PDPA-DPP-01
PERSONAL DATA PROTECTION POLICY

VINDES ENGINEERING PTE LTD

Revision :	0
Date of last revision:	21st July 2025
Reviewed by/Date:	HR / 21st July 2025
Approved by/Date:	COM / 21st July 2025

DATA PROTECTION POLICY FOR EMPLOYEES AND JOB APPLICANTS

Contents

This Data Protection Policy **("Policy")** sets out the basis upon which **Vindes Engineering Pte Ltd** ("we", "us" or "our") may collect, use, disclose or otherwise process personal data of employees and job applicants in accordance with the Personal Data Protection Act **("PDPA").** This Policy applies to personal data in our possession or under our control, including personal data in the possession of organisations which we have engaged to collect, use, disclose or process personal data for our purposes.

APPLICATION OF THIS POLICY

1. This Policy applies to all persons engaged in a contract of service with us (whether on a part-time, temporary or full-time basis) and interns and trainees working at or attached to us (collectively referred to as "employees") as well as persons who have applied for any such position with us ("job applicants"), and all references to "employment" shall apply equally to internships and traineeships (as may be applicable).

2. This policy also applies to employees / job applicants, service providers, business partners, contractors, and any other parties such as visitors and they are collectively name as "Relevant Parties".

3. This policy does not apply to personal data which is business contact information. Business contact information refers to 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.

PERSONAL DATA

4. As used in this Policy**, "personal data"** means data, about an employee or a job applicant who can be identified: (a) from that data; or (b) from that data and other information to which we have or are likely to have access.

5. **If you are a job applicant**, personal data which we may collect includes, without limitation, your:

(a) name or alias, gender, NRIC/FIN or passport number, date of birth, nationality, and country and city of birth;
(b) mailing address, telephone numbers, email address and other contact details;
(c) resume, educational qualifications, professional qualifications and certifications and employment references;
(d) employment and training history;
(e) work-related health issues and disabilities; and

(f) photographs and other audio-visual information.

6. **<u>If you are an employee</u>**, personal data which we may collect in the context of your employment with us includes, without limitation, your:

(a) name or alias, gender, NRIC/FIN or passport number, date of birth, nationality, and country and city of birth;
(b) mailing address, telephone numbers, email address and other contact details;
(c) employment and training history;
(d) salary information and bank account details;
(e) details of your next-of-kin, spouse and other family members;
(f) work-related health issues and disabilities;
(g) records on leave of absence from work;
(h) photographs and other audio-visual information;
(i) performance assessments and disciplinary records; and
(j) any additional information provided to us by you as a job applicant (that is, prior to being engaged as an employee).

7. Other terms used in this Policy shall have the meanings given to them in the PDPA (where the context so permits).

<u>COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA</u>

8. We generally collect personal data that (a) you knowingly and voluntarily provide in the course of or in connection with your employment or job application with us, or via a third party who has been duly authorised by you to disclose your personal data to us (your **"authorised representative",** which may include your job placement agent), after (i) you (or your authorised representative) have been notified of the purposes for which the data is collected, and (ii) you (or your authorised representative) have provided written consent to the collection and usage of your personal data for those purposes, or (b) collection and use of personal data without consent is permitted or required by the PDPA or other laws. We shall seek your consent before collecting any additional personal data and before using your personal data for a purpose which has not been notified to you (except where permitted or authorised by law). Consent may be (i) expressed or (ii) deemed (or implied) as reasonable under the circumstances e.g. when an individual provided his personal data including mobile telephone number in a job application or for work-related communications. Where consent is not obtained, Company may collect, disclose or use your personal data pursuant to an exception under the Personal Data Protection Act or other written law.

9. The collection, use and disclosure of personal data shall only be for purposes that a reasonable person would consider appropriate in the circumstances, and if applicable, have been notified to the individual prior to the collection, use or disclosure of personal data.

Any new purposes for the affected parties where we have collected before will be notified via email. Consent to collecting, use and disclosing personal data for any new purposes will be collected from the following Relevant Parties.

10. **If you are a job applicant,** your personal data will be collected and used by us for the following purposes and we may disclose your personal data to third parties where necessary for the following purposes:

    (a) assessing and evaluating your suitability for employment in any current or prospective position within the organisation; and

    (b) verifying your identity and the accuracy of your personal details and other information provided.

11. **If you are an employee,** your personal data will be collected and used by us for the following purposes and we may disclose your personal data to third parties where necessary for the following purposes:

    (a) performing obligations under or in connection with your contract of employment with us, including payment of remuneration and tax;

    (b) all administrative and human resources related matters within our organisation, including administering payroll, granting access to our premises and computer systems, processing leave applications, administering your insurance and other benefits, processing your claims and expenses, investigating any acts or defaults (or suspected acts or defaults), enrolment with certified training providers, and developing human resource policies;

    (c) managing and terminating our employment relationship with you, including monitoring your internet access and your use of our intranet email to investigate potential contraventions of our internal or external compliance regulations, and resolving any employment related grievances;

    (d) assessing and evaluating your suitability for employment/appointment or continued employment/appointment in any position within our organisation;

    (e) ensuring business continuity for our organisation in the event that your employment with us is or will be terminated;

    (f) performing obligations under or in connection with the provision of our goods or services to our clients;

(g) facilitating any proposed or confirmed merger, acquisition or business asset transaction involving any part of our organisation, or corporate restructuring process;

(h) facilitating our compliance with any laws, customs and regulations which may be applicable to us; and

(i) disclosure to our clients for the purposes of safety, training and security access in any work site under the government of Singapore.

12. By completing and submitting the curriculum vitae (CV) during application of job through the job portal or recruitment agencies for potential or continued employment in the Company (as the case may be), the job applicant or employee (respectively) shall be deemed to have consented to the collection, use and disclosure of his or her personal data by us for the abovementioned purposes. By providing personal data relating to a third party (e.g. spouse, children, parents and/or employees), the individual shall represent and warrant that prior consent is obtained from such third party for the collection, use or disclosure of personal data.

13. In the use, collection and disclosure of personal data held by us:

    a. personal data shall only be used for the purposes set out in clauses 10 and 11; and
    b. personal data shall not be disclosed, either within or outside the Company, to any unauthorised recipients, and if disclosed, shall only be on a need-to-know basis with prior notification and consent.

14. The purposes listed in the above clauses may continue to apply even in situations where your relationship with us (for example, pursuant to a contract) has been terminated or altered in any way, for a reasonable period thereafter (including, where applicable, a period to enable us to enforce our rights under any contract with you).

15. The process steps undertaken by our DPO for notification regarding any changes to purposes for collection, use, and disclosure are as follows:

    i. prepare the Acknowledgement Form for New Purposes when new purpose to be notified is required.
    ii. clearly state the new purposes, the consequences of not consent or withdrawal of consent in the Acknowledgement Form for New Purposes.
    iii. check and notify all affected parties.
    iv. explain and ensure all affected parties are fully aware before getting them to sign the Acknowledgement Form for New Purposes.
    v. maintain the Acknowledgement Form for New Purposes as evidence.

CONSENT WITHDRAWAL

16. The consent that you provide for the collection, use and disclosure of your personal data will remain valid until such time it is being withdrawn by you in writing. We shall cease to retain documents containing personal data and inform any relevant external parties as soon as it is reasonable to assume that (a) the purpose for which the personal data was collected is no longer being served by retention of the personal data; (b) retention is no longer necessary for legal or business purposes; and (c) when personal data owner has withdrawn consent to the use of his/her personal data by the Company which will be recorded in the 'Access, Correction and Consent Withdrawal Log'.

    a. If you are a job applicant, you may withdraw consent and request for us to stop using and/or disclosing your personal data for any or all of the purposes listed above by submitting your request in writing or via email to our Data Protection Officer at the contact details provided below.

    b. If you are an employee, you may withdraw your consent by submitting a formal request in writing to our Data Protection Officer, or to HR department.

17. Upon receipt of your written request to withdraw your consent, we shall verify the requesting individual's identity, sight and confirm the identity is correct. Our DPO will provide the estimated timeframe to process and address the withdrawal request within **TEN (10) business days** of receiving it – please note that we may require reasonable time (depending on the complexity of the request and its impact on our relationship with you) for your request to be processed and for us to notify you of the consequences of us acceding to the same, including any legal consequences which may affect your rights and liabilities to us. In general, we shall seek to process and effect your request within **THIRTY (30) days** of receiving it and shall inform the requestor of the reasons for failing to do so in such a situation.

18. Whilst we respect your decision to withdraw your consent, please note that depending on the nature and extent of your request, we may not be in a position to process your job application (as the case may be) or to fulfil contractual obligations. The withdrawal does not negate any legal consequences that may arise such as a breach of contract. We shall, in such circumstances, notify you before completing the processing of your request (as outlined above). Should you decide to cancel your withdrawal of consent, please inform us in writing in the manner described in clause 16 above.

19. Please note that withdrawing consent does not affect our right to continue to collect, use and disclose personal data where such collection, use and disclosure without consent is permitted pursuant to an exception under the PDPA or required under applicable laws.

ACCESS TO AND CORRECTION OF PERSONAL DATA

20. If you wish to make (a) an access request for access to a copy of the personal data which we hold about you or information about the ways in which we use or disclose your personal data, or (b) a correction request to correct or update any of your personal data which we hold, you may submit your request in writing or via email to our Data Protection Officer at the contact details provided below.

21. Please note that a reasonable fee may be charged for an access request. If so, we will inform you of the fee before processing your request.

22. For access requests by external parties, the DPO and/or appointed employee handling the access request shall ensure completion of the Access Request and Acknowledgement Form.

23. For both internal and external parties, the DPO and/or appointed employee shall:

    i. confirm the individual's identity;
    ii. verify with requestor that we hold personal data about the requesting party;
    iii. request for requestor's reason(s) for accessing personal data.
    iv. provide an estimated timeframe to process and address the access request, typically within **THIRTY (30) days** after receiving the request.

    a. We will respond to your access request as soon as reasonably possible. Should we not be able to respond to your access request within **THIRTY (30) days** after receiving your access request, we will inform you in writing within **THIRTY (30) days** of the time by which we will be able to respond to your request. If we are unable to provide you with any personal data or to make a correction requested by you, we shall generally inform you of the reasons why we are unable to do so (except where we are not required to do so under the PDPA).

    b. The DPO shall wait for confirmation by the requestor to proceed before requiring collection of payment, if any. Thereafter, we shall provide the requesting individual the required access as required. In the event of the access request being rejected due to a valid reason, the DPO shall inform the requestor of the valid reason for not providing the access in writing or email. Access requests may be rejected for the following reasons:

        i. request is prohibited under the PDPA or other written law.
        ii. requestor fails to provide necessary identification card for verification of requestor's identity.
        iii. requestor is unable to provide confirmation that the requestor's personal data is in the Company's possession.
        iv. personal data requested has been destroyed, anonymized, or normalized permanently according to retention period.

v. an individual making an access request on behalf of someone else fails to provide a letter of authorization and copies of the individual's and requestor's identification card.

c. Upon receiving an access request from public agencies, courts, and law enforcement agencies to disclose personal data for purposes of investigations or proceedings under the PDPA or other written law:

i. DPO shall inform the Director of such requests.
ii. DPO appointed employee to take actions to comply and manage as per requirements of public agencies, courts and law enforcement agencies.
iii. DPO shall record request in the 'Access, Correction, and Consent Withdrawal Log'.

24. Please note that depending on the request that is being made, we will only need to provide you with access to the personal data contained in the documents requested, and not to the entire documents themselves. In those cases, it may be appropriate for us to simply provide you with confirmation of the personal data that our organisation has on record, if the record of your personal data forms a negligible part of the document.

25. External and/or internal parties may request to correct his/her personal data in the Company's possession to the DPO via hr@vindes.com.sg.

26. In responding to the correction request, the DPO and/or appointed employee shall:

i. Confirm the requesting individual's identity (may sight identification card and confirm the identity is correct).
ii. Verify with the requestor that the Company holds personal data about the requesting party.
iii. Obtain the individual's consent to send corrected personal data to other relevant third parties.
iv. Inform any relevant external parties to whom personal data was disclosed to update individual's changes in personal data.

a. The Company will respond to a correction and/or omission request as soon as practicable within **ONE (1) month** unless extraordinary circumstances arise (e.g. files archived with external parties).

b. Correction requests may be rejected and individuals will be notified by the DPO through email should the requesting external/internal parties fail to:

i. Provide identification document for verification of identity.
ii. Provide complete and accurate personal data for correction of current personal data in the Company's possession.
iii. Provide reasonable grounds for the correction or omission request.

27. All access, correction and omission cases shall be recorded in the 'Access, Correction and Consent Withdrawal Log'.

PROTECTION OF PERSONAL DATA

28. To safeguard your personal data from unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, we have introduced appropriate administrative, physical and technical measures such as up-to-date antivirus protection, encryption and the use of privacy filters to secure all storage and transmission of personal data by us, and disclosing personal data both internally and to our authorised third party service providers and agents only on a need-to-know basis.

29. You should be aware, however, that no method of transmission over the Internet or method of electronic storage is completely secure. While security cannot be guaranteed, we strive to protect the security of your information and are constantly reviewing and enhancing our information security measures.

ACCURACY OF PERSONAL DATA

30. We generally rely on personal data provided by you (or your authorised representative). By engaging with and providing to us your personal data, you hereby accept that:

    a. Warrant of Accuracy: You warrant that all personal data you provide to us is accurate, complete, and up-to-date to the best of your knowledge at the time of provision. You acknowledge that providing inaccurate, incomplete, or outdated personal data may affect our ability to provide products, services, or communications to you effectively.

    b. Obligation to Update: You agree to promptly notify us of any changes to your personal data (for example, changes in contact details, employment status, or other relevant information) so that we can maintain data accuracy and completeness, particularly when such data is likely to be used to make decisions affecting you or disclosed to third parties.

    c. Reliance and Verification: We may rely on the personal data you provide for the purposes set out in our Data Protection Policy or any service agreements. While we will make reasonable efforts to check and verify data in accordance with our obligations under the PDPA accuracy obligation, we are not obliged to independently verify personal data provided directly by you except where necessary.

d. Limitation of Liability: You accept that we shall not be liable for any loss, damage, or inconvenience arising from your failure to provide accurate, complete, or updated personal data. This includes but is not limited to errors in decision-making, missed notifications, or misdirected communications resulting from inaccurate data.

e. Review of Accuracy Practices: You acknowledge that we may periodically review or update our processes for verifying and maintaining data accuracy, and you agree to cooperate with reasonable requests for confirmation or proof of certain data elements when needed for compliance or risk management.

f. No Implied Additional Obligations: This clause does not create any additional obligation on us beyond making reasonable efforts under the PDPA accuracy obligation and related guidelines; it clarifies your responsibility to provide accurate, complete, and current personal data.

31. In order to ensure that your personal data is current, complete and accurate, please update us if there are changes to your personal data by informing our Data Protection Officer in writing or via email at the contact details provided below.

RETENTION OF PERSONAL DATA

32. We shall review the various types of personal data and the retention periods in our possession on a regular basis, at least once a year, whenever there are any changes to relevant laws, sectorial and international guidelines and/or significant changes to business operations, products or services, to determine if that personal data is still needed for legal or business purposes. We may retain your personal data for as long as it is necessary to fulfil the purposes for which they were collected, or as required or permitted by applicable laws. Any updates to the Retention Schedule and Data Inventory Map shall be reviewed and approved by the DPO. Purposes for retaining the personal data and the retention period shall be indicated in the Data Inventory Map.

33. We will cease to retain your personal data, or remove the means by which the data can be associated with you, as soon as it is reasonable to assume that such retention no longer serves the purposes for which the personal data were collected, and are no longer necessary for legal or business purposes.

TRANSFER OF PERSONAL DATA OUTSIDE OF SINGAPORE

34. We generally do not transfer your personal data to countries outside of Singapore. However, if we do so, we will obtain your consent for the transfer to be made and will take

steps to ensure that your personal data continues to receive a standard of protection that is at least comparable to that provided under the PDPA.

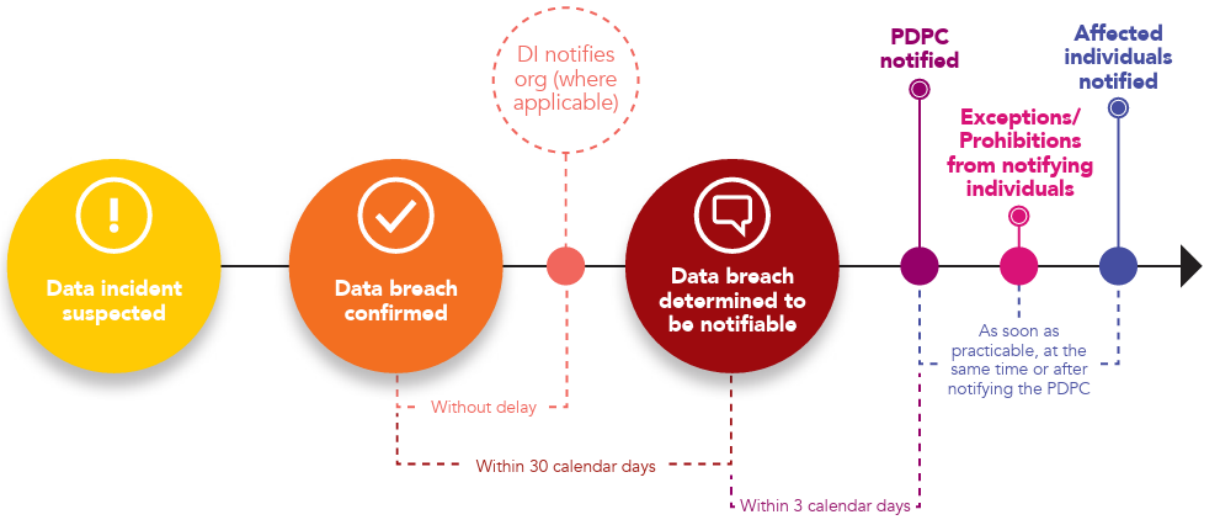
DATA BREACH NOTIFICATION

35. We shall follow the processes documented in the Data Breach Management Plan in the event that there is a data breach. We shall ensure that clear procedures are established in the agreement with the data intermediary engaged to notify the Company of a data breach immediately and to address the security failure as soon as practicable.

36. The data breach management team will follow the four key steps (i.e. Contain, Assess, Report, Evaluate) and take appropriate actions in the event of a data breach.

37. The DPO shall notify the PDPC and/or the affected individuals from the time the data breach management team has determined that the data breach is notifiable as shown in Diagram 1.

38. Diagram 1: Flowchart for Data Breach Notification



Note: Where a data breach affects 500 or more individuals, we shall notify the PDPC even if the data breach does not involve any prescribed personal data in the Personal Data Protection (Notification of Data Breaches) Regulations 2021.

39. The timeframe for a notifiable data breach is as follows:

    a. The PDPC as soon as practicable, but in any case, no later than **THREE (3) calendar days**; and

b. Where required, the affected individuals as soon as practicable, at the same time or after notifying the PDPC.

DO NOT CALL REGISTRY

40. Under the Do-Not-Call Registry established pursuant to the Act, no person shall send specified messages or calls (being marketing messages or calls) to a person, before first checking with the Registry whether the person's telephone number is listed in the Do-Not-Call Registry. If such person's telephone number is listed in the Do-Not-Call Registry, then specified messages should not be sent.

41. Business-to-business marketing messages or calls are not within the scope of the Do-No-Call Registry.

42. In general, we do not engage in telemarketing or perform door-to-door marketing with any individual residential consumer. Notwithstanding the above, where marketing information is sent to individuals such as residential, sole proprietors, partners, companies or businesses (or their respective employees), we shall comply with any restrictions regarding marketing messages or calls or marketing practices to such individuals, businesses, etc.

DATA PORTABILITY

43. Derived personal data is defined under the PDPA to refer to personal data about an individual that is derived by us in the course of business from other personal data about the individual or another individual, in the possession or under the control of us. It generally refers to new data elements created through the processing of personal data (e.g., through mathematical, logical, statistical, computational, algorithmic, or analytical methods based on the application of business-specific rules). Derived data is a general term but in the context of data portability, it does not include personal data derived by us using any prescribed means or methods which are commonly known and used by the industry (e.g., simple mathematical averaging or summation).

44. We shall reserve the right to assess the applicability of future PDPA Data Portability requirements and render personal data transmission services to other third parties in response to the data subjects' requests in a discretionary manner.

COMPLAINTS AND RESOLUTION PROCESS

45. In the event of any complaints that may arise in respect of the application of this Policy, the Company shall, through the DPO, investigate and resolve the complaint and respond to or inform the complainant accordingly, as soon as practicable.

46. A record of the investigation and outcome shall be retained.

DATA PROTECTION OFFICER (DPO)

47. You may contact our Data Protection Officers if you have any enquiries or feedback on our personal data protection policies and procedures; or if you wish to make any request, in the following manner:

Name	: MS Benedette Chay
Position	: HR Officer / DPO
Address	: 2 Venture Drive #09-15 Vision Exchange Singapore 608526
Tel/Fax	: 6250 7275
Email	: hr@vindes.com.sg

Or Back-Up DPO as below:

Name	: MR Lawrence Toh
Position	: Chief Operation Manager / DPO
Address	: 23 Tuas Ave 4 Singapore 639373
Tel / Fax	: 6250 7275
Email	: Lawrence_toh@vindes.com.sg

EFFECT OF POLICY AND CHANGES TO POLICY

48. This Policy applies in conjunction with any other policies, notices, contractual clauses and consent clauses that apply in relation to the collection, use and disclosure of your personal data by us.

    All Data Protection Policies and Procedures will be reviewed by the DPOs from time to time as required or appropriate to take into account PDPA and any relevant laws, sectorial and international guidelines, not less than once every year or as and when necessary. We may revise this Policy from time to time without any prior notice. You may determine if any such revision has taken place by referring to the date on which this Notice was last updated. Your continued employment and participation in our recruitment process constitute your acknowledgement and acceptance of such changes.