

THE SOFTWARE PRACTICE PTE LTD	No of Pages	1 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION IMPACT ASSESSMENT & RISK ASSESSMENT	Doc No	DPMP-PRO-01
	Revision	1.0

AMENDMENTS LOG

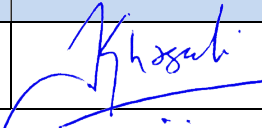
Revision History

Version	Date	Revision Author	Summary of Changes
1.0	10 June 2024	Edwin Soedarta DPO	First Release

Distribution

Name	Location
<i>All employees</i>	<i>Shared Folder</i>

Review & Approval

Name	Position	Signature	Date
Khasali M	Director		10 June 2024

THE SOFTWARE PRACTICE PTE LTD	No of Pages	2 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION IMPACT ASSESSMENT & RISK ASSESSMENT	Doc No	DPMP-PRO-01
	Revision	1.0

Contents

AMENDMENTS LOG 1

RECORDS FOR DOCUMENT REVIEW 3

PURPOSE 4

SCOPE..... 4

DEFINITION..... 4

RESPONSIBILITIES & AUTHORITIES..... 4

PROCEDURE..... 6

 PHASE 1: ASSESS NEED FOR DPIA6

 PHASE 2: PLAN DPIA7

 PHASE 3: IDENTIFY PERSONAL DATA & PERSONAL DATA FLOWS.....7

 PHASE 4: IDENTIFY AND ASSESS DATA PROTECTION RISKS.....7

 PHASE 5: CREATE AN ACTION PLAN (RISK TREATMENT).....8

 PHASE 6: IMPLEMENT ACTION PLAN AND MONITOR OUTCOMES.....9

FORMS 9

ANNEX A – RISK REGISTER 10

ANNEX B – RISK ASSESSMENT FRAMEWORK..... 12

THE SOFTWARE PRACTICE PTE LTD	No of Pages	4 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION IMPACT ASSESSMENT & RISK ASSESSMENT	Doc No	DPMP-PRO-01
	Revision	1.0

PURPOSE

This document provides an outline of key principles, considerations, and steps on conducting a Data Protection Impact Assessment (DPIA) and Risk Assessment (RA).

SCOPE

This procedure applies to all the organization's systems, processes or services that involved the collection and processing of personal data.

DEFINITION

DPIA A key component the Data Protection by Design ("DPbD") approach, in which an organization considers the protection of personal data from the earliest possible design stage, and throughout the operational lifecycle, of the new system, process or service. This way, the appropriate safeguards to protect personal data would have been embedded within. It involves identifying, assessing, and addressing personal data protection risk.

RESPONSIBILITIES & AUTHORITIES

The table below lists out typical roles and responsibilities of key parties involved in the DPIA.

Who is involved?	Who are they?	Role in DPIA
The Management	Management of organization who is responsible for the review and approval of the data protection framework and the action plans for addressing the data protection risks	<ul style="list-style-type: none"> • Commissions the DPIA • Approves the DPIA and proposed action plans and solutions arising from DPIA
Process Owner	Person in charge of the system, process or service	<ul style="list-style-type: none"> • DPIA Lead, overall, in-charge of the DPIA for a particular system, process or service • Assesses the need for DPIA, plans the DPIA and conducts the DPIA • Identifies and seeks input from relevant stakeholders on: <ul style="list-style-type: none"> ○ Potential data protection risks and challenges from an implementation perspective

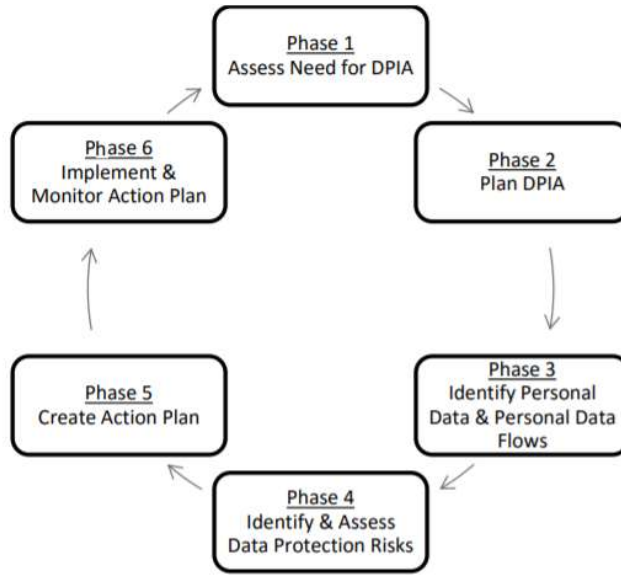
THE SOFTWARE PRACTICE PTE LTD	No of Pages	5 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION IMPACT ASSESSMENT & RISK ASSESSMENT	Doc No	DPMP-PRO-01
	Revision	1.0

Who is involved?	Who are they?	Role in DPIA
		<ul style="list-style-type: none"> ○ How identified data protection risks should be addressed and possible solutions ● Documents DPIA report which includes proposing action plan ● Monitors DPIA outcomes, reviews the DPIA when there is a change in risks to data protection
Data Protection Officer (DPO)	Person responsible for creating and enforcing the data protection policies within the organization and for ensuring compliance with PDPA	<ul style="list-style-type: none"> ● Advises DPIA Lead through the DPIA process including: <ul style="list-style-type: none"> ○ Identifying and mitigating identified data protection risks by providing support based on best practices adapted to organization's needs and circumstances ○ Ensuring that DPIAs are conducted according to this procedure ○ Reviewing DPIA report prior to submission to management ● Assists in reviewing the DPIA when there is a change in risks to data protection
Others	Other organizational functions or departments that have some level of involvement in the system, process or service, external parties such as subject matter experts or even potentially affected individuals, where needed.	<ul style="list-style-type: none"> ● Provides input on potential risks and challenges with respect to their function. For example: <ul style="list-style-type: none"> ○ IT: Advising the DPIA Lead on possible IT solutions and security risks in implementing measures to protect personal data. This may also include advising on potential challenges on system design and development. ○ Business Development: Advising the DPIA Lead on possible customer impact if the DPIA outcomes warrants a change to customer interaction or day-to-day operations. ○ HR: Advising on the appropriate training programmes or resources should the DPIA outcomes require staff to be able to carry out new data protection measures or activities.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	6 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION IMPACT ASSESSMENT & RISK ASSESSMENT	Doc No	DPMP-PRO-01
	Revision	1.0

PROCEDURE

A DPIA typically comprises the following phases:



Phase 1: Assess Need for DPIA

- 1) Before conducting the DPIA, we will assess whether there is a need for a DPIA with the following considerations:
 - a. First, the DPIA Lead and DPO would have to assess whether there is a need for a DPIA by determining if the system, process, or service involves personal data. If personal data is not involved, then a DPIA is not necessary.
 - b. Once it has been determined that the system, process, or service involves personal data, the following threshold questions can be used to further assess the need for a DPIA. If the answer is “yes” to any of the questions below, then a DPIA should be conducted. If the answer is “no” to both questions, the DPIA Lead should confirm that there is no potential data protection risks associated with the system, process or service and DPIA is not necessary.

S/N	Considerations	Yes/No
1	Is a new system, process or service being introduced, developed or implemented? <i>For example, a new IT system or a new process or service that involves the handling of personal data.</i>	
2	Is an existing system, process or service being reviewed, or substantially redesigned? <i>For example, a redesign of operational process workflow that involves different groups of users to handle personal data.</i>	

THE SOFTWARE PRACTICE PTE LTD	No of Pages	7 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION IMPACT ASSESSMENT & RISK ASSESSMENT	Doc No	DPMP-PRO-01
	Revision	1.0

- 2) Once the decision is made to conduct a DPIA, the DPIA Lead should proceed to plan the DPIA in consultation with the DPO. The DPO should also advise the DPIA Lead throughout the conduct of the DPIA.

Phase 2: Plan DPIA

- 1) In establishing the key activities or steps needed to conduct the DPIA, the DPIA Lead should cover the following aspects in the DPIA & RA Worksheet (DPMP-PRO-01-F1):
 - System / Process / Service Description and Scope – an overview of the system, process, or service
 - Parties Involved – identify relevant internal departments/functions or external stakeholders’ inputs, views or advisories / instructions would have to be considered; and
 - DPIA Traceability – identify who prepared, reviewed, and approved the DPIA with date of last update.

Phase 3: Identify Personal Data & Personal Data Flows

- 1) To identify and map personal data involved in the system, process, or service, the DPIA Lead would need to collate and review documentation related to the scope in order to determine how personal data is being collected, used, disclosed, retained and disposed of. The DPIA Lead should also consult with the identified relevant internal and external stakeholders to ensure comprehensiveness and accuracy of information.
- 2) The DPIA Lead can then proceed to:
 - Identify all the various types of personal data handled (or envisaged to be handled) in relation to the specific system, process, or service, and determine the organization’s purposes for collecting, using, disclosing, and retaining them; and
 - Map the way that personal data flows through various stages or touchpoints of the system, process, or service, across its lifecycle i.e., from collection to storage and/or disposal.

The above will be recorded through the DPMP-PRO-01-F2 Data Inventory Map (DIM). This DIM shall be reviewed at least once a year and when there is a change in risks associated with the personal data handling of the system, process, or service. The DIM shall be maintained by the DPO and the copy shall be made available in a Shared Folder to be accessed by the Data Protection Committee.

Phase 4: Identify and Assess Data Protection Risks

- 1) Having documented how personal data is being handled, the DPIA Lead can proceed to identify and assess personal data protection risks by:
 - Answering the questions in the DPIA & RA Worksheet (DPMP-PRO-01-F1) to assess the system, process, or service against PDPA requirements and/or data protection best practices; and
 - Identifying areas in the DIM which could lead to a breach of the PDPA or are gaps compared to requirements and/or industry best practices.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	8 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION IMPACT ASSESSMENT & RISK ASSESSMENT	Doc No	DPMP-PRO-01
	Revision	1.0

Refer to *Annex A Risk Register* for examples of a breach of PDPA and or gaps.

Any areas which could lead to breach or gaps identified will be analysed for potential impact and likelihood based on the pre-defined risk framework detailed in *Annex B Risk Assessment Framework*.

Phase 5: Create an Action Plan (Risk Treatment)

- 1) In this phase, the DPIA Lead would need to propose how the identified data protection risks should be addressed. Documented in the form of a risk treatment plan, the DPIA Lead should indicate the action owner(s) responsible for the implementation of specified recommendations (such as technical, physical, or organizational measures), as well as implementation timelines, and monitoring of implementation outcomes.
- 2) The approach to develop the action plan and prioritization of risks based on their likelihood and impact levels will be in line with the risk acceptance criteria, risk treatment options and recommended timelines detailed below:

- i. Risk Acceptance Criteria

A risk be recommended for acceptance if it meets one or more of the following criteria:

- the risk is calculated as 4 or less (Refer to Annex B Risk Assessment Matrix);
- the cost of an appropriate control is judged to be more than the potential loss however, strict monitoring must be implemented to prevent data breach; and
- known changes within 1 month or less will soon mean that the risk is reduced or disappears completely however, strict monitoring must be implemented to prevent data breach within the said period.

- ii. Risk Treatment Options

The following options may be applied to the treatment of the risks that have been agreed to be unacceptable:

- **Avoid** the risk by taking action that means it no longer applies
- **Modify** the risk - apply appropriate controls to lessen the likelihood and/or impact of the risk
- **Share** the risk with another party e.g., insurer or supplier

- iii. Recommended Timelines

High risks must be prioritized for remediation within 3 months, medium risks will be remediated within 6 months and low risks will be addressed (if necessary) within 1 year. In the event more time is required, justification shall be approved by the Top Management.

- 3) The risk treatment plans with the action plans, responsibilities, timelines, and status shall be documented in the DPIA & RA Worksheet (DPMP-PRO-01-F1).

THE SOFTWARE PRACTICE PTE LTD	No of Pages	9 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION IMPACT ASSESSMENT & RISK ASSESSMENT	Doc No	DPMP-PRO-01
	Revision	1.0

Phase 6: Implement Action Plan and Monitor Outcomes

- 1) The completed DPIA & RA Worksheet (DPMP-PRO-01-F1) will be reviewed by the DPO to ensure that the proposed action plans are in line with the organization's policies and contains effective data protection practices. Once the worksheet has been reviewed by the DPO, it should be submitted to The Management, and seek approval to implement the action plans.
- 2) Once approved, the respective action owners can start to implement the action plans. The DPO will monitor the outcomes of the action plans to ensure that identified risks are addressed as planned, and risks to personal data continue to be managed responsibly.
- 3) When there is a change in risks associated with the personal data handling of the process, the existing DPIA & RA Worksheet (in particular, the action plan outcomes) would need to be reviewed and updated so that any new gaps or risks to individuals' personal data can be addressed. Examples when risks can change are:
 - Subsequent developments to the system, process, or service (e.g., changes to the purposes or context, the type of personal data collected, how the processing is conducted)
 - Technology or security developments (e.g., when a system may face new security vulnerabilities)
 - Broader environmental changes (e.g., legislative amendments).
- 4) As a good practice, the organization shall consider regularly reviewing (at least once a year and when changes occur) the DPIA & RA process, DIM and DPIA & RA Worksheet to ensure their relevance as part of business planning and data protection management.

FORMS

DPMP-PRO-01-F1	DPIA & RA Worksheet
DPMP-PRO-01-F2	Data Inventory Map

ANNEXES

Annex A	Risk Register
Annex B	Risk Assessment Framework

THE SOFTWARE PRACTICE PTE LTD	No of Pages	10 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION IMPACT ASSESSMENT & RISK ASSESSMENT	Doc No	DPMP-PRO-01
	Revision	1.0

ANNEX A – RISK REGISTER

Obligations	Examples of PDPA non-compliance
Consent	Failure to obtain consent, forced consent / no choice given, withdrawal of consent prohibited, no consent given for disclosure to third parties so consent to third parties is unauthorised, indiscreet conversations, misleading purpose, unauthorised secondary purpose, negligent usage / misuse, illegal collection
Notification	Notification required but not given
Purpose Limitation	Unreasonable/excessive collection in view of the stated purpose
Accuracy	Inaccurate/outdated data Error in processing
Retention Limitation	Unlimited Retention, Improper disposal
Protection	Unsecured handling of personal data, failure to have adequate cybersecurity measures to protect personal data, failure to have policies and processes to protect data, insecure transmission of data
Access & Correction	Denial of access to or correction of personal data without reasonable basis
Transfer Limitation	Failure to ensure that personal data is transferred to another country only according to the requirements prescribed under the PDPA.
Accountability	No DPO appointed, no documented internal policies and processes
Data Breach Notification	No documented process for managing data breach and notification requirements
DNC	Failure to check the relevant DNC registry before sending a marketing message.

Some causes of cyber security incidents or personal data breaches

Hacking, Unauthorised Access of databases
Malware (viruses, spyware)
Social Engineering (Phishing scams, malware in email)
Loss or theft of devices
Failure/weakness of program code resulting in personal data revealed to incorrect parties
Compromised network devices
Not disposing electronic data properly
Unintended recipient

THE SOFTWARE PRACTICE PTE LTD	No of Pages	11 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION IMPACT ASSESSMENT & RISK ASSESSMENT	Doc No	DPMP-PRO-01
	Revision	1.0

Risks relating to the Data Lifecycle Stages

Collection	Is there excessive or unauthorised collection? Are there any “sensitive” data collected? Is the individual notified of purpose and consent given?
Storage	Is the storage and backup location outside Singapore? Is the data secured or encrypted? Is there controlled access? Are there online threats?
Use	Are the purposes for processing data reasonable? Are there secondary purposes you are not aware of? Is the person authorised to process the data? Are there incidents of employee negligence? Are the client instructions complied with?
Disclosure	Are there any unauthorised disclosure of data? Is there excessive disclosure of personal data? Can the vendor be trusted? Is there a contract in place with the vendor? Are there risks with vendors located outside Singapore? Are the client instructions complied with?
Disposal	Is the data disposed securely? Are the client instructions complied with?
Archival	Is the data secured or encrypted? Is there controlled access? How long is the data retained? Are there online threats? Is the storage and backup location outside Singapore?

Risks relating to Data Intermediaries

IT system/network of data intermediary hacked
Unauthorised disclosure of personal data by the data intermediary
Data intermediary staff not complying with data intermediary’s information security policy or practices
Insufficient information security controls in the data intermediary’s IT system
Poor or no written contract between the organisation and the data intermediary leading to violation by the data intermediary of the organisation’s information security requirements and
Lack of oversight by organisation

THE SOFTWARE PRACTICE PTE LTD	No of Pages	12 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION IMPACT ASSESSMENT & RISK ASSESSMENT	Doc No	DPMP-PRO-01
	Revision	1.0

ANNEX B – RISK ASSESSMENT FRAMEWORK

	1= Rare	2= Unlikely	3=Possible	4=Likely	5=Almost Certain
Likelihood	Remote and not conceivable	Conceivable but no indication or evidence to suggest possibility of occurrence in the near term	Indication suggests possibility of occurrence in the near term	Indications suggest expected occurrence in the near term	Indications suggest high probability of occurrence in the near term

	1=Insignificant	2= Minor	3=Moderate	4=Major	5=Severe
Impact	Remote and no impact	May experience inconvenience, but no indication or evidence to suggest major damage which will result in financial / reputation loss	Experience some inconvenience or consequences, however indications suggest damage can be overcome or recovered in a short time	Experience significant consequences, indications suggest damage will be widespread resulting in loss of financial, reputation and support from stakeholders	Experience severe consequences, indications suggest that damage sustained may see organisation not be able to operate as usual for a prolonged period of time, or which they may not be able to overcome.

Risk Classification

- HIGH – Risk Likelihood X Risk Impact = 12 to 25 inclusive
- MEDIUM – Risk Likelihood X Risk Impact = 5 to 10 inclusive
- LOW – Risk Likelihood X Risk Impact = 1 to 4 inclusive

