

THE SOFTWARE PRACTICE PTE LTD	No of Pages	1 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION GOVERNANCE POLICY	Doc No	DPMP-POL-01
	Revision	1.0

AMENDMENTS LOG

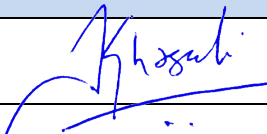
Revision History

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 GOVERNANCE POLICY	Doc No	DPMP-POL-01
	Revision	1.0

Contents

AMENDMENTS LOG	1
RECORDS FOR DOCUMENT REVIEW	3
PURPOSE	4
SCOPE.....	4
RESPONSIBILITIES & AUTHORITIES.....	4
1 POLICY STATEMENT	5
2 GOVERNANCE STRUCTURE	6
3 COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA.....	6
4 WITHDRAWAL OF CONSENT	9
5 ACCESS TO AND CORRECTION OF PERSONAL DATA	9
6 MAINTAINING PERSONAL DATA ACCURACY AND QUALITY.....	9
7 PROTECTION OF PERSONAL DATA	9
8 STORAGE AND TRANSMISSION.....	9
9 RETENTION	10
10 DISPOSAL AND DESTRUCTION	10
11 COMPLIANT OVERSEAS TRANSFERS.....	10
12 QUERIES AND COMPLAINTS	11
13 DATA BREACH NOTIFICATION.....	11
14 DATA PROTECTION IMPACT ASSESSMENT AND DATA PROTECTION BY DESIGN.....	11
15 DATA PROCESSING AGREEMENTS.....	12
16 COMPLIANCE MONITORING AND REPORTING.....	12

THE SOFTWARE PRACTICE PTE LTD	No of Pages	4 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION GOVERNANCE POLICY	Doc No	DPMP-POL-01
	Revision	1.0

PURPOSE

This document provides a high-level framework for the protection of personal data in accordance with the Singapore Personal Data Protection Act (“**PDPA**”) and all associated regulations and guidelines which may from time to time be issued by the Personal Data Protection Commission (PDPC) of Singapore.

SCOPE

This policy applies to all persons involved in the processing of personal data, and extends to all processing of personal data.

RESPONSIBILITIES & AUTHORITIES

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

The Data Protection Officer (DPO) shall ensure compliance with this policy and all relevant personal data protection regulations and guidelines, and shall communicate this policy to all persons involved in the processing of personal data.

This document shall be reviewed at least once a year and if significant changes occur by the Top Management and the DPO, and amend it where necessary to ensure continued compliance with the PDPA. The review must ensure that changed requirements are captured and feedback from process owners and other relevant interested parties are considered.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	5 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION GOVERNANCE POLICY	Doc No	DPMP-POL-01
	Revision	1.0

1 Policy Statement

1.1. All personnel working for or on our behalf who are involved in the processing of personal data are responsible for ensuring compliance with this policy, and to clarify any of its provision with the DPO.

1.2. This Personal Data Governance Policy is based on the following PDPA obligations:

- **Accountability**
 - Comply with the law and applicable local and regulatory regulations and best practices to reduce data protection risks throughout the personal data lifecycle.
- **Consent and Choice**
 - Only collect, use or disclose personal data with consent, and give individuals choice and control over how their personal data is collected, use or disclose including allowing them to withdraw consent.
- **Purpose Limitation and Legitimacy**
 - Collect, use or disclose personal data only for specified, explicit and legitimate purposes for which consent has been given (unless an exception applies), and that would be considered appropriate to a reasonable person in the given circumstances;
 - Minimize personal data collection to what is relevant and is necessary for specified, explicit and legitimate purpose, and ensure that personal data is not retained longer than is necessary; and
 - Limit the ways personal data is used, disclosed and retained only for identified purposes for which consent has been obtained after notification to the individuals.
- **Notice and Transparency**
 - Notify individuals of the purposes for collection, use or disclosure of their personal data no later than at the time of collection and/or on each occasion of change of purpose; Make information about data protection policies including retention and disposal of personal data, and DPO contact details publicly available.
- **Accuracy and Completeness**
 - Ensure personal data collected is reasonably accurate, up to date, complete and meaningful for the identified purposes for which it is to be used.
- **Protection**
 - Protect personal data at rest, in transit, and in use by reasonable physical, technical and organizational security safeguards against such risks as loss or unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks.
- **Retention Limitation**
 - Cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served, and retention is no longer necessary for legal or business purposes.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	6 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION GOVERNANCE POLICY	Doc No	DPMP-POL-01
	Revision	1.0

- Transfer Limitation
 - Limit transfer of personal data outside Singapore only in accordance with the requirements prescribed under the PDPA to ensure that overseas recipient provides a standard of protection to personal data transferred that is comparable to the protection under the PDPA.
- Individual Rights for Access & Correction
 - Upon request, provide information about use or disclosure of personal data in a reasonable timeframe and manner, and in a form that is readily intelligible to the individuals; Allow individuals to challenge the personal data related to them, and have it erased, rectified, completed or amended.
- Data Breach Notification
 - Notify the PDPC and affected individuals of the data breach within the prescribed timeline unless an exception applies to not notify the individuals.

2 Governance Structure

- 2.1. The Management shall formally endorse and approve this policy.
- 2.2. The Management shall appoint and empower the Data Protection Officer (DPO) and commission the Data Protection Impact Assessments (DPIA).
- 2.3. The DPO has been appointed to champion personal data protection initiatives and be primarily responsible for ensuring and monitoring the organization's compliance with data protection obligations.
- 2.4. The Appointment Letter for the DPO contains the details of the duties that the DPO must perform.
- 2.5. Each personal data processing activity must have a process owner who shall work closely with the DPO to implement practices, procedures, and systems relating to his/her personal data processing activities that will ensure that the organization complies with the PDPA and other applicable regulations and guidelines.

3 Collection, Use and Disclosure of Personal Data

3.1. Collection of Personal Data

We shall not collect personal data unless the information is reasonably necessary for, or directly related to, one or more personal data processing activities. We shall only collect personal data only by lawful and fair means, and not in an intrusive way, and must take reasonable steps to ensure that the individual is aware of the following:

- The identity and contact details of the organization collecting and storing the information;
- The purpose for which the information is collected;

THE SOFTWARE PRACTICE PTE LTD	No of Pages	7 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION GOVERNANCE POLICY	Doc No	DPMP-POL-01
	Revision	1.0

- The intended recipients or organizations to which it usually discloses information of that kind;
- Any law that requires the particular information to be collected;
- The main consequences (if any) for the individual if all or part of the information is not provided; and
- The latest version of the data protection notice intended for the type of individual.

Where it is reasonable and practical to do so, we will collect personal data about an individual only from the individual itself. If, however, this information is collected from a person other than the individual, we must act reasonably to ensure that the individual is or has been made aware of the matters listed above.

We will ensure that collection, use, processing and disclosure of personal data is limited only for purposes that are reasonable, and which have been informed to the individuals concerned, and consent had been obtained.

We may collect personal data pursuant to an exception under the PDPA or other written law such as during the following situations:

- Relying on vital interests of the individual for the purpose of contacting the next-of-kin or emergency contact person of any injured, ill or deceased individual.
- Relying on the legitimate interest exception (LIE) for the purposes such as detecting or preventing illegal activities or threats to physical safety and security, IT and network security, preventing misuse of services, and carrying out other necessary corporate due diligence (e.g., the collection, use and disclosure of personal data for the consolidation of official watch lists).

We shall conduct assessments to eliminate reduce the likelihood or mitigate likely adverse effect to the individual when relying on deemed consent by notification, or legitimate interests' exception.

3.2. Use and Disclosure of Personal Data

As a general rule, we must only use or disclose personal data in a manner consistent with any data protection notice provided to the individual and to which consent has been obtained for a legitimate purpose. We must not use or disclose personal data about the individual other than for its primary purpose of collection, unless:

- The individual has consented to the use or disclosure; or
- The individual would reasonably expect us to use or disclose non-sensitive personal data for a secondary purpose and the secondary purpose is related to the primary purpose (e.g., fulfilment of the contract); or
- We have reason to suspect that unlawful activity has been, or may be engaged in, and use or disclose the personal data as a necessary part of its investigation of the matter or in reporting its concerns to relevant authorities; or
- The use or disclosure is required or authorized by or under law, rule or regulation;

THE SOFTWARE PRACTICE PTE LTD	No of Pages	8 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION GOVERNANCE POLICY	Doc No	DPMP-POL-01
	Revision	1.0

- We reasonably believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to public health or public safety or the life or health of an individual.

3.3. Collection of Sensitive Personal Data

We must only collect sensitive personal data if the collection is required by any written law or where the information is reasonably necessary for the purpose and with the consent from the individual to accurately establish or verify the identity of the individual to a high degree of fidelity.

Sensitive personal data may be defined as personal data which is considered likely to result in significant harm to an affected individual when compromised. Examples are:

- NRIC, FIN, Passport Details and other government-issued identifications
- Financial, medical, private key to authenticate or authorize a record or transaction

In collecting sensitive personal data, we shall consider whether alternative forms of personal data can be collected that can allow us to carry out our functions or to achieve the same purpose, as the potential adverse effect to the individuals will be higher if the personal data is sensitive in nature.

Currently, sensitive data collected by us are limited to NRIC, FIN and Passport Details for employment-related purposes, and bank account information for payroll / payment of service purposes.

3.4. Use and Disclosure of Sensitive Personal Data

We must not use and/or disclose sensitive data unless such use or disclosure is required or authorized under law or applicable regulation, or with consent from the individual in line with the notice provided on legitimate business purpose and that would be considered appropriate to a reasonable person in the given circumstances e.g., to accurately establish or verify the identity of the individual to a high degree of fidelity.

Currently, sensitive data collected from employees as mentioned in 3.3 above are only use and/or disclosure for the purpose of employment and payroll.

3.5. Unsolicited Personal Data

When we receive unsolicited personal data about an individual, we must either destroy (e.g., shredding if hardcopy) or permanently delete (e.g., deletion of email and deleted items bin) the personal data immediately upon detection. If it is part of a document that we keep, use or disclose, we will mask the unsolicited personal data before keeping, using or disclosing such document.

3.6. Obligation to Inform Third Parties on any Modification or Withdrawal of Consent, or Objections Pertaining to the Shared Personal Data

THE SOFTWARE PRACTICE PTE LTD	No of Pages	9 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION GOVERNANCE POLICY	Doc No	DPMP-POL-01
	Revision	1.0

In light of our obligations as a Data Controller, we must ensure that third parties are informed on any modification or withdrawal of consent or objections pertaining to the shared personal data, where applies.

Communication of such modifications, withdrawals or objections to the third party shall be done by the DPO or the designated individual and recorded to maintain an audit trail. The DPO or the designated individual shall monitor the acknowledgment of receipt of the information.

4 Withdrawal of Consent

4.1. The consent the individuals provide for the collection, use and disclosure of their personal data will remain valid until such time it is being withdrawn by them in writing. They may withdraw consent and request us to stop collecting, using and/or disclosing their personal data by submitting their request in writing or via email to our DPO as communicated in the data protection notices intended for them. However, withdrawing consent does not affect our right to continue to collect, use and disclose personal data where such collection, use and disclose without consent is permitted or required under applicable laws.

4.2. For withdrawal of consent, we will notify the individuals of the consequences before acceding to the same, including any legal consequences which may affect the individuals' rights and liabilities to our organization, prior to implementation of the withdrawal.

5 Access to and Correction of Personal Data

As a general rule, we will, on the request by an individual, provide him or her with access to their personal data, and will consider a request from the individual for correction of that information. A standard process with clear responsibilities and timelines in line with our PDPA obligations shall be followed for handling this type of request.

6 Maintaining Personal Data Accuracy and Quality

We will take reasonable steps to make sure that the personal data we collect, use, or disclose is accurate, complete, up to date, and not misleading. These steps may include verification of identity and supporting documents, where applies.

7 Protection of Personal Data

7.1. We must take reasonable steps to protect the personal data that we hold from misuse, interference, and loss, and from unauthorized access, modification, or disclosure, or other similar risks.

7.2. We shall ensure that appropriate physical, technical, and organizational security measures are implemented on personal data in whatever form it takes in line with the controls we implement as part of our Information Security Management System.

8 Storage and Transmission

THE SOFTWARE PRACTICE PTE LTD	No of Pages	10 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION GOVERNANCE POLICY	Doc No	DPMP-POL-01
	Revision	1.0

8.1. Access to personal data within our organization shall be limited only to authorized and appropriate employees based on role-based access control.

8.2. We allow outside transmission of information to the effect that encryption or password-protection is employed to personal data, whichever of the two controls is efficiently feasible for the transmission activity, and that the transmission is over an encrypted channel.

9 Retention

9.1. We shall retain personal data only for the duration necessary to fulfil the identified lawful business purpose. All personal data shall be retained only for as long as necessary:

- For the fulfilment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated; or
- The establishment, exercise, or defence of legal claims; or
- As prescribed by law.

9.2. Retention periods, modes of storage and disposal method shall be documented for the personal data involved in each processing activity, and shall be reviewed at least once a year and when significant changes occur.

9.3. Personal data shall not be retained if there is no longer a legal or business purpose.

10 Disposal and Destruction

10.1. Upon the expiration of identified lawful business purposes or withdrawal of consent, we must take reasonable steps to securely destroy or permanently de-identify or anonymize the personal data if it is no longer needed.

10.2. Disposal should be in a manner that the personal data shall be unreadable (for hardcopy records) or irretrievable (for softcopy records).

10.3. All hard, system, soft copies and removable media will be disposed appropriately following our standard process for disposal and destruction.

11 Compliant Overseas Transfers

11.1. Personal data may be transferred to recipients outside Singapore under certain conditions:

- 11.1.1. The recipient has all necessary controls to fulfil all applicable obligations regarding the processing of personal data taking account of security and privacy risks and the scope of processing;
- 11.1.2. The recipient can demonstrate evidence of compliance with the instructions and/or agreements/contracts. We may rely on applicable certifications such as ISO/IEC 27001 & ISO/IEC 27701, APEC CBPR, APEC PRP, EU-GDPR Compliance, etc. where available to satisfy this requirement); and

THE SOFTWARE PRACTICE PTE LTD	No of Pages	11 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION GOVERNANCE POLICY	Doc No	DPMP-POL-01
	Revision	1.0

11.1.3. Any legally binding instrument, contract or binding corporate rules that imposes a standard of protection that is comparable to that under the PDPA.

11.2. Given the above, if there is a need to transfer personal data to recipients outside Singapore, we shall:

11.2.1. Ensure that the recipient is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA e.g., by reason of their domestic law or of the international commitments they have entered to before deciding to transfer to a specific jurisdiction.

11.2.2. We shall ensure that the overseas recipient has an adequate level of protection to the fundamental right of the individuals to data privacy, and that the personal data receives a comparable standard as that which it would receive under the Singapore PDPA.

12 Queries and Complaints

We shall receive queries and complaints related to the personal data, as well as facilitate and institute an investigation in relation thereof. A standard process with clear responsibilities and timelines shall be followed for handling personal data queries and complaints.

13 Data Breach Notification

Our employees and data intermediaries (if any) must immediately notify our DPO if they become aware of a data breach to enable the appropriate assessment, investigation and remediation measures to be taken in a timely manner, including possible notification to PDPC and other relevant bodies, and to the affected individuals. Data breach notification protocols have been established and maintained within our organisation in order to deal with a data breach concerning personal data with clear notification timelines, detailed responsibilities and steps to follow.

14 Data Protection Impact Assessment and Data Protection by Design

14.1. Data Protection Impact Assessment (DPIA) shall be completed when there are events that significantly change in the privacy environment or affect the processing of personal data, either a new system, process or service is being introduced, developed or implemented, or an existing system, process or service being reviewed, or substantially redesigned.

14.2. We shall follow Data Protection by Design (DPbD) principles and practices including, but not limited to:

14.2.1. Proactive and Preventive - We will assess, identify, manage and prevent any data protection risks before any data breach occurs.

14.2.2. Data Protection as the Default - We will provide personal data protection in default settings, where applies.

14.2.3. End-to-End Security - We will implement best practices and security features from the point that personal data is collected till it is disposed of.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	12 of 12
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA PROTECTION GOVERNANCE POLICY	Doc No	DPMP-POL-01
	Revision	1.0

14.2.4. Data Minimization - We will only collect, store and use personal data that is relevant and necessary.

14.2.5. User-centric - We will develop and implement processes with individuals in mind and make them user-friendly.

14.2.6. Transparency - We will inform customers what personal data is collected from them and how it is being used.

14.2.7. Risk Minimization - We will design and implement the right processes and relevant security measures when processing personal data to reduce risks.

15 Data Processing Agreements

In light of our obligations under applicable PDPA, relevant regulations and guidelines, we must ensure that appropriate wording is included in an external provider contract where the external provider will receive, or have access to any personal data that our organization holds. We shall conduct due diligence assessment on external providers prior to engagement to ensure that they can protect the personal data comparable to the standards of PDPA.

16 Compliance Monitoring and Reporting

16.1. Non-compliance with this policy may result in a breach of Singapore Personal Data Protection Act (PDPA) and other applicable regulations and guidelines.

16.2. We shall perform regular review (at least once a year and as when changes occur) of contracts, policies, data protection procedures and practices, notices, data inventory map and data protection impact assessment to ensure compliance.

16.3. Any non-compliance by an employee shall subject the employee to appropriate disciplinary actions.