PERSONAL DATA PROTECTION POLICY

1. DEFINITIONS

i. Personal Data: Data, whether true or not, that can identify an individual (e.g., full name, NRIC/passport number, mobile number, address, biometric identifiers, employment records).
ii. Processing: Any operation on personal data including collection, use, disclosure, storage, or deletion.
iii. Data Subject: Any individual whose personal data is processed by or on behalf of the Company.
iv. DPO: The appointed Data Protection Officer.

2. INTRODUCTION

This Personal Data Protection Policy ("Policy") outlines how the companies under Slim Doc SG Pte Ltd (“we”, “our”, or “the Company”) manage personal data in compliance with the Personal Data Protection Act 2012 (“PDPA”) of Singapore.

We are committed to ensuring that personal data belonging to our customers, employees, vendors, and business partners is handled with the highest standard of integrity, security, and transparency. This Policy sets out our practices for the collection, use, disclosure, protection, and retention of personal data, as well as the rights of individuals under the PDPA.

By accessing our websites or providing personal data to us through any channel, you acknowledge and agree to the terms set out in this Policy.

3. WEBSITE PRIVACY STATEMENT

This section outlines the Company’s obligations and practices relating to the collection, use, disclosure, and management of personal data through its websites, in accordance with the Personal Data Protection Act 2012 (“PDPA”).

This Website Privacy Policy applies to the following official websites operated by the Company:

- https://hairdoc.com.sg
- https://onedoc.com.sg
- https://slimdoc.com.sg

The Company collects personal data via these websites through functions such as service bookings, contact forms, inquiries, or subscription to promotional materials. Prior to or at the point of collection, users will be notified of the purposes for which their data is being collected, and their consent will be obtained, unless such collection is exempted under the PDPA.

Consent may be provided through affirmative actions, such as ticking consent boxes, submitting contact forms, or continuing to use the website after being notified of such purposes. Users may withdraw their consent at any time by contacting the Company’s Data Protection Officer. Any withdrawal of consent may affect the Company’s ability to provide

services or respond to inquiries, which will be communicated clearly to the individual.

The Company implements reasonable administrative, technical, and physical safeguards to protect personal data collected through its websites. This includes the use of secure servers, encrypted communications, restricted access protocols, and routine system audits.

Where personal data is transferred outside Singapore, the Company ensures that appropriate safeguards are in place to provide a standard of protection that is comparable to the protection under the PDPA. Transfers will only be conducted in accordance with applicable legal requirements.

The Company takes reasonable steps to ensure that personal data collected through its websites is accurate and up to date. Individuals are encouraged to contact the Company should any updates or corrections be required.

Personal data will be retained only for as long as necessary to fulfill the purposes for which it was collected, or as required by applicable laws and regulations. Upon expiry of the retention period, data will be securely deleted or destroyed using appropriate methods.

4. CONSENT AND PURPOSE LIMITATION

The Company shall obtain the individual's consent before collecting, using, or disclosing any personal data, unless such collection, use, or disclosure is permitted or required by the Personal Data Protection Act 2012 ("PDPA") or any other applicable laws.

Consent may be obtained through written, electronic, or recorded means, including but not limited to submission of forms, acceptance of terms on our websites, and other affirmative actions. The Company shall ensure that individuals are notified of the purposes for which their personal data is being collected, used, or disclosed at or before the point of collection.

The Company shall not, as a condition of providing a product or service, require an individual to consent to the collection, use, or disclosure of personal data beyond what is reasonably necessary to provide the product or service.

Individuals have the right to withdraw their consent at any time, with reasonable notice. Upon withdrawal of consent, the Company will inform the individual of the likely consequences, including any impact on service delivery. The Company will cease the collection, use, or disclosure of the personal data unless such action is permitted or required under the PDPA.

The Company will only collect, use, or disclose personal data for purposes that a reasonable person would consider appropriate under the circumstances. Personal data collected shall not be used for new purposes unless consent is obtained afresh from the individual.

5. ACCESS AND CORRECTION RIGHTS

In accordance with Sections 21 and 22 of the Personal Data Protection Act 2012 ("PDPA"), individuals have the right to request access to their personal data in the Company's possession or control, as well as information about the ways in which the data has been used or disclosed by the Company in the past 12 months prior to the request.

Individuals may also request the correction of any errors or omissions in their personal data. The Company shall take reasonable steps to verify the accuracy of the data and make the necessary amendments as soon as practicable, unless there are legal grounds to refuse such

correction.

Requests for access or correction must be made in writing and addressed to the Company's Data Protection Officer via the contact details provided in this Policy. The Company may charge a reasonable administrative fee for access requests and will inform the individual of the fee before processing the request.

Upon receipt of a complete request, the Company will respond within thirty (30) calendar days. If the Company is unable to provide access or make a correction within this period, it shall inform the individual in writing of the reason for the delay and the expected time frame for response.

The Company reserves the right to reject frivolous, vexatious, or abusive requests and requests that would pose a threat to the safety or privacy of others, or that may contravene the law.

6. PROTECTION OF PERSONAL DATA

The Company adopts reasonable administrative, physical, and technical safeguards to protect personal data in its possession or under its control, in accordance with Section 24 of the Personal Data Protection Act 2012 ("PDPA"). These measures are specifically implemented to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks to the personal data.

Protection measures include, but are not limited to:

- Role-based access controls and password-protected systems to limit access to authorized personnel;
- Use of encryption protocols and firewalls for digital data storage and transmission;
- Secure storage facilities for physical records;
- Implementation of CCTV monitoring and visitor access controls;
- Employee training on data protection responsibilities and the requirement to sign non-disclosure agreements (NDAs);
- Regular system reviews, audits, and updates to security protocols.

The Company also ensures that third-party service providers who handle personal data on its behalf are contractually bound to adhere to similar levels of data protection and are subject to regular oversight.

These safeguards are reviewed periodically and enhanced as necessary to maintain the confidentiality, integrity, and availability of personal data.

7. TRANSFER OF PERSONAL DATA OUTSIDE SINGAPORE

In accordance with Section 26 of the Personal Data Protection Act 2012 ("PDPA"), the Company shall not transfer personal data to a country or territory outside Singapore except in compliance with the requirements prescribed under the PDPA to ensure that a standard of protection comparable to that under the PDPA is provided.

Before transferring any personal data internationally, the Company will ensure that:

- The recipient country has data protection laws that offer a comparable level of protection to Singapore's PDPA; or
- Contractual clauses, binding corporate rules, or other legally enforceable instruments are in place to ensure the recipient provides a standard of protection that is at least equivalent to the PDPA; or
- The individual has given express consent to the transfer after being informed of the risks.

International transfers may occur in connection with service providers, cloud storage providers, affiliates, or business partners located overseas who are engaged by the Company for the purposes stated in this Policy. All such transfers will be carried out only to the extent necessary and with appropriate safeguards.

The Company shall maintain records of all cross-border data transfers and will regularly assess the effectiveness of protective measures implemented.

8. ACCURACY & CORRECTION

The Company takes reasonable steps to ensure that the personal data collected, used, or disclosed is accurate, complete, and up to date, particularly when such data is likely to be used to make decisions that affect the individual or to be disclosed to other organizations.

Individuals are encouraged to notify the Company of any changes to their personal data as soon as reasonably practicable. Upon receiving a request for correction, the Company will verify the request and update the personal data accordingly unless it has reasonable grounds to believe that the correction should not be made.

Where corrected personal data has been disclosed to third parties within the year preceding the correction, the Company shall, where appropriate, inform such third parties of the correction unless it is impracticable or prohibited by law.

The Company reviews its internal databases periodically and before any significant use or disclosure of personal data to ensure the accuracy and relevance of the information held.

9. RETENTION AND DISPOSAL

The Company shall retain personal data only for as long as it is necessary to fulfill the purpose for which it was collected, or as required by applicable laws and regulations. Once the personal data is no longer required for business or legal purposes, the Company will take reasonable steps to ensure that the data is disposed of in a secure manner.

Retention periods are determined based on the nature of the data and the legal or operational requirements of the Company. As a general guideline:

- Employee and customer records shall be retained for a minimum of seven (7) years after the end of the employment or service relationship;
- Rejected job applicant records shall be retained for up to six (6) months;

- Expired or invalid records (such as outdated identification documents) shall be disposed of immediately upon invalidation.

Disposal methods include secure shredding of physical records, and permanent deletion or digital wiping of electronic data using appropriate tools. The Company also requires that third-party service providers handling personal data on its behalf apply similar secure disposal practices.

The Company reviews its retention schedules periodically to ensure alignment with evolving legal requirements and industry standards.

10. THIRD-PARTY DISCLOSURE AND DO NOT CALL (DNC) PROVISIONS

10.1 Disclosure To Third Parties

The Company may disclose personal data to authorized third parties where such disclosure is necessary for the purposes outlined in this Policy, or where it is required or permitted under applicable laws. Such third parties may include, but are not limited to:

- IT service providers, cloud hosting partners, and system vendors;
- Banks, insurers, auditors, and legal or professional advisors;
- Government authorities, regulators, and law enforcement agencies.

All third parties engaged to process personal data on behalf of the Company are contractually bound to implement appropriate safeguards to ensure the confidentiality, integrity, and security of the data, in accordance with the standards set under the Personal Data Protection Act 2012 (“PDPA”).

10.2 Do Not Call (DNC) Provisions

The Company is committed to complying fully with the Do Not Call (DNC) provisions under Part IX of the PDPA. We do not send marketing messages via voice calls, text messages, or fax to Singapore telephone numbers listed in the DNC Registry unless:

- The individual has provided clear and unambiguous consent to receive such messages; or
- The communication is exempted under the PDPA as service-related or transaction-based.
- Prior to sending any telemarketing communication, the Company shall:
- Conduct screenings of phone numbers against the DNC Registry;
- Maintain proper records of individuals who have provided consent;
- Ensure that all messages include sender identification and contact details; and
- Provide a clear and easy mechanism for recipients to opt out of future marketing messages.

Individuals who wish to withdraw consent for receiving marketing messages may contact our Data Protection Officer via the details provided in this Policy. The Company will respect such requests and cease all related communications within a reasonable period.

11. DATA BREACH MANAGEMENT

The Company is committed to responding swiftly and effectively to any suspected or confirmed data breach involving personal data under its control. A data breach refers to any unauthorized access, collection, use, disclosure, copying, modification, or disposal of personal data, as well as the loss of any storage medium or device on which personal data is stored.

Upon discovery of a data breach, the Company shall activate its internal Data Breach Response Plan, which includes the following key steps.

11.1 Containment and Preliminary Assessment

The affected systems and processes will be promptly contained to prevent further unauthorized access or damage.

An internal assessment team, led by the Data Protection Officer (DPO), will evaluate the nature and scope of the breach to determine whether it meets the criteria of a "notifiable data breach" under the PDPA.

11.2 Notification Obligations

If the breach is assessed to result in, or is likely to result in, significant harm to affected individuals, or involves the loss or unauthorized disclosure of personal data affecting 500 or more individuals, the Company shall notify the Personal Data Protection Commission (PDPC) as soon as practicable, and in any case, within three (3) calendar days from the date of determination.

Affected individuals will also be notified without undue delay, providing sufficient information to help them take protective actions, where applicable.

11.3 Investigation and Remediation

A root cause analysis will be conducted to identify contributing factors and determine whether additional security measures are necessary.

Corrective and preventive actions will be implemented to mitigate recurrence, and updates may be provided to the PDPC where required.

The Company shall maintain records of all data breaches, including those not deemed notifiable under the PDPA. Employees are trained to report any actual or suspected data breach to the DPO immediately upon detection.

12. ROLES & RESPONSIBILITIES

12.1 Responsibilities of Employees And Representatives

All employees, contractors, agents, and representatives of the Company are responsible for ensuring that personal data in their possession or under their control is managed in accordance with the Personal Data Protection Act 2012 ("PDPA") and this Policy.

They are required to:

- Handle personal data confidentially and securely;
- Limit access to personal data on a strict need-to-know basis;
- Report any suspected or actual data breach to the Data Protection Officer immediately;
- Participate in relevant data protection training and awareness activities as required by the Company.

Any failure to comply with the Company's data protection policies or procedures may result in disciplinary action, including termination of employment or contract, and possible legal consequences.

12.2 Responsibilities of the Data Protection Officer (DPO)

The Company has appointed a Data Protection Officer ("DPO") pursuant to Section 11 of the PDPA. The DPO is responsible for overseeing the Company's compliance with the PDPA and other applicable data protection laws and standards.

Key responsibilities of the DPO include:

- Monitoring and reviewing the Company's personal data protection policies and practices;
- Conducting regular audits and risk assessments on data handling processes;
- Coordinating staff training and awareness programs on data protection;
- Responding to data access, correction, and withdrawal-of-consent requests from individuals;
- Managing and investigating data breaches, and notifying the Personal Data Protection Commission (PDPC) and affected individuals where applicable;
- Serving as the main liaison with the PDPC on compliance matters.

12.3 Contacting the DPO

Individuals may contact the DPO regarding any inquiries, feedback, complaints, or requests relating to the Company's handling of personal data via the following:

Data Protection Officer
Email: hr_support@onedocgroup.com
Telephone: +65 9018 1629

The Company shall make reasonable efforts to respond to all data protection-related inquiries in a timely and appropriate manner.

13. POLICY REVIEW

This Policy is reviewed annually or when there are changes to the law or our business operations.

Effective Date: 1st April 2025
Last Reviewed: 9th May 2025