

DATA PROTECTION NOTICE

This Data Protection Notice (“**Notice**”) sets out the basis which PALO IT Thailand (“**we**”, “**us**”, or “**our**”) may collect, use, disclose or otherwise process personal data in accordance with the Personal Data Protection Act (“**PDPA**”). This Notice 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.

PERSONAL DATA

1. As used in this Notice:

“**job applicants**” means persons who have applied for any such position with us; and

“**personal data**” means data, whether true or not, about a person 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.

2. **If you are a job applicant**, personal data which we may collect includes, without limitation, your: (a) name or alias, gender, 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.
3. Other terms used in this Notice shall have the meanings given to them in the PDPA (where the context so permits).

COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

4. We generally do not collect your personal data unless (a) it is provided to us voluntarily by you directly or via a third party who has been duly authorised by you to disclose your personal data to us (your “**authorised representative**”) 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).
 - 4.1. 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 authorized by law).

- 4.2. By providing personal data relating to a third party (e.g., spouse, children, parents, referees and/or employees), you shall obtain consent from them before providing to PALO-IT for collection, use or disclosure.
5. **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 Company, and
 - b) verifying your identity and the accuracy of your personal details and other information provided.
6. We may disclose your personal data:
- (a) where such disclosure is required for performing obligations in the course of or in connection with our provision of the goods and services requested by you.
7. Please be noted that should you not consent and provide us with the relevant personal information to fulfil the “purposes” of collection, use and disclose of your personal information by us, it may hinder our ability to continue to interact with you.

We may not be able to make a decision on your suitability for recruitment or employment or comply with the law, therefore we may not be able to make an offer of employment.

WITHDRAWING YOUR CONSENT

8. 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. You may withdraw consent and request us to stop collecting, 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.
9. Upon receipt of your written request to withdraw your consent, 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 your request within thirty (30) days of receiving it.
10. Whilst we respect your decision to withdraw your consent, please note that depending on the nature and scope of your request, we may not be in a position to continue providing our goods or services to you and we shall, in such circumstances, notify you by email before completing the processing of your request. Should you decide to cancel your withdrawal of consent, please inform us in writing in the manner described in clause 7 above.

11. Please note that 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.

ACCESS TO AND CORRECTION OF PERSONAL DATA

12. 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 about you, you may submit your request in writing or via email to our Data Protection Officer at the contact details provided below.
13. 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.
14. We will respond to your request as soon as reasonably possible. In general, our response will be within thirty (30) days. Should we not be able to respond to your request within thirty (30) days after receiving your 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).

PROTECTION OF PERSONAL DATA

15. 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 minimised collection of personal data, authentication and access controls (such as good password practices, need-to-basis for data disclosure, etc.), encryption of data, up-to-date antivirus protection, regular patching of operating system and other software, securely erase storage media in devices before disposal, web security measures against risks, usage of one time password(OTP)/2 factor authentication (2fa)/multi-factor authentication (MFA) to secure access, security review and testing performed regularly, firewall, data loss prevention system, single sign on, information security policy, and network segmentation.
16. 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

17. We generally rely on personal data provided by you (or your authorised representative). 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

18. We may retain your personal data for as long as it is necessary to fulfil the purpose for which it was collected, or as required or permitted by applicable laws.
19. 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 purpose for which the personal data was collected, and is no longer necessary for legal or business purposes.

TRANSFERS OF PERSONAL DATA OUTSIDE OF THAILAND

20. We generally use data processing facilities outside of Thailand in Singapore, Europe and the USA. We 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 PROTECTION OFFICER

21. You may contact our Data Protection Officer if you have any enquiries or feedback on our personal data protection policies and procedures, or if you wish to make any request, by submitting this form [Personal Data Request](#).

EFFECT OF NOTICE AND CHANGES TO NOTICE

22. This Notice applies in conjunction with any other notices, contractual clauses and consent clauses that apply in relation to the collection, use and disclosure of your personal data by us.
23. We may revise this Notice 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 use of our services constitutes your acknowledgement and acceptance of such changes.

Effective date: 01/06/2022
Last updated: 01/06/2022

Frequently Asked Questions

1. General

What is personal data?

Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. For more information, please visit [Office of the Personal Data Protection Committee](#).

Is there any type of data that is not covered under the PDPA?

All non-personal data (such as statistics, numbers and other information that cannot be linked back to an individual) and business contacts are not covered under PDPA. For more information, please visit [Office of the Personal Data Protection Committee](#).

Are the rights of a child covered under the PDPA?

For any child below 13 years of age, the rights to consent, access and correction can only be granted by their guardians.

2. Collection, Use & Disclosure

How does PALO IT obtain my consent for collecting, using, or disclosing my personal data?

You may have given your consent when you signed up for our services:

- via any legal contract
- when you submit a form, accepting the privacy notice

How do I withdraw consent from Palo-IT to collect, use and/or disclose my personal data?

You may request to withdraw your consent submitting this form [Personal Data Request](#). Your request for withdrawal of consent for all modes will take effect within 30 days. Please note that the use of your personal data may be essential in order for us to provide the product/service which you have signed/subscribed.

Am I able to reinstate my consent after I have withdrawn it?

Yes, you may do so by submitting this form [Personal Data Request](#).

3. Access & Correction

Can I access the personal data that Palo-IT has of me?

Under the PDPA, you have the right to request access to your personal data that we have, by submitting this form [Personal Data Request](#).

Do I need to pay for accessing my personal data with Palo?

Depending on the type of personal data that you have requested for, a fee may be charged to cover our costs for providing such data. No fee will be charged when you access your personal information over the Internet or when making basic inquiries.

Can I submit a request for access to personal data on behalf of someone else?

You may request for access to personal data on behalf of someone else only if you obtain and are able to produce documents of proof of his/her authorisation. These documents include:

- Copy of identity card/passport of the person authorising the access
- Copy of identity card/passport of the person being authorised to access the data
- Letter of authorisation signed by the person authorising the access
- Any other supporting documents where applicable