GUIDE TO

MANAGING DATA INTERMEDIARIES

SG:D
EMPOWERING POSSIBILITIES

pdpc
PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

CONTENTS

INTRODUCTION

INTRODUCTION

This Guide highlights the relevant obligations under the Personal Data Protection Act (PDPA) and key considerations for organisations (i.e., Data Controllers) which outsource data processing activities to other entities (i.e., Data Intermediaries). Data Controllers (DC) that ensure accountability[1] through their management of Data Intermediaries (DI) provide greater assurance for customers and enhance their business competitiveness. DIs on their part have to ensure compliance with their obligations under the PDPA and adopt good practices when processing data on behalf of a DC[2]. For an overview of the key considerations, refer to **Annex A.**

[1] Accountability refers to the undertaking and demonstration of responsibility for the personal data in the organisation's possession or control.

[2] For data processing on behalf of public agencies, DIs should refer to the relevant requirements set out under the Government's Third-Party Management Framework.

DATA PROTECTION OBLIGATIONS UNDER THE PDPA

DATA PROTECTION OBLIGATIONS UNDER THE PDPA

The PDPA defines a DI as an organisation that processes personal data on behalf of a DC pursuant to a contract[3]. The DI may carry out any operation or set of operations in relation to the personal data which may include, but are not limited to, the following: a) recording; b) holding; c) organisation, adaptation or alteration; d) retrieval; e) combination; f) transmission; and g) erasure or destruction.

A DI is subject to the Data Protection Provisions relating to protection of personal data ("**Protection Obligation**"[4]) and retention of personal data ("**Retention Limitation Obligation**"[5]) when it is processing personal data on behalf of the DC and for the DC's purposes. In the event that a DI uses or discloses personal data in its possession or control beyond the remit granted by the DC, the DI will be responsible for complying with all the Data Protection Provisions under the PDPA.

[3] An organisation may also be a DI of another organisation under the PDPA, even if the contract between the organisations does not clearly identify the organisation as a DI.

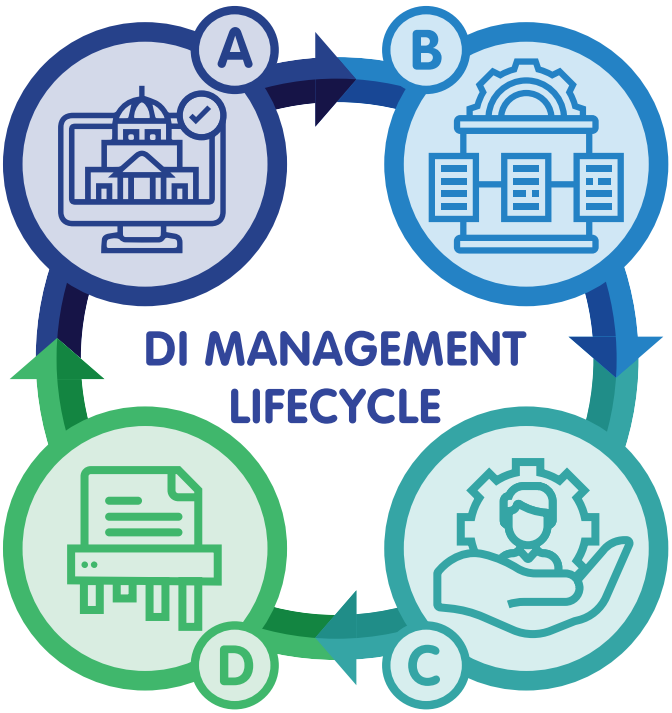
[4] Section 24 of the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

[5] Section 25 of the PDPA requires an organisation to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes.

DATA INTERMEDIARY (DI) MANAGEMENT LIFECYCLE

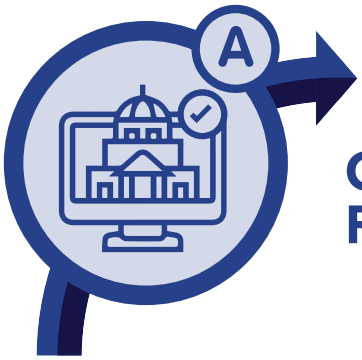
DATA INTERMEDIARY (DI) MANAGEMENT LIFECYCLE

The roles, responsibilities[6] and key considerations for the DC and the DI are covered in this Guide through the DI Management Lifecycle, namely **(A) Governance and Risk Assessment, (B) Policies and Practices, (C) Service Management,** and **(D) Exit Management.**



The considerations discussed are not exhaustive, and DCs should determine the most appropriate measures to adopt in managing their DIs given their specific circumstances. The examples provided draw on lessons from the PDPC's data protection enforcement cases. Organisations may refer to published cases on the PDPC's website for details on measures to implement to prevent similar occurrences.

[6] *Re National Healthcare Group Pte. Ltd.* [2019] SGPDPC 46 at paras 17 to 19. An illustrative case of the respective roles of the DC and DI would be *Re Central Depository Pte. Ltd.* [2019] SGPDPC 24, at paras 19 to 33.



GOVERNANCE AND RISK ASSESSMENT

Good accountability practices begin with the organisation's leadership and governance structure. The decision to outsource data processing activities to DIs and the scope of such data processing activities should be determined by the senior management of a DC. The senior management of the DC should also have an understanding of the risks involved in outsourcing data processing activities. This entails identifying and assessing the personal data risks[7] on a regular basis, and establishing the relevant measures covered in this Guide to mitigate the risks.

At this stage of the DI Management Lifecycle, the DC's roles and responsibilities include:

- Establishing the business objectives and requirements for the proposed data processing outsourcing.
- Determining the scale of outsourcing and the sensitivity of personal data that will be processed.
- Identifying the potential high-level risks that are relevant to establishing the evaluation and selection criteria for the DI.
- Identifying requirements that can be set out in the contract with the DI.

[7] For more information on conducting personal data risk assessments, refer to the PDPC's Guide to Data Protection Impact Assessments (DPIA).

In general, a good understanding of the roles and responsibilities will help in determining the specific policies and practices for managing data processing activities by the DI. For instance, knowing the scale of outsourcing and the sensitivity of the personal data that will be processed by the DI will help the DC ensure that any potential DI must have the ability to provide the appropriate standard of protection to the personal data.

Example: Scoping requirements according to the scale and sensitivity of personal data for processing by a DI[8]

Organisation XYZ is a childcare centre that collects, uses and discloses personal data of children who attend its childcare centre.

Prior to engaging a DI, the management of XYZ should establish their business objectives and requirements with regard to the scale and sensitivity of personal data that will be processed by the selected DI. As a big chain childcare centre, XYZ requires specialised service from a DI that is able to process the personal data of its full enrolment of 800 children, including the children's family details, medical history and parents' income.

In view of the scale and sensitivity of the personal data XYZ collects, XYZ evaluates potential DIs based on their record of accomplishments and ability to provide a high standard of protection to the personal data that will be processed.

[8] For similar topics of investigation conducted by the PDPC, refer to –
- *Re Ncode Consultant Pte. Ltd.* [2019] SGPDPC 11
- *Re Singapore Health Services and another Pte. Ltd.* [2019] SGPDPC 3
- *Re AIG Asia Pacific Insurance Pte. Ltd.* and another [2019] SGPDPC 2
- *Re Aviva Ltd and another* [2016] SGPDPC 15

As part of the selection process, XYZ may also require potential DIs to demonstrate security arrangements that are sufficiently robust and comprehensive to guard against a possible intrusion or attack.

XYZ could also consider whether the scale and sensitivity of the personal data requires it to adopt a Data Protection by Design approach to help ascertain the appropriate measures and safeguards by its DIs.

For more information on Data Protection by Design, refer to the PDPC's Guide to Data Protection by Design for ICT Systems.

Evaluation and selection of DI

The DC should ensure that the DI is able to meet its data processing requirements and provide the protection and care that is commensurate with the volume and sensitivity of the personal data that the DI is to process. In evaluating a potential DI, the DC should be satisfied that the DI has the necessary data protection framework[9], including policies, practices and training for its staff, as well as the appropriate security arrangements to ensure that the personal data it processes will be properly safeguarded[10].

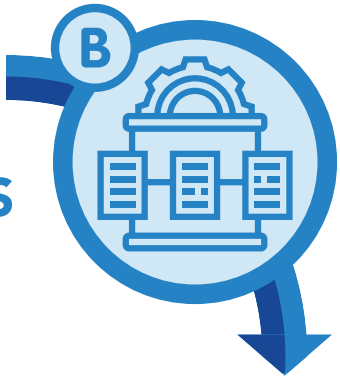
As part of exercising due diligence by checking a DI's track record, the DC could consider whether the DI's data protection practices are subject to regular external reviews and validation, such as the Data Protection Trustmark ("**DPTM**") Certification[11] or other forms of certification[12].

[9] For more information on data protection frameworks, refer to the PDPC's Guide to Developing a Data Protection Management Programme (DPMP).

[10] See *Re Singapore Health Services and another Pte. Ltd.* [2019] SGPDPC 3 para 61.

[11] The DPTM is a voluntary enterprise-wide certification that helps organisations demonstrate accountable and responsible data protection practices. For more information on the DPTM, visit www.imda.gov.sg/dptm.

[12] These may include the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System, and the APEC Privacy Recognition for Processors (PRP) System certifications.



POLICIES AND PRACTICES

The business objectives, data processing requirements and risks involved in data processing will shape how the DC manages its DI. This section outlines how the various data protection policies and practices may operate and how they should be communicated internally to employees involved in managing the DI.

Contracting

The primary means by which a DC may ensure appropriate protection and retention of the personal data processed by its DI is through a contract[13]. As the range of data processing activities that can potentially be outsourced is very broad, it is necessary for the scope of outsourced data processing activities to be clearly defined and agreed upon. There should be clear communication between the DC and the DI on the scope of outsourced data processing activities and the personal data protection requirements[14]. For the DC, this is crucial in ensuring that its business requirements and management decisions in relation to the outsourcing are made clear to the DI.

There are also limits to what the DC can outsource. Hence, the scope of processing that a DI is engaged to carry out is central to the DC-DI relationship and forms the basis for the PDPA's requirement of a contract to clearly document this[15].

[13] See *Re Singapore Health Services and another Pte. Ltd.* [2019] SGPDPC 3 paras 59-62.
[14] *Re Society of Tourist Guides (Singapore)* [2019] SGPDPC 48 at para 12.
[15] *Re KBox Entertainment Group Pte. Ltd.* [2016] SGPDPC 1, para 29 (b)(ii) at pg 11; *Re Singapore Cricket Association and another* [2018] SGPDPC 19 at para 27.

The binding contractual agreement in place between the DC and its DI should set out clearly the obligations and responsibilities of all parties, in particular the DI with regard to the processing of the personal data on behalf of and for the purposes of the DC. If the contract is not made in writing, the key terms setting out the obligations and responsibilities of the DI have to be evidenced in writing. These terms could also reference technical standards[16] like ISO 27001 (for cloud services) as a standard for protecting personal data stored on the cloud. It is a breach of the PDPA if there is no contractual agreement or document setting out the key obligations and responsibilities of the DI[17].

In setting out the contract, the DC should also consider and review details like the schedules to the contract and any other administrative instructions outside the contract. These could be developed in consultation with the DI, as the DI may have the requisite technical and/or operational expertise and experience in processing the personal data. However, the DC is ultimately responsible for determining the scope of responsibilities and security requirements for the processing of personal data[18]. Accordingly, the DC should take all reasonable steps[19] to communicate any specific requirements to its DI. For further considerations on developing contract clauses, refer to **Annex B.**

[16] Other relevant international standards include, but are not limited to:
- ISO/IEC 27018:2019 (Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)
- ISO/IEC 29100:2011 (Information technology – Security techniques – Privacy framework)
- Multi-Tier Cloud Security (MTCS) Standard For Singapore (SS 584) (2013)

[17] *Re Royal Caribbean Cruises (Asia) Pte. Ltd.* [2020] SGPDPC 5 at para 12. Whilst the IT vendor was not a DI, the requirement of the DC to document the obligations and responsibilities of the party it engaged to perform IT services was clearly stated. The statement ended with a warning – "Without clarity, the risks of any omissions will fall on the Organisation, which as data controller is ultimately responsible."

[18] Section 4(3) of the PDPA.

[19] *Re SCAL Academy Pte. Ltd.* [2020] SGPDPC 22 at paras 8 & 9 "organisations [must] articulate their business requirements, work with their vendors on a set of agreed technical measures, and to follow through with proper testing based on risk scenarios derived from the business requirements."

Example: Contractual clauses on overseas transfers of personal data[20]

Before signing up for its services, Organisation ABC conveys to DEF, a Cloud Service Provider ("**CSP**"), that it wishes to store the personal data in data centres in Singapore and Hong Kong, and includes a clause in the contract to state so.

The contractual clause was intended to ensure that DEF was bound by legally enforceable obligations to protect personal data that it received to a standard comparable to that under the PDPA. This is because organisations, such as ABC, are expected to make an assessment of the risks of trans-border transfer of personal data in their possession or under their control, and determine how identified risks (if any) can be addressed.

For more information on cloud services, refer to Chapter 8 of the PDPC's Advisory Guidelines on the PDPA for Selected Topics (Cloud Services).

[20] For similar topics of investigation conducted by the PDPC, refer to *Re Spize Concepts Pte. Ltd.* [2019] SGPDPC 22.

Standard operating procedures

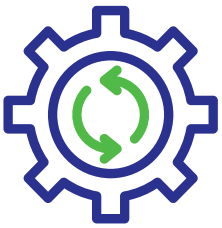
The governance and operational measures are as important as the contractual documentation in ensuring that a DI meets its obligations. As part of ensuring that accountable measures are in place, the DC could establish standard operating procedures ("**SOPs**"). SOPs may be further sub-divided into the following areas:

a) Operational Procedures; and

b) Reports

i. Regular management report

ii. Ad-hoc incident report



a) Operational Procedures

Operational procedures are important means for the DC to assert control and effectively manage operational procedures. These can be developed jointly or proposed by the DI as in most instances, the DI would have the relevant technical and operational experience and expertise for ensuring compliance with the obligations. However, as the DC is ultimately responsible, it is good practice for the DC to approve the final procedures and any significant changes to them. The DI is responsible for implementing these procedures as approved by the DC.

For outsourcing of IT operations, an operational procedure may include IT maintenance processes such as regular security patching. Patching is one task that system owners are required to perform in order to keep their security measures current against external threats. It may also include conducting regular penetration tests on IT applications and databases to fix potential vulnerabilities. For good practices on protecting electronic personal data, refer to the PDPC's Guide to Securing Personal Data in Electronic Medium.

Example: Establishing an operational procedure[21]

Financial institution ABC engages XYZ to handle the processing, printing and delivery of monthly financial reports to ABC's customers. As part of its business offering, ABC plans to provide a personalised report charting each customer's investment history with ABC. ABC puts in place an agreement obliging XYZ to take the necessary data protection measures to protect customers' personal data during the printing and delivery process.

As merely having a data protection policy may not be a sufficient security arrangement given the sensitive nature of the information in the personalised report, ABC may additionally consider having XYZ develop an operational procedure governing the processing, printing and mailing of these reports.

For instance, if a new delivery process was required, an employee of XYZ would be required to test the delivery programme first before any actual delivery. Additionally, XYZ also has processes in place to ensure that any personal data collected from ABC is accurate and complete. In this way, any errors or issues arising from new processes or information would be contained. This enables XYZ to detect and rectify any issues in the delivery process before its actual implementation. In addition, an operational procedure for the secure transfer of personal data between ABC and XYZ is established by ensuring that the files containing the customers' personal data is sent via a secured format, i.e., Secured File Transfer Protocol.

For more information on securing personal data, refer to the PDPC's Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data and Guide on Printing Processes for Organisations.

[21] For similar topics of investigation conducted by the PDPC, refer to –
- *Re Learnaholic Pte. Ltd.* [2019] SGPDPC 31
- *Re Singapore Telecommunications Limited and another* [2017] SGPDPC 4
- *Re Central Depository Pte. Ltd. and another* [2016] SGPDPC 11

b) Reports

Another role of the DC is to define the format (e.g. level of detail required) and frequency (e.g. daily, weekly, ad-hoc) of the reports from its DI.

i. **Regular management report**

Management reports should be surfaced regularly to provide the DC's management with the information to monitor and manage business operations. Such regular reports help to ensure effective management of DIs.

ii. **Ad-hoc incident report**

Incident reports are surfaced based on issues that require special attention, such as a data incident. In this regard, the DC should have in place an escalation process and a reporting chain for incident reporting to ensure DIs notify them without undue delay when DIs become aware of any data incidents. SOPs should also cover incident investigation and management, and data breach notification procedures. Additionally, in the event of a data breach, DCs should put in place drawer plans for data breach management for their DIs to take remedial actions to address the data breach.

Example: Establishing an SOP to report ad-hoc events[22]

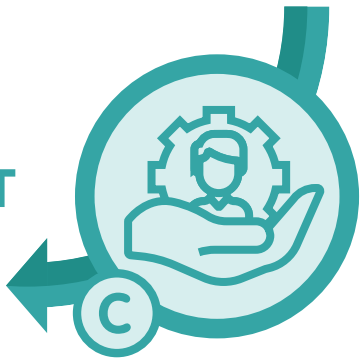
Organisation ABC engages an IT vendor, DEF, to manage its customer portal. In the course of updating the portal, DEF erroneously disclosed one of ABC's customer's personal data to other customers of ABC. DEF subsequently rectified the error but did not notify ABC of the incident. ABC only became aware of the incident through queries received from customers who were able to view the affected customer's personal data on its online customer portal.

ABC could have established an SOP with DEF on the notification of ad-hoc events related to both IT and data incidents. In the SOP, DEF should notify ABC of any data incident without undue delay as soon as it becomes aware of the data incident.

For more information on securing personal data, refer to the PDPC's Guide to Securing Personal Data in Electronic Medium.

[22] For similar topics of investigation conducted by the PDPC, refer to –
- *Re Singapore Telecommunications Limited and another* [2017] SGPDPC 4
- *Re Singapore Cricket Association and another* [2018] SGPDPC 19

SERVICE MANAGEMENT



An accountable DC not only develops and communicates its data protection policies, it also puts in place monitoring and reporting structures to manage its DI.

Examples of such structures include establishing project management committees which report to the Board or senior management, and regular meetings with DIs. Depending on the nature and extent of the outsourcing arrangement, this could potentially include periodic audits, as well as on-site inspections. Another important aspect of service management is proper on-boarding of the DI and training of its staff at the commencement of the outsourcing relationship.

On the part of DIs, proactive monitoring is a useful way to protect the personal data and detect any unauthorised access, given the DIs' proximity to and technical expertise in carrying out the relevant data processing activities.

On-boarding and Training

It is important to ensure that the DI's personnel involved in the data processing activities are aware of the DC's business requirements, the data protection risks and mitigation measures for the data processing activities, contractual arrangements (including the roles and responsibilities of the DI), and standard operating procedures (including expectations on reporting). To achieve that, an on-boarding process may be needed for data processing activities of a bigger scale[23]. For data processing activities of a smaller scale (e.g. engaging a DI to take photos of a business conference), a kick-off meeting with the DI may serve the same purpose.

As part of the on-boarding process, the DC may wish to brief *key* members of the DI's project team. The briefing will then form the basis of the structured training to be conducted for the relevant personnel and other third parties involved in the data processing activities.

A structured training plan is critical in equipping the DI's personnel and relevant third parties with the knowledge and resources to manage the personal data in accordance with the DC's requirements. The training plan should include the appropriate frequency, target audience and platforms for training to ensure that its objectives are met.

If a DC has multiple DIs involved in overlapping data processing activities, an on-boarding process would help to ensure a clear meeting of minds on the roles and responsibilities that each DI is to undertake, and that each DI is aware of the scope of its respective data processing activities.

[23] See *Re Tiger Airways Singapore Pte. Ltd.* [2017] SGPDPC 6 as a case in which the DI, Asia-Pacific Star Private Limited was found not to have implemented the required SOPs (paras 33-34S) and training (para 35). See also *Re EU Holidays Pte. Ltd.* [2018] SGPDPC 38 as an example of a case in which an IT vendor, iClick Media Pte. Ltd., was directed to train its staff in data protection. The report is in a separate stub from the main report.

Example: On-boarding a DI[24]

Organisation ABC engages IT vendor DEF to manage its public-facing website and IT vendor GHI to provide hosting for the website. As ABC foresees potential overlaps in data processing activities between both vendors, ABC holds an on-boarding meeting to ensure that DEF and GHI are aware of the obligations and scope of their respective data processing activities.

The areas of discussion between ABC and its IT vendors at the on-boarding could include:

a. Requiring that both IT vendors consider how the personal data should be handled as part of the design and layout of the website;

b. Planning and developing the website in a way that ensures that it does not contain any web application vulnerabilities that could expose the personal data of individuals collected, stored or accessed via the website;

c. Requiring that the IT vendor who provides hosting for the website securely configures and adequately protects the servers and networks against unauthorised access;

d. Requiring that any maintenance and/or administrative changes to the website do not contain vulnerabilities that could expose the personal data;

e. Discussing whether there are technical and/or non-technical processes in place to prevent the personal data from being exposed accidentally or otherwise.

For more information on building websites, refer to the PDPC's Guide on Building Websites for SMEs.

[24] For similar topics of investigation conducted by the PDPC, refer to –
- *Re Singapore Cricket Association and another* [2018] SGPDPC 19

Management Meetings with DIs

Regular meetings with key members of the DI's data processing team will ensure the steady flow of information and allow the DC to ensure that its DI's operations are going according to contractual arrangements and the agreed SOPs. The meetings will also help the DC to fulfil its responsibilities by ensuring proper supervision of its DI.

As these meetings provide an important channel of communication between the DI and the DC, there should be an appropriate level of representation from the DC and DI at these meetings. For instance, the representatives from both the DC and DI should be sufficiently senior to make decisions if necessary. Such meetings are also a conducive forum for management reports to be tabled for discussion and for decisions to be made on issues raised in incident reports.

Proactive monitoring by DIs

In order for a DI to meet its requirements, it will have to put in place proactive monitoring practices. Examples of proactive monitoring include reviewing document database logs and system logs, and monitoring access, to identify possible unauthorised access or disclosure, particularly if the DI uses several systems or databases to store or process large amounts of personal data[25].

DCs that outsource the processing of large volumes of personal data should consider getting their DIs to implement database access monitoring that provides real-time (or close to real-time) dynamic review of access activity as it is also useful for detecting unauthorised access to personal data.

[25] See *Re Singapore Health Services and another Pte. Ltd.* [2019] SGPDPC 3 para 119.

Audits and on-site inspections

There may be circumstances where a DC would like to verify that its DI is properly carrying out its roles and responsibilities, particularly where the DI is involved in processing large amounts of sensitive personal data over long periods. In such cases, the DC could consider conducting audit exercises, requesting an independent audit report or having on-site inspections at the DI's premises[26]. The necessity and frequency of audits and on-site inspections will be determined by the risk profile of the DC, the nature and extent of data processing activities outsourced, and the severity and likelihood of occurrence of the risks identified. Audit remediation measures are also critical in ensuring that any data protection risks are addressed effectively.

Simulation or table-top exercises

While audits and inspections are put in place to monitor and evaluate the DIs' *operations*, simulations and table-top exercises should be considered to test out the effectiveness of ad-hoc incident reporting and remediation *plans*. Such exercises provide an opportunity for the DC and DI to go beyond day-to-day operational procedures and train their personnel to respond to pre-defined situations like data incidents or crisis circumstances. This provides the DI with the necessary training context to build up and sharpen its responsiveness to actual situations.

[26] See *Re Singapore Health Services and another Pte. Ltd.* [2019] SGPDPC 3 para 17.

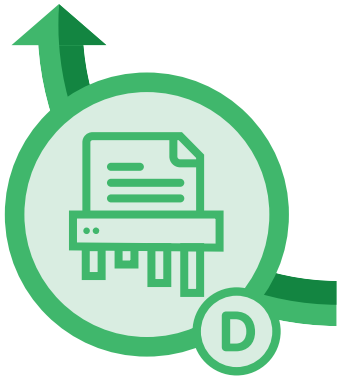
Example: On-site inspection of a DI

Voluntary welfare organisation ABC engages DEF to dispose of its confidential documents such as applications for financial assistance.

To ensure that DEF adheres to the agreed SOP such that the personal data in the documents are not disclosed to unauthorised parties during the disposal process, ABC decides to inspect how DEF disposes of the documents, as part of its supply chain arrangement.

For instance, to ensure that containers with the disposed paper are secured during transit and the shredding facility has physical security in place, ABC deploys employees to witness the transportation and actual destruction of the paper.

For more information on outsourcing the disposal of documents and other physical media, refer to the PDPC's Guide to Disposal of Personal Data on Physical Medium.



EXIT MANAGEMENT

DCs should establish exit management plans for the conclusion of their engagement with DIs to ensure business continuity and proper handling of personal data where they are no longer required for legal or business purposes[27]. This includes establishing clear time frames for the DI to cease retention of the personal data after it has completed the processing activities.

An organisation ceases to retain documents containing personal data when it no longer has access to those documents and the personal data they contain. Examples include:

- Destroying the documents – e.g. by shredding them or disposing of them in an appropriate manner; or
- Anonymising the personal data.

Part of exit management could include the requirement for DIs to ensure that all work done is fully documented and that all documentation is handed over to the DC upon completion of the project. For IT-related projects such as data migration, the documentation could include information such as the database mapping, extraction, transformation and loading scripts, verification test scripts and test results. To ensure that their DIs abide by the agreed plans, DCs could also include exit audits and checks.

In the event of a change in DI, the DC should ensure that any data migration or transfers of data from one DI to another is done in a secure manner. Thereafter, the DC should follow through with the same steps of the DI Management Lifecycle.

[27] Section 25 of the PDPA (The Retention Limitation Obligation).

ANNEX A: OVERVIEW OF KEY CONSIDERATIONS

ANNEX A: OVERVIEW OF KEY CONSIDERATIONS

Organisations should determine the appropriate measures to adopt based on the data protection risk involved. In general, organisations should consider the scale of the outsourcing and sensitivity of the personal data that their DI is processing, as well as the duration of the DI contract period, in determining the appropriate measures to adopt.

Recommended measures for complex data processing activities (i.e., where there is either a significant scale of personal data, sensitive types of personal data involved, or a combination of these factors) are highlighted below.

In addition, the Government has introduced a Third-Party Management Framework for organisations ("**third parties**") who work with public sector agencies. Key policies from the framework on safeguarding data are referenced below. For more information on the Government's Third-Party Management Framework, please visit the SmartNation website.

Key Considerations of the PDPC's DI Management Lifecycle to Manage DIs of Private Sector Organisations	Key Policies of the Government's Third-Party Management Framework to Manage DIs of Public Sector Agencies
(A) Governance and Risk Assessment √ Begin with the organisation's leadership and governance structure. Decisions to outsource data processing activities and the scope of such data processing activities should be determined by the senior management of the DC. √ Have an understanding of the risks involved in outsourcing data processing activities. This entails identifying and assessing the personal data risks on a regular basis, and establishing the relevant measures covered in this Guide. √ Roles and responsibilities: • Establishing the business objectives and requirements for the proposed data processing outsourcing; • Determining the scale of outsourcing and the sensitivity of personal data that will be processed; • Identifying the potential high-level risks that are relevant to establishing the evaluation and selection criteria for the DI; and • Identifying requirements that can be set out in the contract with the DI. √ Determine the specific policies and practices for managing the processing activities carried out by the DI. √ Ensure that the DI selected is able to meet the data processing requirements and provide the protection and care that is commensurate with the volume and sensitivity of the personal data. √ Be satisfied that the DI has the necessary data protection framework. √ [For complex data processing activities] • Consider engaging DIs that have obtained the Data Protection Trustmark ("**DPTM**") Certification or other forms of certification.	**Stage 1: Evaluation and Selection** √ To ensure that the Government adequately manages its security, data and project risks when engaging Third Parties, Agencies shall identify, assess, prioritise and mitigate the risks when outsourcing to Third Parties during the evaluation and selection process.

(B) Policies and Practices	Stage 2: Contracting and On-boarding
√ Communicate clearly with the DI on areas such as the scope of outsourcing and their personal data protection requirements. √ Have a binding contractual agreement that sets out the obligations and responsibilities of all parties. √ Take reasonable steps (such as having project documentation) to communicate specific requirements and ensure that the DI understands its obligation. √ Tailor operational procedures to the scope of the outsourcing arrangement. √ Approve the final operational procedures and any significant changes. √ [For complex data processing activities] • Consider and review details like the schedules to the contract and other administrative instructions outside the contract. • Put in place appropriate standard operating procedures ("**SOPs**") for the DIs for reporting (regular management report and ad-hoc incident report) and operational procedures. • Define the format and frequency of the reports from the DI. • Surface management reports regularly to provide the DC's management with the information to monitor and manage business operations. • Put in place an escalation process and a reporting chain for incident reporting for ad hoc events. Additionally, in the event of a data breach, DCs could put in place drawer plans for their DIs to take remedial actions to address the data breach.	√ To ensure that the security, data and project risks involved in assigning work to Third Parties are addressed, Agencies shall establish contracts or other equivalent instruments with their Third Parties to govern how the Third Parties should perform the assigned work in a manner that addresses all identified risks involved. √ To ensure that the appointed Third Parties (and their personnel) are adequately assessed, cleared and prepared for the assigned work, Agencies shall implement an on-boarding process which includes briefings on applicable data security requirements, security clearance and obtaining undertakings from Third-Party personnel, where necessary.
(C) Service Management	**Stage 3: Service Management**
√ Have a kick-off meeting to brief key members of the DI's project team. √ Have the appropriate level of representation from the DC and DI in meetings. √ Conduct ad-hoc meetings as and when necessary to address data protection issues in a timely manner.	√ Agencies shall regularly monitor and review the Third Parties' performance and compliance with applicable public sector policies and standards which are incorporated in the contracts or equivalent instruments established with the Third Parties.

√ [For complex data processing activities] • Develop an on-boarding process to brief key members of the DI's project team on the business requirements, policies and practices, standard operating procedures as well as the roles and responsibilities of the DI. • Conduct regular meetings with key members of the DI's data processing team. • Use the briefing to key members of the project team to form the basis for the structured training to be conducted. • Include the appropriate frequency, target audience and platforms for training so as to develop the right corporate culture towards data protection. • Consider proactive monitoring by having the DI document through document database logs and system logs and monitoring access to identify possible unauthorised access or disclosure, particularly if the DI uses several systems or databases to store or process large amounts of personal data. • Consider conducting audit exercises, requesting for an independent audit report, or having on-site inspections to verify that the DI is delivering the agreed services in accordance with the policies, practices and SOPs. • Consider simulations and table-top exercises to test out the effectiveness of ad-hoc incident reporting and remediation plans.	√ Agencies shall perform regular checks or audits on their Third Parties throughout the period of engagement to ensure that the Third Parties carry out their assigned work in compliance with contractual obligations and applicable public sector policies and standards. More stringent requirements will be imposed on Third Parties dealing with systems and services of a higher risk.
D) Exit Management √ Establish exit management plans for the conclusion of the engagement with DIs to ensure business continuity and proper handling of personal data. √ Establish clear time frames for the DI to cease retaining the personal data after it has completed the data processing activities. √ Include the requirement for DIs to ensure that all work done is fully documented and that all documentation is handed over to the DC. √ Conduct exit audits and checks to ensure that the DI abides by the agreed plans. √ Ensure that any data migration or transfers of data from one DI to another is done in a secure manner in the event of a change in DI. √ Follow through with the same steps of the DI Management Lifecycle.	**Stage 4: Transition Out** √ To ensure business continuity and the proper transfer and disposal of data and assets back to Agencies upon the exit of the Third Parties, Agencies shall put in place and maintain up-to-date exit management plans for all Third Parties' work and services, which shall include the conduct of exit checks or audits before the Third Parties discontinue their services.

ANNEX B: FURTHER CONSIDERATIONS ON DEVELOPING CONTRACT CLAUSES

ANNEX B: FURTHER CONSIDERATIONS ON DEVELOPING CONTRACT CLAUSES

DCs may consider the following factors when negotiating contracts with DIs:

Governance and Risk Assessment

a. prohibition against any use or disclosure of the personal data by the DI for any unauthorised purposes;

b. specific data protection measures required to be taken by the DI to protect the personal data entrusted to it (e.g. encryption of database, not storing the full string of NRIC numbers);

Polices and Practices

c. prohibition of sub-contracting or requirement of the DC's approval before sub-contracting data processing activities that the DI is engaged to provide;

d. where sub-contracting is allowed by the DC, the DI's agreement with the sub-contractor should impose the same obligations in relation to processing on the sub-contractor as imposed on the DI by the DC;

e. no undue delay in reporting any signs of abnormalities detected (e.g. audit trail of unusual frequent access at odd hours);

f. no undue delay in reporting data incidents or breaches that the DI becomes aware of;

g. where there is overseas transfer of personal data, consider i) the overseas locations where the personal data will be transferred; and (ii) the standard of protection for the transferred personal data, such that the DI only transfers to overseas locations with comparable data protection regimes, or the recipient is bound by legally enforceable obligations to ensure a comparable standard of protection;

h. where the DI is to obtain consent on behalf of the DC for the collection, use or disclosure of personal data for specific purposes, the processes to ensure that the DI obtained valid consent on behalf of the DC;

Service Management

i. measures required of the DI (e.g. having SOPs and regular management meetings), to ensure proper governance and accountability, and to ensure that its relevant staff are properly on-boarded and adequately trained to handle personal data;

j. DC's right to request audit of how the DI handles and stores personal data;

k. DC's right to conduct on-site inspections to verify that the DI is delivering its services in accordance with the agreed policies, practices and SOPs; and

Exit Management

l. timely return or irreversible destruction, deletion or anonymisation of the personal data when it is no longer required for the purpose for which it was provided by the DC.

The above list is not exhaustive and DCs may need to revise or include additional obligations to meet their own specific requirements having regard to factors such as the amount and nature of personal data involved, the type and extent of processing, and the potential harm or impact that may result from a data breach. Contracts should also be reviewed regularly. For more information on data protection clauses, refer to the PDPC's Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data.

BIBLIOGRAPHY

(Relevant cases investigated by the PDPC relating to DC-DI relationships)

2016

- *Re KBox Entertainment Group Pte. Ltd.* [2016] SGPDPC 1
- *Re Central Depository Pte. Ltd. and another* [2016] SGPDPC 11
- *Re Aviva Ltd and another* [2016] SGPDPC 15

2017

- *Re Singapore Telecommunications Limited and another* [2017] SGPDPC 4
- *Re Tiger Airways Singapore Pte. Ltd.* [2017] SGPDPC 6

2018

- *Re Singapore Cricket Association and another* [2018] SGPDPC 19
- *Re EU Holidays Pte. Ltd.* [2018] SGPDPC 38

2019

- *Re AIG Asia Pacific Insurance Pte. Ltd. and another* [2019] SGPDPC 2
- *Re Singapore Health Services and another Pte. Ltd.* [2019] SGPDPC 3
- *Re Ncode Consultant Pte. Ltd.* [2019] SGPDPC 11
- *Re Spize Concepts Pte. Ltd.* [2019] SGPDPC 22
- *Re Central Depository Pte. Ltd.* [2019] SGPDPC 24
- *Re Learnaholic Pte. Ltd.* [2019] SGPDPC 31
- *Re National Healthcare Group Pte. Ltd.* [2019] SGPDPC 46
- *Re Society of Tourist Guides (Singapore)* [2019] SGPDPC 48

2020

- *Re Royal Caribbean Cruises (Asia) Pte. Ltd.* [2020] SGPDPC 5
- *Re SCAL Academy Pte. Ltd.* [2020] SGPDPC 22

The PDPC publishes decisions relating to organisations that are found to have contravened the data protection provisions under the PDPA. These decisions provide valuable insights and lessons so that organisations can implement measures to prevent similar occurrences. They also serve to remind individuals and organisations of their respective rights and obligations under the PDPA. In the longer term, the publication of cases aims to promote accountability among organisations to build and strengthen consumer trust and confidence.

For more information on the cases referenced in this Guide, visit the PDPC website at www.pdpc.gov.sg/Commissions-Decisions.

#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

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

This Guide highlights the relevant obligations under the Personal Data Protection Act (PDPA) and key considerations for organisations when outsourcing data processing activities to data intermediaries.