PERSONAL DATA PROTECTION POLICY

Data Protection Statement

Tourism Management Institute of Singapore Pte Ltd (TMIS) understands and respects your privacy is important and we are committed to protect your personal information in accordance with the requirements of the Personal Data Protection Act ("PDPA").

Purpose of the Data Protection Policy

This Data Protection Policy sets out the basis upon which TMIS management ("**we**", "**us**" or "**our**") may collect, use, disclose or otherwise process personal data of job applicants in accordance with the 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 persons who have applied for any position with us ("**job applicants**").

Personal Data

2. As used in this Policy, "**personal data**" means data, whether true or not, about 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.

3. As 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.

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

Collection, Use and Disclosure of Personal Data

5. We generally collect personal data that

    (a) you knowingly voluntarily provide in the course of or in connection with your job application
        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).

6. As a job applicant, your personal data will be collected and used by us 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.

Withdrawing Consent by Job Applicants

7. 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 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.

8. 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 and effect your request within 10 working days of receiving it.

9. 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). 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 8 above.

10. 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

11. 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 at the contact details provided below.

12. 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).

13. 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 Institute has on record, if the record of your personal data forms a negligible part of the document.

Protection of Personal Data

14. 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.

15. 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

16. 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 in writing or via email at the contact details provided below.

Retention of Personal Data

17. 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.

18. 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

19. 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 of Personal Data

20. Under the PDPA Amendment Act in 2020 which came into effect on 1st February 2021, it is mandatory to notify PDPC within 3 calendar days, upon confirmation that the data breach is notifiable. Once the data breach is assessed to be likely to result in significant harm to an affected individual or significant scale of more than 500 individuals.

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, in the following manner:

    Email address : dpo@tmis.edu.sg

Date of issue : July 2023