

THE SOFTWARE PRACTICE PTE LTD	No of Pages	1 of 7
	Document Classification:	Internal
	Effective Date	10 June 2024
EXTERNAL PROVIDER DUE DILIGENCE ASSESSMENT & EVALUATION	Doc No	DPMP-PRO-06
	Revision	1.0

AMENDMENTS LOG

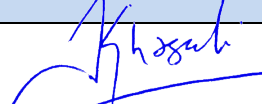
Revision History

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 7
	Document Classification:	Internal
	Effective Date	10 June 2024
EXTERNAL PROVIDER DUE DILIGENCE ASSESSMENT & EVALUATION	Doc No	DPMP-PRO-06
	Revision	1.0

Contents

AMENDMENTS LOG 1

RECORDS FOR DOCUMENT REVIEW 3

PURPOSE 4

SCOPE 4

DEFINITION 4

PROCEDURE 4

FORMS 7

THE SOFTWARE PRACTICE PTE LTD	No of Pages	3 of 7
	Document Classification:	Internal
	Effective Date	10 June 2024
EXTERNAL PROVIDER DUE DILIGENCE ASSESSMENT & EVALUATION	Doc No	DPMP-PRO-06
	Revision	1.0

RECORDS FOR DOCUMENT REVIEW

To ensure the continuing suitability, adequacy and effectiveness of the documented information and its relevancy, a review of its contents should be conducted at a planned interval or when significant changes occur. The review should include assessing opportunities for improvement of the documented information and the approach to managing data protection in response to changes to the organization environment, business circumstances, legal conditions as well as the technical environment.

Instruction Guide:

Version 1.0, 2.0, 3.0... Version changed with amendments

Version 1.0 Version remained unchanged but update the last and next date of review

VERSION	REVIEW BY	DATE OF REVIEW	NEXT REVIEW DATE
1.0	Edwin Soedarta (DPO) Khasali M (Director)	10 June 2024	9 June 2025

THE SOFTWARE PRACTICE PTE LTD	No of Pages	4 of 7
	Document Classification:	Internal
	Effective Date	10 June 2024
EXTERNAL PROVIDER DUE DILIGENCE ASSESSMENT & EVALUATION	Doc No	DPMP-PRO-06
	Revision	1.0

PURPOSE

This document describes how due diligence assessment of external providers will be carried out, and how their compliance with their contractual obligations will be evaluated within the context of the personal data protection obligations.

SCOPE

This applies to external providers also referred to as “data intermediaries” engaged by the organization to handle or process personal data on its behalf.

DEFINITION

Data Intermediary An organization which processes personal data on behalf of another organization but does not include an employee of that organization.

RESPONSIBILITIES AND AUTHORITIES

The Top Management has the prime responsibility and approval authority for this procedure.

The Data Protection Officer (“DPO”) together with the respective process owners are responsible to ensure appropriate due diligence of external providers and evaluation of their performance with respect to management of personal data.

PROCEDURE

A. Due Diligence Assessment

The following steps shall be followed before the decision to engage the external provider, and any commitment, is made.

1. Top Management shall establish to what extent the external provider meets the requirements for the product or service. If sufficient requirements are not met, the external provider should not be used, and this procedure terminates.
2. The DPO shall find out what information is available about the data protection security controls used by the external provider including, but not limited to personal data protection policy, appropriate use and disclosure, security safeguards, data breach management and notification, handling of complaints, server location, retention and disposal, and relevant

THE SOFTWARE PRACTICE PTE LTD	No of Pages	5 of 7
	Document Classification:	Internal
	Effective Date	10 June 2024
EXTERNAL PROVIDER DUE DILIGENCE ASSESSMENT & EVALUATION	Doc No	DPMP-PRO-06
	Revision	1.0

compliance with applicable industry standards like DPTM, APEC-CBPR or APEC-PRP, ISO/IEC 27001, ISO/IEC 27701.

3. When all relevant information has been obtained and recorded, reach a decision about whether the external provider should be contracted with approval from The Management. The DPMP-PRO-06-F1 External Provider Due Diligence Assessment Form must be completed for this purpose.
4. The organization shall establish a contractual agreement with the external provider to ensure personal data disclosed to them will only be used within the scope of the agreement and not to be used or disclosed for other purposes.
5. To satisfy item number 4 above, the organization shall ensure that the contract with the external provider includes a confidentiality clause, or the external provider may be required to sign a non-disclosure agreement (NDA). Additionally, the external provider shall be required to sign a Data Processing Agreement which may include, but not limited to:
 - Appointing an individual to be responsible for overall compliance with the data protection requirements.
 - Defining the purpose of collection, use and disclosure of the personal data limited to fulfilling its obligations and providing the services required in the contract.
 - Creating policies and procedures for the handling of personal data and complying with their contractual obligations.
 - Giving the organization the right to monitor compliance of the external provider relating to the contractual terms.
 - Restricting the external provider from further disclosing or transferring personal data without the explicit written instruction or approval of the organization.
 - Seeking evidence or declaration from the external provider that it has processes in place to assess sub-contractor's data handling practices and ensure it complies with the data protection requirements stipulated in the contract in case engagement of sub-contractor is allowed by the organization.
 - Making reasonable security arrangements to meet the required level of protection of personal data (to prevent unauthorized access, collection, use disclosure, copying, modification, disposal, or similar risks).
 - Including breach notification obligation and requirements to assist organization in containing / assessing the breach.
 - Defining data retention, disposal, and mechanisms for the personal data so that the external provider can cease to retain the personal data when the purpose of the data is no longer being served and retention is no longer necessary for legal or business purposes.
 - Including the obligation to notify the organization of any inaccurate, incomplete, or outdated personal data disclosed to them.

In the event that a Data Processing Agreement cannot be signed by the external provider, the external provider shall be required to submit their justification for their refusal to sign and

THE SOFTWARE PRACTICE PTE LTD	No of Pages	6 of 7
	Document Classification:	Internal
	Effective Date	10 June 2024
EXTERNAL PROVIDER DUE DILIGENCE ASSESSMENT & EVALUATION	Doc No	DPMP-PRO-06
	Revision	1.0

their acknowledgement in black and white (e.g., e-mail) that they will comply with PDPA in line with their established Privacy Policy.

- For cloud service providers (CSPs) where no physical agreement such as NDA or Data Processing Agreement is signed, the organization shall review the CSP's data processing or equivalent arrangements such as its Terms & Conditions, and privacy and security policies to ensure it includes appropriate policies and practices on its management of the organization's personal data that meet the standards of protection in processing personal data as well as the relevant compliance with applicable industry standards like DPTM, APEC-CBPR or APEC-PRP, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27017, ISO/IEC 27018, Tier 3 of the Multi-Tiered Cloud Security (MTCS), etc. The DPMP-PRO-06-F2 Cloud Service Provider Questionnaire must be completed for this purpose by the DPO.

B. Evaluation of Compliance

Several ways may be used in evaluating whether the external providers are meeting their contractual obligations. This can be demonstrated by any of the following, whichever is the most appropriate for the nature of the engagement.

- The external provider may provide the organization with their self-assessment report or internal audit report that its practices meet the contractual obligations. Where required, the organization may perform an audit or inspection of the external provider to verify that they are carrying out its roles and responsibilities properly.
- The external provider may provide the organization with an independent report or certification assessed by an independent auditor.
- The organization may evaluate the external provider using the DPMP-PRO-06-F4 External Provider Performance Evaluation.

Evaluation through any of the above shall be done at least once a year for contract duration exceeding 1 year or at the end of the contract if duration is less than 1 year prior to any renewal.

For any non-compliance noted during the evaluation, the external provider will be given 30 calendar days to rectify the findings unless reasonable justification is provided for extension of the timeline. If no rectifications have been made as per the agreed timeline, the external provider shall be delisted from the DPMP-PRO-06-F3 Approved External Provider / CSP List and the organization may start the due diligence assessment process again to select a replacement, where required.

For CSPs, the organization may rely on the validity of its certification to industry standards like DPTM, APEC-CBPR or APEC-PRP, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27017, ISO/IEC 27018 and may decide to re-assess them using the DPMP-PRO-06-F2 Cloud Service Provider Questionnaire in the event a data breach happens to determine the need for replacement.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	7 of 7
	Document Classification:	Internal
	Effective Date	10 June 2024
EXTERNAL PROVIDER DUE DILIGENCE ASSESSMENT & EVALUATION	Doc No	DPMP-PRO-06
	Revision	1.0

FORMS

- DPMP-PRO-06-F1 External Provider Due Diligence Assessment
- DPMP-PRO-06-F2 Cloud Service Provider (CSP) Questionnaire
- DPMP-PRO-06-F3 Approved External Provider / CSP List
- DPMP-PRO-06-F4 External Provider Performance Evaluation