

THE SOFTWARE PRACTICE PTE LTD	No of Pages	1 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

AMENDMENTS LOG

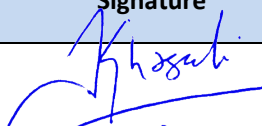
Revision History

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 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

Contents

AMENDMENTS LOG	1
RECORDS FOR DOCUMENT REVIEW	3
1. PURPOSE	4
2. NORMATIVE REFERENCE	4
3. THE ORGANIZATION	4
4. TERMS, DEFINITIONS & SHORT TITLES	5
5. PRINCIPLE 1: GOVERNANCE AND TRANSPARENCY	6
5.1 Appropriate Policies and Practices	6
5.2 Accountability	10
5.3 Communication	10
6. PRINCIPLE 2: MANAGEMENT OF PERSONAL DATA	11
6.1 Appropriate Purpose	11
6.2 Appropriate Notification	11
6.3 Appropriate Consent, Use & Disclosure	12
6.4 Compliant Overseas Transfer	14
7. PRINCIPLE 3: CARE OF PERSONAL DATA	15
7.1 Appropriate Protection, Retention and Disposal	15
7.2 Retention and Disposal	16
7.3 Accurate and Complete Records	17
8. PRINCIPLE 4: INDIVIDUALS' RIGHTS	19
8.1 Effect Withdrawal of Consent	19
8.2 Provide Access and Correction Rights	19
8.3 Data Breach Notification	20

THE SOFTWARE PRACTICE PTE LTD	No of Pages	3 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

RECORDS FOR DOCUMENT REVIEW

To ensure the continuing suitability, adequacy, relevancy and effectiveness of this document, a review of its contents should be conducted at least once a year and when significant changes occur. The review should include assessing opportunities for improvement and the approach to managing data protection in response to changes to the organization environment, business circumstances, legal conditions as well as 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 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

1. PURPOSE

This manual defines how a Data Protection Management Programme (DPMP) is established, managed, monitored and maintained within The Software Practice Pte Ltd. It covers management policies and processes for the handling of personal data as well as defined roles and responsibilities to manage our data protection risks and comply with our obligations with respect to Singapore’s Personal Data Protection Act (PDPA), giving our stakeholders the confidence that their personal data is secure and well managed.

Our DPMP is developed and established to comply with the Data Protection Trustmark Certification requirements. The DPTM Certification framework was developed based on adopting and aligning it with Singapore’s PDPA and incorporating elements of international benchmarks and best practices. The requirements are organized around 4 Principles, and each principle is framed by a set of assessment criteria with controls under each criterion. The 4 Principles are outlined below:

- Principle 1: Governance and Transparency
- Principle 2: Management of Personal Data
- Principle 3: Care of Personal Data
- Principle 4: Individuals’ Rights

2. NORMATIVE REFERENCE

This Data Protection Management Programme (DPMP) references the guidelines presented by Personal Data Protection Commission (PDPC) Singapore (<https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines>) and Infocomm Media Development Authority (IMDA) (<https://www.imda.gov.sg/programme-listing/data-protection-trustmark-certification>), and adheres to related acts and laws enacted by the Government of Singapore and general administrative policies of The Software Practice Pte Ltd.

3. THE ORGANIZATION

The Software Practice Pte Ltd is a technology company based in Singapore that builds sophisticated web and mobile applications for Enterprises and Government Agencies.

Our company location is available on <https://thesoftwarepractice.com/contact/>

We collect, use and/or disclose personal data mainly for the following purposes:

- Recruitment
- Employee and Contract Staff (“contractors”) Administration
- Processing of Security Clearance, where needed at the clients’ premises
- CCTV operations
- Photo and video recording for our internal events attended by our internal staff for the purpose of updating our communication materials including social media pages

THE SOFTWARE PRACTICE PTE LTD	No of Pages	5 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

4. TERMS, DEFINITIONS & SHORT TITLES

4.1 Definitions of Personal Data Protection Act

The following are some definitions and interpretations used under the PDPA, the list is not exhaustive, refer to <https://sso.agc.gov.sg/Act/PDPA2012> (and [Personal Data Protection \(Amendment\) Act 2020](#)):

- **Business Contact Information** – means an individual’s name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes.
- **Data intermediary** – means an organization which processes personal data on our behalf. Common examples of data intermediaries in our context include cloud service providers (CSPs) that offers cloud-based services for processing and hosting personal data.
- **Individual** – a natural person, whether living or deceased.
- **Personal Data** – data, covers electronic & non-electronic, whether true or not, about an individual who can be identified from that data; or from that data and other information to which we have or we likely to have access.

4.2 Other Relevant Definitions

- **Audit** – systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled
- **Data Breach** – A data breach refers to an incident exposing personal data in an organization’s possession or under its control to the risks of unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.
- **Data Breach Management Plan** – A process that helps organizations to manage and respond to data breaches more effectively.
- **Data Protection Officer (DPO)** – is an enterprise security leadership role required by PDPA to oversee the data protection responsibilities within the organization and ensure compliance with the PDPA.
- **Policy** – intentions and direction of an organization, as formally expressed by its top management
- **Process** – set of interrelated or interacting activities which transform inputs into outputs
- **Risk assessment** – overall process of risk identification, risk analysis and risk evaluation
- **Risk treatment** – process to modify risk
- **Threat** – a potential cause of an unwanted incident, which can result in harm to a system or organization
- **Vulnerability** – weakness of an asset or control that can be exploited by one or more threats

THE SOFTWARE PRACTICE PTE LTD	No of Pages	6 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

5. PRINCIPLE 1: GOVERNANCE AND TRANSPARENCY

The Software Practice Pte Ltd shall have appropriate data protection policies and practices implemented to manage personal data, and these policies and practices shall be communicated to relevant stakeholders.

5.1 Appropriate Policies and Practices

5.1.1 We have established appropriate data protection policies and practices on managing personal data including management of special categories of personal data such as personal data of sensitive nature, and by external parties engaged by us, e.g., data intermediaries, throughout the data lifecycle from the collection, storage, use, disclosure, archival to disposal. Reference shall be made to our DPMP-POL-01 Data Protection Governance Policy.

5.1.2 When engaging third parties to handle or process personal data on our behalf, we will ensure that these third parties do so in accordance with our policies and practices. We will clearly communicate personal data protection requirements through a binding contractual agreement highlighting their protection and retention obligations among other responsibilities they have in the processing of personal data. We will conduct regular reviews to ensure external providers' compliance as per the procedure DPMP-PRO-06 External Provider DDA & Evaluation.

5.1.3 We have established an appropriate governance structure for management oversight and endorsement of our policies and practices on the management of personal data. A Data Protection Committee has been established for the above purpose.

- The Management – The Company's Director who is overall accountable to ensure that the organization complies with PDPA, appoint a Data Protection Officer (DPO), approved the organization's data protection policies and Data Protection Management Programme (DPMP), and commission Data Protection Impact Assessment (DPIA).
- Data Protection Officer – appointed to oversee the data protection policies, practices and information security measures within the organization and ensure compliance with the PDPA. Reference shall be made to the actual appointment letter.
- Data Protection Committee Member – to assist the DPO in implementing personal data protection measures and ensuring employee awareness of our data protection and information security policies and practices. Reference shall be made to the actual appointment letter.

5.1.4 Awareness of the policies and practices of all relevant stakeholders to whom the policies and practices apply shall be ensured by the DPO. The following training plan shall be used as a guide to ensure awareness of relevant stakeholders.

What to train?	When to train?	Who to train?	Why must they be trained?	How to train?
PDPA and its implications for the organization;	• At the start of the organization's PD	• The Management (Director)	• Awareness and support of PD protection risks	• PDPC's E-learning module

THE SOFTWARE PRACTICE PTE LTD	No of Pages	7 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

Table 1 – Training Plan				
What to train?	When to train?	Who to train?	Why must they be trained?	How to train?
Role of the management team; Any significant amendments to the PDPA, the management role and organization’s policies and relevant practices; Risk Register and information security arrangements	<ul style="list-style-type: none"> compliance journey Prior to or when amendments in PDPA and the organization’s policies and practices take effect At the completion of the risk register and any review or changes in it 		<ul style="list-style-type: none"> Signoff on the risk register Highlight the importance of personal data protection and the implication of data breaches Highlight the key roles of management in personal data protection and information security 	<ul style="list-style-type: none"> Shared Drive / internal circular/email to inform and update on new or revised DP policies and practices Internal briefing by DPO
Data Protection Management Programme (DPMP) covers applicable policies, notices, processes, data protection and information security policies and measures	<ul style="list-style-type: none"> On-boarding of new staff on the first day At least once a year refresher Ad-hoc when there is a revision to DPMP Upon assignment to a specific job role or change in role/job scope 	<ul style="list-style-type: none"> All employees Contract staff that handles personal data 	<ul style="list-style-type: none"> Educating them on the DPMP and their contribution to the effectiveness of DPMP Educating them on information security policies and measures 	<ul style="list-style-type: none"> Internal briefing by DPO PDPC’s E-learning module Training by external training providers, if needed Shared Drive / internal circular/email to inform and update on new or revised DP policies and practices
Fundamentals of PDPA / DPO Practitioner Training PDPA Awareness	<ul style="list-style-type: none"> Upon appointment 	<ul style="list-style-type: none"> DPO DPC Members 	<ul style="list-style-type: none"> Understand the DPO / DPC role and responsibilities Understand PDPA and how to operationalize its requirements to ensure organization compliance 	<ul style="list-style-type: none"> Training by approved external training providers for the Fundamentals of PDPA Internal briefing by DPO / PDPC’s E-learning module
Applicable data protection obligations and information security requirements	<ul style="list-style-type: none"> At the start of engagement 	<ul style="list-style-type: none"> External Providers with personal data involvement 	<ul style="list-style-type: none"> Address DP obligations and information security requirements 	<ul style="list-style-type: none"> Confidentiality and Personal Data Protection Agreement to be explained to them prior to signing

5.1.5 Policies and/or notices for stakeholders shall be made available at the points of collection and use, and more information about it shall be provided upon request. These policies and practices are easily accessible and provided clearly and concisely, clearly worded for easy understanding by the recipients of the information. Internal policies and practices are maintained by the DPO and made available in our shared drive for staff reference.

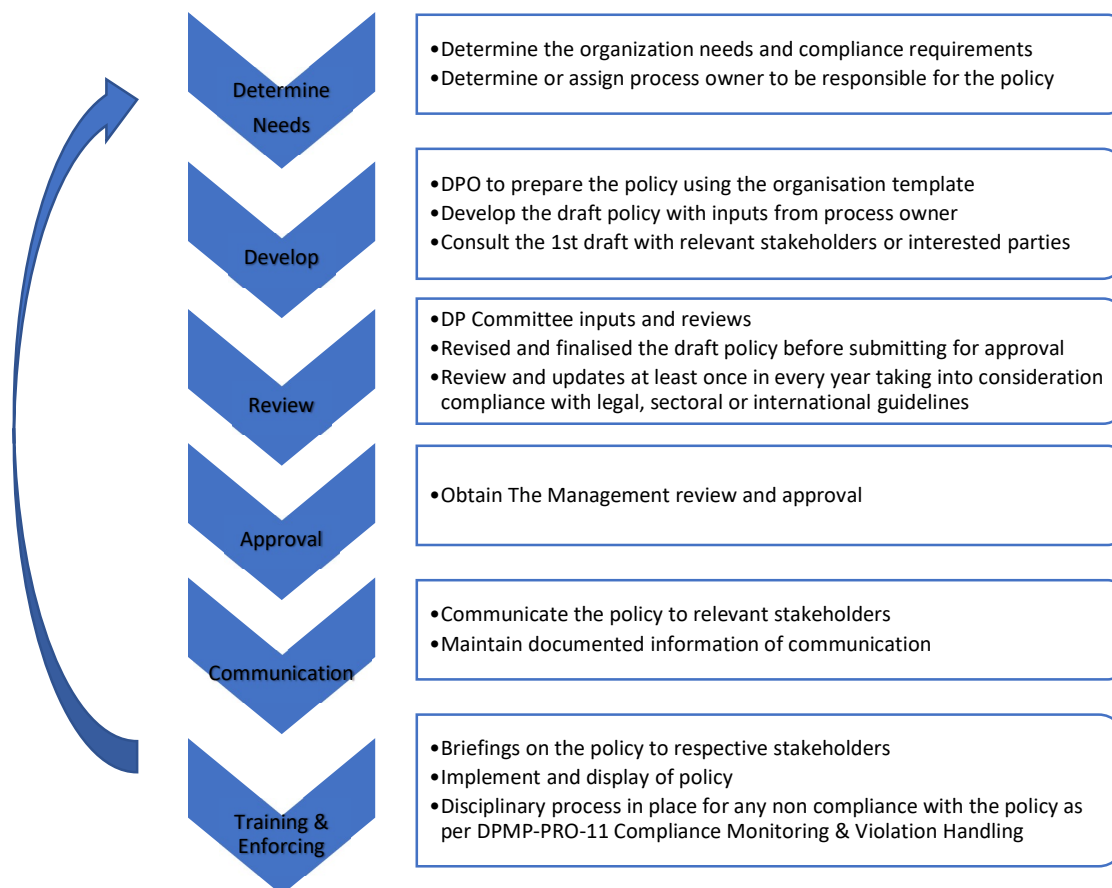
THE SOFTWARE PRACTICE PTE LTD	No of Pages	8 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

5.1.6 Policies and practices shall be reviewed and updated, if necessary, at least once a year, and as and when there is any change in processes, systems, services, emerging technologies, significant feedback from stakeholders, or any changes in legal, regulatory requirements, relevant sectoral and international guidelines to ensure suitability, adequacy and relevancy of the policies and practices. All changes shall be properly documented in the amendment log page of the policy or process document and shall be endorsed by the management.

5.1.7 For any change, the Top Management and the DPO shall assess the need to conduct a DPIA in line with DPMP-PRO-01 Data Protection Impact Assessment and Risk Assessment.

5.1.8 Updated policies and practices shall be communicated within 1 month to all relevant stakeholders as per the Training Plan above, and to other stakeholders as soon as reasonably possible (e.g., updating of the Privacy Statement on the website, addendum agreement for external providers).

5.1.9 The following flowchart describes the “policy lifecycle” for the review, updating and communication process.



Flow 1: Policy Review, Update & Communication Process

THE SOFTWARE PRACTICE PTE LTD	No of Pages	9 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

5.1.10 We will monitor our compliance with data protection policies and practices regularly through the following activities such as:

- Conducting quarterly inspection
- Conducting yearly internal audit
- Maintaining Data Protection Trustmark Certification through an assessment by an accredited assessment body

Reference shall be made to DPMP-PRO-11 Compliance Monitoring & Violation Handling.

5.1.11 The DPO will document the outcomes of all reviews and report to the top management.

5.1.12 We have established a process for handling queries and complaints that may arise with respect to the organization's collection, use or disclosure of personal data. Reference shall be made to DPMP-PRO-02 Handling Complaints & Queries. This process shall be made readily available to stakeholders including how to contact the organization for any queries or complaints and more information shall be provided upon request.

5.1.13 We have established a process to respond to requests to disclose personal data to public agencies, courts and law enforcement agencies when required for purposes of investigations or proceedings under the PDPA or other written law. Reference shall be made to DPMP-PRO-10- Personal Data Sharing, Transfer & Disclosure.

5.1.14 We have established a process to identify, assess and address data protection risks as per procedure DPMP-PRO-01 Data Protection Impact Assessment and Risk Assessment.

5.1.15 We consider data protection across the various stages of the design and development of a service, system or process. This includes, but is not limited to:

- Conducting DPIA to review its existing system thoroughly, considering what personal data is being collected and whether the collection is completely necessary.
- Implementing relevant data protection by designing good practices to better protect personal data and reduce the risks identified.
- Taking steps to ensure that data protection settings protect users by default.

Reference shall be made to Acceptable Use Policy v1.12

5.1.16 We have established a data breach management plan to comply with the mandatory data breach notification requirements as per procedure DPMP-PRO-03 Data Breach Management.

5.1.17 We have established a Data Protection ("DP") Committee as per section 5.1.3 of this manual, with appointment letter(s) endorsed by our Director to clearly define and document their data protection responsibilities. The DPO shall be responsible for ensuring the organization's overall compliance with the data protection obligations, and shall receive relevant training on data protection compliance with the PDPA (e.g., attended data protection training or obtained data protection certifications).

THE SOFTWARE PRACTICE PTE LTD	No of Pages	10 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

5.2 Accountability

- 5.2.1 Our DPO business contact information is readily accessible and operational during Singapore business hours. We have registered our DPO in ACRA BizFILE including the DPO contact information.
- 5.2.2 The business contact information of the DPO is also reflected in our website privacy policy and other applicable means which is available and easily accessible to the intended audience (e.g., relevant data protection notices).

5.3 Communication

- 5.3.1 We have established a process to communicate or make available data protection policies, practices and relevant matters to internal stakeholders such as the management and employees. Our DPO shall ensure that communication is happening as per the table below.

Internal Stakeholders	When to communicate	What to communicate	How to communicate
The Management	During the yearly management reporting and if significant changes occur	Policies and relevant practices Risk Register DPMP performance	Yearly Management Reporting and ad-hoc reporting if significant changes occur
	Quarterly signoff from management	Quarterly Compliance Inspection	Management signoff on the quarterly compliance checklist once conducted
	In the event of a data breach	Data breach and action plans	Management reporting through the data breach report and log
All Employees Contract Staff that handles personal data	Yearly and if significant changes occur	Policies and relevant practices Any significant changes	Yearly refresher briefing to be conducted by the DPO; Any significant changes (ad-hoc changes) to be communicated through email, internal circulars or postings
	If significant findings relevant to employees / contract staff are noted during the quarterly inspection and yearly internal audit	Significant findings during quarterly compliance inspection and yearly internal audit	To be communicated through email, internal circulars or postings, or through arranged briefings by the DPO
New Hires	First Day on Board	DP Notice for Employees and Contract Staff Policies and relevant practices Relevant client instructions (where applicable)	Employee On-boarding (orientation) to be conducted by HR and DPO

- 5.3.2 Our DPO shall ensure that relevant policies are communicated and/or made available to external stakeholders as per the table below.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	11 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

External Stakeholder	When to communicate	What to communicate	How to communicate
Public / General Enquirers / Customers	During the enquiry stage and upon request / when visiting our website	Privacy Policy	Website
External Providers (a.k.a. Data Intermediaries)	At the start of engagement	Confidentiality and Personal Data Protection Agreement	Requiring them to sign the Confidentiality and Data Protection Agreement to inform them of our requirements
Job Applicants	When applying for a position	DP Notice for Job Applicants	Copy of notice to be attached to the Job Application Form

6. PRINCIPLE 2: MANAGEMENT OF PERSONAL DATA

6.1 Appropriate Purpose

6.1.1 We have established DPMP-POL-01 Data Protection Governance Policy to give the principles and guidelines on data being collected. We shall ensure that personal data collected (including, where relevant, personal data of a sensitive nature) are limited to which are necessary to meet the specified purpose(s), and that the purposes are appropriate and consistent with requirements under the PDPA.

6.1.2 We shall limit the collection of personal identifiers (e.g., NRIC, FIN and other government-issued IDs) only to necessary purposes permitted under the law or when necessary to accurately establish or verify the identity of the individual to a high degree of fidelity e.g., employment purposes and for processing of security clearance at clients' premises (clients requesting for this are generally public agencies or those residing in restricted zones or highly restricted secure premises)

6.1.3 We shall clearly identify and document the types of personal data (including sensitive data where applicable) collected from individuals, the sources, and the respective purposes for collecting and processing the personal data in the form of a data inventory map (DIM).

6.1.4 Policies and procedures on personal data collection, use or disclosure and the data inventory map will be reviewed at least once a year and when significant changes occur to ensure that the purposes for which collection of personal data are still necessary and appropriate. The review shall take into consideration the types of personal data collected in relation to the purposes identified. Reference shall be made to DPMP-PRO-07 Consent, Purpose and Notification.

6.2 Appropriate Notification

6.2.1 We ensure clear and concise notifications to individuals of the purposes for collecting their personal data on or before collecting their PD. Clear and concise notification in a written form (which may be an electronic or physical copy) shall be provided through the following mechanisms:

THE SOFTWARE PRACTICE PTE LTD	No of Pages	12 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

Audience	Notification
Job Applicants	Data Protection Notice for Job Applicants
Employees and Contract Staff	Data Protection Notice for Employees and Contract Staff
Clients, Website Users, General Enquirers and the Public	Website Privacy Policy

- 6.2.2 Through the mechanisms above, we will provide information relating to:
- The collection, use or disclosure of their personal data and its intended purposes for them to make informed decisions on or before collecting the personal data;
 - Any purposes for use or disclosure of personal data which has not been informed, before such use or disclosure of personal data for that purpose;
 - How individuals may exercise choice in the collection, use or disclosure of their personal data;
 - If the collection is obligatory or optional to provide a particular service or to fulfill a particular purpose; and
 - Consequences of not providing the personal data necessary for a transaction or service.

6.2.3 In the event the PD collected may be disclosed to third parties, we will provide clear and concise notifications to individuals.

6.2.4 In the event that PD is to be used or disclosed for a new or different purpose(s), we shall notify the affected stakeholders and obtain consent from the individuals for the use or disclosure of their PD for new purposes.

6.2.5 Requestor for the new or different purpose shall fill in the Management of Change (MOC) Form for DPO review and Director approval as per the procedure DPMP-PRO-07 Consent, Purpose and Notification. MOC Form will be used to ensure relevant policies, procedures, documents and forms are reviewed and updated accordingly. Respective relevant stakeholders affected by the change will be notified.

6.3 Appropriate Consent, Use & Disclosure

6.3.1 The organization shall obtain individuals' consent for the collection, use and disclosure of their personal data through the following mechanisms:

Process where PD collected	Purpose of collection	How is consent being collected	Evidence
Recruitment	Evaluation of Job fit	Job Application Form with consent declaration DP Notice for Job Applicants	<ul style="list-style-type: none"> • Signed Job Application Form • Signed DP Notice for Job Applicants
Employees and Contract Staff	HR and payroll administrative processes; Processing of security clearance at clients' premises, if required;	Employment Contract with PDPA clause DP Notice for Employees and Contract Staff	<ul style="list-style-type: none"> • Signed Employment Contract / Letter of Offer • Signed DP Notice for Employees and Contract Staff

THE SOFTWARE PRACTICE PTE LTD	No of Pages	13 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

	Photo and video recording during company events for company communication materials and official social media pages		
Clients, Website Users, General Enquirers and the Public	Answering enquiries / requests	Consent declaration in relevant PD collection forms e.g., request form, complaint form	<ul style="list-style-type: none"> Opt-in checkbox in the collection form or deemed consent declaration in case opt-in checkbox is not feasible

6.3.2 If we are to rely on deemed consent, we shall demonstrate and document how the individual has deemed to consent to the collection, use or disclosure of personal data through:

- Deemed consent by conduct, where the individual voluntarily provides personal data and the purposes are limited to those that are objectively obvious and reasonably appropriate from the surrounding circumstance (e.g., when applying in a 3rd party job search platform, or our career page)
- Deemed consent by contractual necessity, where consent may be deemed to be given for disclosure of the personal data from one organization to another for the necessary conclusion or performance of a contract/transaction (e.g., security clearance processing in client premises); and
- Deemed consent by notification, where consent may be deemed if the organization notifies the individuals of the purpose and gives a reasonable period by which to opt-out, and the individual does not opt out within the period. If the organization is to rely on deemed consent by notification, the organization must conduct an assessment to ensure that the collection, use or disclosure of personal data is not likely to have an adverse effect on the individuals. When conducting the assessment, reference shall be made to [DPMP-PRO-07 Consent, Purpose and Notification](#).

Note: We will not rely on deemed consent by notification for the purposes of sending direct marketing messages to the individuals. We will obtain a clear and unambiguous (e.g., opt-in consent checkbox) consent for such activity.

6.3.3 If we are to collect without consent personal data pursuant to an exception under the PDPA or as required/authorized under any other written law, we shall conduct a risk assessment to identify and mitigate adverse effects for certain uses of personal data. When conducting the assessment, reference shall be made to [DPMP-PRO-07 Consent, Purpose and Notification](#). This may be applicable during the following situations:

- Vital interests of the individual for contacting the next-of-kin or emergency contact person of any injured, ill or deceased individual.
- Detecting or preventing illegal activities or threats to physical safety or security, IT and network security, preventing misuse of services, and carrying out other necessary corporate due diligence e.g., the collection, use or disclosure of personal data for the consolidation of official watch lists.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	14 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

6.3.4 We shall ensure that the person providing consent on behalf of an individual is validly acting on behalf of the individual e.g., authorized representative. We will verify that the person providing consent on behalf of the individual is validly acting on behalf of the individual through:

- Verifying the identity through supporting documents e.g., authorization letters, proof of relationship
- Notifying the purposes to the person acting on behalf of the individual for which the individual's personal data will be collected, used and disclosed
- Validating that the individual has given consent for those purposes

6.3.5 In the event that we need to collect personal data from third-party sources, we shall exercise due diligence to ensure valid collection of personal data such that necessary consent has been obtained from the individuals by the third parties on the disclosure of their personal data to the organization (e.g., when there is a need to engage recruitment agency). The organization may establish contractual agreements with the third-party sources or obtain confirmation in writing from the third party on consent obtained or obtain a copy of the document containing or evidencing that consent has been obtained from individuals within the scope of the specified purposes.

6.3.6 We have established a principle and governance on appropriate management of personal data including what, when, why, who and how the personal data should be collected, the purpose of collection, use, disclosure and disposal.

- Organization-wide internal policy covering different areas of data protection and information security
- Website Privacy Policy
- Several notices depending on the audience e.g., DP Notice for Employees and Contractors, DP Notice for Job Applicants

6.4 Compliant Overseas Transfer

6.4.1 We will keep track of any personal data that need to be transferred overseas, if any, and the recipients of the transferred data including the jurisdiction or country where the recipient is located. Refer to DPMP-PRO-10 Personal Data Sharing, Transfer & Disclosure.

6.4.2 For any overseas disclosure / transfer, we shall take appropriate steps to ensure that the recipient overseas is bound by legally enforceable obligations or have valid relevant privacy certifications or has signed a Personal Data Processing Agreement with us to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA.

6.4.3 For use of any cloud service provider (CSP) where the server may be located overseas, we shall ensure its cloud security and complete a Cloud Service Provider (CSP) Questionnaire for this purpose to ensure that personal data which will be hosted in the cloud are protected in line with the requirements of PDPA.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	15 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

7. PRINCIPLE 3: CARE OF PERSONAL DATA

7.1 Appropriate Protection, Retention and Disposal

7.1.1 We have put in place appropriate security policies, practices and measures to secure personal data in its possession or under its control to prevent any unauthorized access, collection, use, disclosure or similar risks. The summary of general technical, physical and administrative controls we implement for data protection can be found in DPMP-PRO-09 Physical and Administrative Security and Acceptable Use Policy v1.12.

7.1.2 We shall conduct relevant risk assessments to identify, assess and address personal data protection and security risks and implement appropriate security measures to safeguard against data protection risks. This risk assessment shall be conducted in line with DPMP-PRO-01 Data Protection Impact Assessment & Risk Assessment.

7.1.3 We shall ensure that Data Protection by Design (DPbD) principles are followed and embedded into our practices to better safeguard personal data. The principles and best practices are described in Acceptable Use Policy v1.12.

7.1.4 We have assigned and allocated security responsibilities to relevant stakeholders in accordance with our security policies, practices and measures and with details documented in the following:

- The management responsibilities and Data Protection Committee (DPC) as per section 5.1.3 of this manual.
- Appointment letter for DPO;
- Information security responsibilities as documented in our DPMP-POL-02 Policies for Information Security, Acceptable Use Policy v1.12, and DPMP-PRO-03 Data Breach Management;
- Compliance checks, audits, management reporting and violation handling as documented in DPMP-PRO-11 Compliance Monitoring & Violation Handling;
- Confidentiality and Personal Data Processing Agreements signed by external parties, where applicable.

7.1.5 Briefing on policies and practices will be conducted internally at least once a year by the DPO for all staff, and when significant changes occur. Communication of relevant policies, practices, or notices to external stakeholders shall be carried out promptly as appropriate (e.g., upon engagement).

7.1.6 These security policies, practices and measures are monitored, reviewed, updated and endorsed at least once a year and when significant changes occur by the management and are communicated to all relevant internal and external stakeholders promptly. The reviews should keep abreast of the changes and developments within (e.g., new systems or processes, feedback from stakeholders, etc) and outside our organisation (e.g., emerging new technologies, revisions to relevant laws and regulations, international or industry guidelines, etc).

THE SOFTWARE PRACTICE PTE LTD	No of Pages	16 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

7.1.7 In the event a third party is engaged and personal data is involved, we will establish an arrangement (e.g., Personal Data Processing Agreement) with these third parties to notify us promptly when they become aware of an occurrence of a breach of data protection or security of our personal data, and to address/rectify the security failure as soon as practicable. When engaging a CSP where a physical agreement cannot be signed, we will review the CSP's data processing or equivalent arrangements and security policies to ensure they meet the standards of protection in processing personal data as DIs (e.g., industry standards like ISO27001, ISO 27701, Tier 3 of the Multi-Tiered Cloud Security (MTCS) Certification Scheme, etc). Due diligence assessment of external providers shall be carried out and their performance shall be evaluated in line with DPMP-PRO-06 External Provider DDA & Evaluation.

7.1.8 A third party-listing to whom we disclose personal data and the purposes, contracts/requirements and applicable period for the contract/agreement will be maintained and updated in line with DPMP-PRO-10 Personal Data Sharing, Transfer & Disclosure.

7.1.9 Quarterly compliance check and yearly internal audit shall be done to verify and ensure the effectiveness of security measures, policies, procedures and practices. We shall make appropriate modifications and update our security policies, practices and measures based on the verification results from these activities and report the verification results, modifications and action plan to the management.

7.1.10 Ad-hoc reviews may be conducted during the policies and procedures periods when there are significant changes to business operations, processes, systems or services. This shall be facilitated by the DPO and the The Management.

7.2 Retention and Disposal

7.2.1 Specific retention periods are set out for various types of personal data in our possession or under our control. The retention periods shall be based on the purposes for which the personal data was collected and other legal or business purposes.

7.2.2 The retention periods are documented in the DIM and the DPMP-PRO-08-F1 PD Retention List.

7.2.3 We implement a process to ensure we cease to retain personal data in our possession or under our control, as soon as the purpose for which personal data was collected is no longer being served and retention is no longer necessary for legal or business purposes. Reference shall be made to DPMP-PRO-08 Data Retention & Destruction Process.

7.2.4 We will clearly define, document and inform via contractual agreements or data processing agreements or through confirmation from the third party on the data retention periods, data disposal methods and mechanisms for various sets and types of personal data disclosed to third parties (e.g., DIs), so that third parties can cease to retain personal data when the purpose of the data is no longer being served and retention is no longer necessary for legal or business purposes.

7.2.5 We will make information available to individuals on how to request information about the retention and disposal of their personal data such as the duration and the purposes for which

THE SOFTWARE PRACTICE PTE LTD	No of Pages	17 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

their personal data is retained by us, and how we will destroy all personal data once the retention period is over. The DPO contact details shall be available in the applicable notices for individuals to request for information about the retention and disposal of their personal data. Queries on retention and disposal will be handled in line with [DPMP-PRO-02 Handling Complaints & Queries](#).

- 7.2.6 Any unsolicited data received by us via our website, or through emails, SMS or any messaging platform will not be retained and will be deleted right away. If received by telephone, the personal data will not be recorded. We shall review documents received by us to ensure that any personal data that we do not need but provided in the document are masked off or anonymized.
- 7.2.7 We will review the retention periods declared in the DIM, notices, and retention list together with the retention policy and processes at least once a year and when significant changes occur to business operations, systems and services to ensure relevancy and currency of the retention periods and retention purposes. The review should keep abreast of the changes and developments within (e.g., new systems or processes, feedback from stakeholders, etc) and outside our organisation (e.g., emerging new technologies, revisions to relevant laws and regulations, international or industry guidelines, etc.).
- 7.2.8 We have in place appropriate processes to cease retention of documents containing personal data, or remove the means by which the personal data can be associated with particular individuals at the end of the retention period. We will implement appropriate data disposal, destruction or anonymization methods to ensure documents are completely destroyed, disposed or deleted irretrievably, or anonymized data (where applicable) does not identify any particular individual. Reference shall be made to [DPMP-PRO-08 Data Retention & Destruction Process](#).
- 7.2.9 Where third-party service providers are engaged to dispose of, destroy or anonymize personal data, we shall take reasonable measures to ensure that the personal data is not disclosed to unauthorized parties during the entire disposal, destruction or anonymization process. They shall be required to sign a non-disclosure agreement or their contractual agreement shall have a confidentiality clause. Furthermore, a data processing agreement will be required for them to sign.

7.3 Accurate and Complete Records

- 7.3.1 We make reasonable effort to verify that personal data under our possession or control is accurate and complete to make decisions that affect individuals to whom the personal data relates in line with the procedure [DPMP-PRO-05 Personal Data Verification Process](#).
- 7.3.2 In the event personal data is obtained from a third party, we shall exercise due diligence to ensure that personal data obtained from third-party sources are accurate and complete. This can be done through obtaining a confirmation from the third-party source that it had verified the accuracy and completeness of that personal data disclosed to the organization or require an undertaking from them or through contractual agreement to ensure that personal data disclosed to the organization is accurate and complete.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	18 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

- 7.3.3 Where there are reasonable grounds for believing that personal data to be used to make a decision affecting the individual is inaccurate, incomplete or outdated, we shall inform the individual on any inaccurate/outdated personal data and require the individual to provide updated data with supporting documents for verification of the accuracy of the personal data before using it.
- 7.3.4 Channels for updating personal data are available for individuals who may request to correct their personal data. Refer to [DPMP-PRO-04 Withdrawal of Consent, Access & Correction Process](#) for further details.
- 7.3.5 Where relevant, we may communicate the corrections to third parties to whom the personal data was disclosed. This can be through notifying third parties via email or through the third-party portal (where available) on changes or deletion of personal data, if required, where there is inaccurate, incomplete or out-of-date information.
- 7.3.6 We shall ensure the accuracy and completeness of personal data that may be disclosed to another organization:
- Using the latest supporting documents to validate whether the data is accurate and up to date before disclosing personal data.
 - Validate with individuals on the accuracy and currency of their data before any disclosure.
 - Checking e-mails recipient list, email body and any attachments to ensure all are accurate and complete before sending. Any attachment with personal data must be password-protected or the email encrypted (where applies) and the email must be deleted once acknowledged by the recipient.
- 7.3.7 We will implement mechanisms for the third party to notify us as soon as practicable of any inaccurate personal data disclosed to them, where applies, through putting an obligation for the third party to notify the organization of any inaccuracy, in the contractual agreement established with the third parties (e.g., personal data processing agreement).

THE SOFTWARE PRACTICE PTE LTD	No of Pages	19 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

8. PRINCIPLE 4: INDIVIDUALS' RIGHTS

8.1 Effect Withdrawal of Consent

8.1.1 Information on how individuals from whom we are collecting personal data may withdraw consent provided for a specific purpose are made available to them through the respective data protection notice intended for them.

The information relating to the individual's choice is easily accessible and provided clearly and concisely, clearly worded and easy to understand in the respective notices.

8.1.2 We will clearly state the likely consequences of withdrawing consent, either before or upon receiving the notice of withdrawal, before giving effect to the withdrawal of consent in line with the withdrawal of consent process in DPMP-PRO-04 Withdrawal of Consent, Access & Correction Process.

8.1.3 We will retain all withdrawal requests received and processed in accordance with our retention policy. Records should include relevant details such as the requestor's name, date of request, the reason for requesting, all correspondences between the individual and us, and between us and third parties notified of the consent withdrawal, outcome and status of the request, etc.

8.2 Provide Access and Correction Rights

8.2.1 Information on how individuals from whom we are collecting personal data may request access or correction to their personal data are made available to them through the respective data protection notice intended for them. The information provided is easily accessible, clearly worded and easy to understand.

8.2.2 Whenever a request for access or correction of individuals' PD is received, it will be handled in line with the access and correction process in DPMP-PRO-04 Withdrawal of Consent, Access & Correction Process.

8.2.3 If we have determined that it is appropriate under section 21 of the PDPA and Part II of the Personal Data Protection Regulations 2014 to not provide some or all of the personal data requested in the individual's access request ("withheld personal data"), we shall preserve a copy of the withheld personal data for a period of 30 calendar days¹ after rejecting the access request – as the individual may seek a review of our decision. In the event, that the individual applies to review to the PDPC and the PDPC determines that it will take up the review application, as soon as we receive a Notice of Review Application from the PDPC, we should, as good practice, preserve the withheld personal data until the review by PDPC is concluded and any right of the individual to apply for reconsideration and appeal is exhausted.

¹As prescribed in the Personal Data Protection Regulations.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	20 of 20
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION MANAGEMENT PROGRAMME (DPMP) MANUAL	Doc No	DPMP-MANUAL
	Revision	1.0

8.2.4 We will retain all access and correction requests received and processed in accordance with our retention policy, documenting information on whether the request was completed or not. The record should include relevant details such as the requestor's name, date of request, the reason for requesting, all correspondences between the individual and us, and between us and third parties notified of the requests, outcome and status of the request, etc.

8.3 Data Breach Notification

8.3.1 We have established a data breach management process highlighting the mandatory data breach notification obligation to PDPC. Affected individuals will also be notified of any data breach if we have reasons to believe that the breach will likely cause significant harm to them based on the type of personal data that was compromised (e.g., sensitive data such as NRIC, financial information, account details), unless an exception applies. The details of the process are described in DPMP-PRO-03 Data Breach Management.

~ End of Document