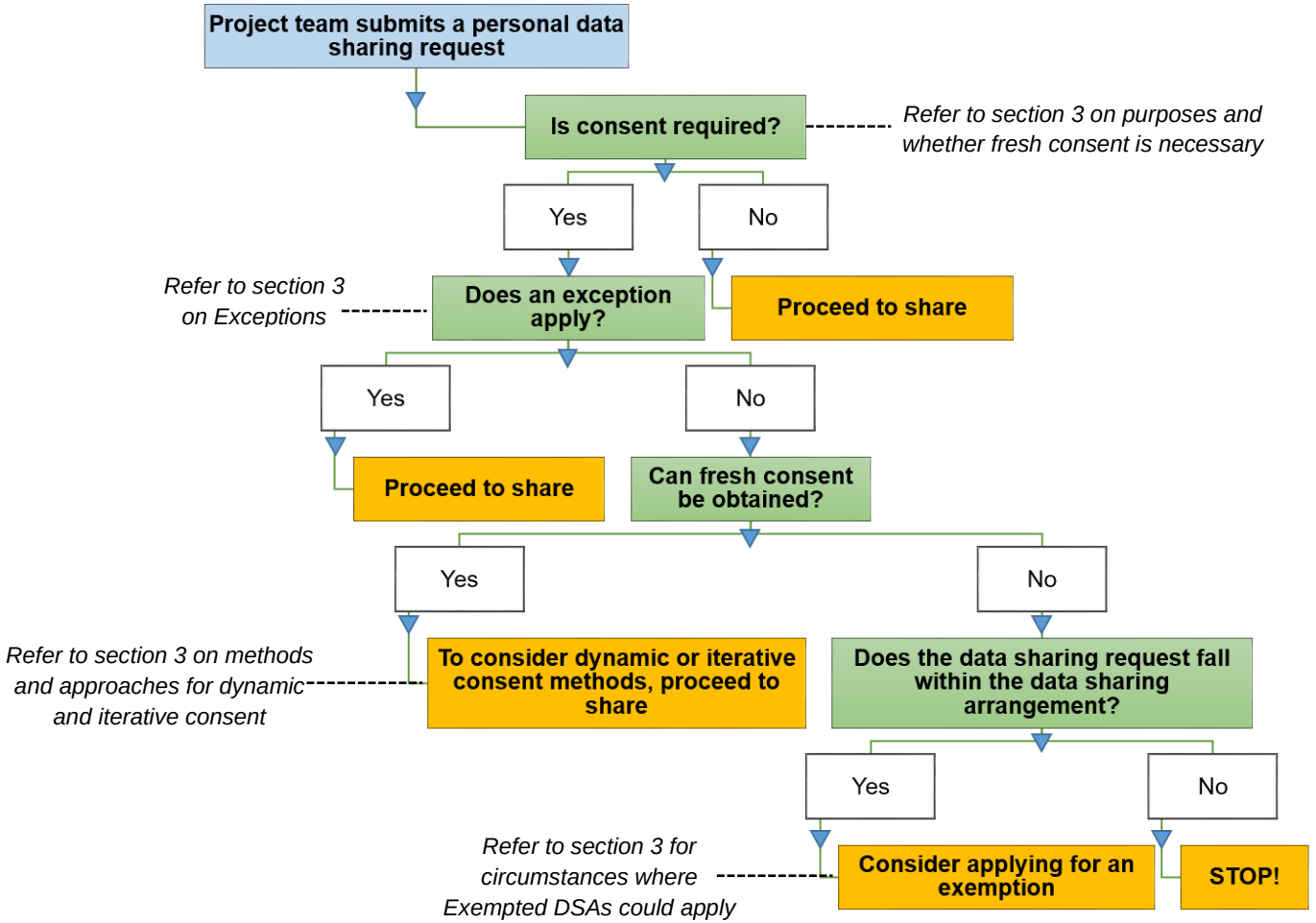
Annex A: Checklist for Data Sharing Based on Consent or Exceptions (For Organisation's Internal Use)

S/N	QUESTIONS TO CONSIDER
I.	**Organisations or departments involved**
1	Which department or organisation is collecting, using or disclosing the personal data? Is the department or organisation located outside of Singapore? **Additional reading** – If data shared will be transferred out of Singapore, the organisation must ensure that it can comply with the transfer limitation obligation. Refer to **Chapter 19** of the Key Concepts Guidelines
II.	**Frequency of sharing**
2	Is the sharing of data an ad-hoc, one-off exercise, routine process or will the sharing take place in response to a specific event?
III.	**Types of Personal Data**
3	What types of personal data will be shared? **Additional reading** – Refer to **Chapter 5** of the Key Concepts Guidelines on personal data
4	The nature of the personal data the organisation has been asked to share **Note** – For example, the personal data was provided in confidence
IV.	**Purpose of the data sharing**
5	What is the purpose of the data sharing? **Additional reading** – Refer to **Chapter 8** of the Key Concepts Guidelines on purpose limitation obligation
6	Is the personal data to be shared limited to those that are relevant for the purpose? State reasons for why you consider the purpose of sharing to be reasonable? **Additional reading** – Refer to **Chapter 8** of the Key Concepts Guidelines on purpose limitation obligation and **Chapter 9** of the Key Concepts Guidelines on reasonableness **Note** – Consider data minimisation principle
7	Can the purpose be achieved if anonymised data is shared?

S/N	QUESTIONS TO CONSIDER
	Additional reading – Refer to **Chapter 3** of the Selected Topics Guidelines on anonymisation
V.	**Risks assessment and mitigation**
8	Has any risk assessment been carried out for the data sharing? **Note** – If applicable, refer to organisation's internal policies on risk management
9	What are the risks mitigation plans to address the risks of data sharing? **Note** – If applicable, refer to organisation's internal policies on risk management
VI.	**Consent**
11	Is consent required to share the data? Has consent been obtained? **Note** – Project teams to consider whether consent during the initial collection covers the collection, use or disclosure of the personal data for the intended purpose, or whether fresh consent is needed for the purpose **Additional reading** – Refer to **Chapter 12** of the Key Concepts Guidelines on consent
12	Do any of the PDPA exceptions apply? Does any other written law authorise or require the collection, use of disclosure of personal data without consent? Elaborate on the relevant law(s) and/or provision(s) **Additional reading** – Refer to **Chapter 12** of the Key Concepts Guidelines on consent and Section 3 of this guide for examples of exceptions
13	Can "dynamic consent" or innovative consent approach be adopted to obtain meaningful consent? **Note** – Where applicable, elaborate if organisation has such means to obtain consent
VII.	**Other considerations**
14	Are there processes in place to facilitate access and correction requests to personal data shared between organisation(s)/department(s)? Elaborate on the processes. **Additional reading** – refer to **Chapter 15** of the Key Concepts Guidelines on access and correction obligations

Annex B: Sample Workflow

For organisations looking to translate the principles highlighted in this guide into a workflow process, the PDPC has put together a sample for reference.



BROUGHT TO YOU BY