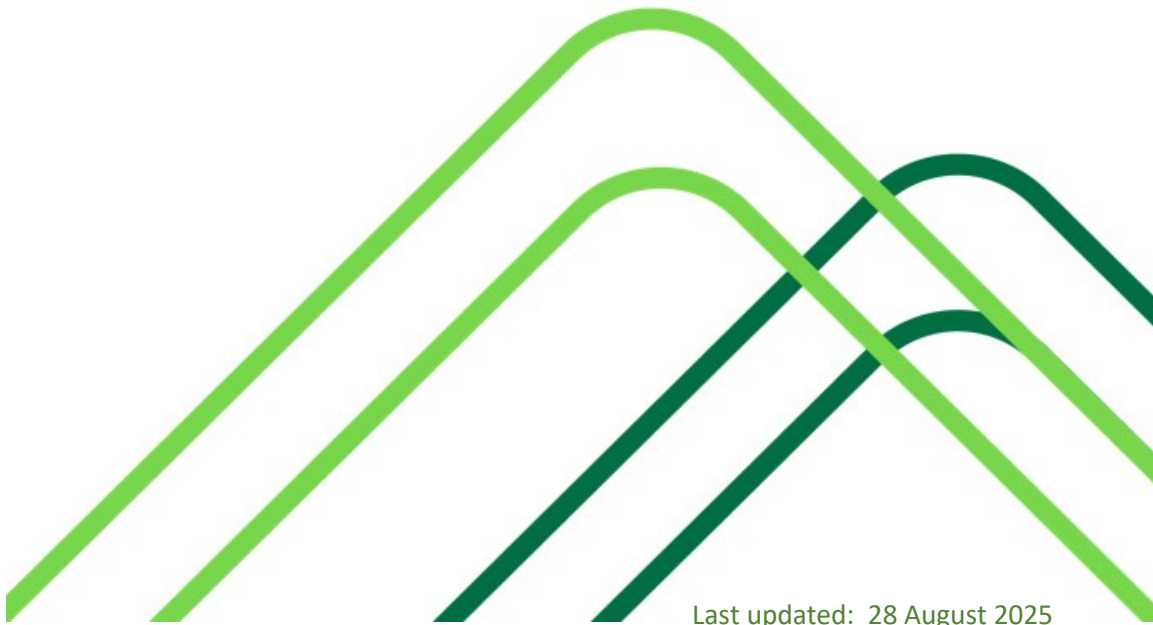


Personal Data Protection Act (PDPA) Policy



Last updated: 28 August 2025

www.uhylsc.com.sg

CHANGE HISTORY

Version	Date	Author	Description of Change	Reviewed By	Approved By
1.	9-10-2019	Crispin Lee	Initial draft		POP
2.	30-06-2020	Crispin Lee	Update changes to DPO		POP
3.	18-03-2021	Crispin Lee	Updated DPC information		POP
4.	19-12-2022	Crispin Lee	Updated DPC Information		POP
5.	28-08-2025	Crispin Lee	Updated DPC & contents		POP

UHY Lee Seng Chan & Co (the “Firm” or “UHY LSC”) is a member of Urbach Hacker Young International Limited, a UK company, and forms part of the international UHY network of legally independent accounting and consulting firms. UHY is the brand name for the UHY international network. The services described herein are provided by the Firm and not by UHY or any other member firm of UHY. Neither UHY nor any member of UHY has any liability for services provided by other members.

Table of Contents

CHANGE HISTORY	2
I. INTRODUCTION	4
II. PERSONAL DATA	5
III. HOW WE COLLECT YOUR PERSONAL DATA.....	6
IV. TYPES OF PERSONAL DATA WE COLLECT ABOUT YOU.....	7
V. HOW WE USE YOUR PERSONAL DATA.....	8
VI. WITHDRAWING YOUR CONSENT	10
VII. ACCESSING AND MAKING CORRECTION TO YOUR PERSONAL DATA.....	11
VIII. PROTECTION OF PERSONAL DATA.....	12
IX. ACCURACY OF PERSONAL DATA	13
X. RETENTION OF PERSONAL DATA	13
XI. TRANSFER OF YOUR PERSONAL DATA.....	13
XII. DO-NOT-CALL (DNC) PROVISION AND TELEMARKETING ACTIVITIES	14
XIII. CONTACTING US.....	14
XIV. EFFECT OF POLICY AND CHANGES TO POLICY	14
XV. REFERENCES	15
XVI. PDPA CONSENT FORM (SAMPLES)	16
XVII. DATA PROTECTION COMMITTEE (DPC)	17
XVIII. ROLES AND RESPONSIBILITY OF THE DPO.....	17

I. INTRODUCTION

Personal Data Protection Act (PDPA) was passed by the Parliament in October 2012. It is a new data protection law comprises various rules governing the collection, use, disclosure and care of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes. The law safeguard consumers' personal data against misuse.

We have developed this Data Protection document ("**Policy**") to assist you in understanding how we collect, use, disclose, process and retain your personal data. 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 for our purposes. This will provide clarity to internal stakeholders on the responsibilities and processes on handling personal data in their day-to-day work. Policies also demonstrate accountability to external parties by informing them on the ways in which the organisation handles personal data.

We at UHY LSC respect the privacy and confidentiality of our employees' and clients' personal data. We are committed to ensure that UHY LSC complies with the Personal Data Protection Act 2012 (PDPA) in the collection, use, disclosure, maintenance of accuracy, handling and security of personal data in a manner that recognises both the right of individuals to protect their personal data and the need of the organisation to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

The Policy is reviewed by the Data Processing Officer ("**DPO**") on an annual basis, or as and when there are changes in the environment, Act or the Policy, to ensure relevancy and alignment to regulatory development. Any updates or changes to the Policy will be sent to the Data Protection Committee for approval.

II. PERSONAL DATA

1. As used in this Policy:

“Customer” means an individual who (a) has contacted us through any means to find out more about any goods or services we provide, or (b) may, or has, entered into a contract with us for the supply of any goods or services by us; and

This Policy also 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).

“Personal data” means data, whether true or not, about a customer or an employee 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.
- Depending on the nature of your interaction with us, some examples of personal data which we may collect from you include name, identification numbers such as NRIC, FIN, passport number, work permit and birth certificate, residential address, email address, telephone number, nationality, gender, date of birth, marital status, employment information and financial information.
- ### 3.
- Other terms used in this Policy shall have the meanings given to them in the PDPA (where the context so permits).

III. HOW WE COLLECT YOUR 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).
5. We collect the personal data of our employees, prospects and clients through the following methods / channels:
 - When you make payment
 - When you respond to a marketing call for new product or service
 - When you call in to request for information or enquiry
 - When you submit an application form
 - When you request for technical support
 - When you wish to preview a product or service
 - When you send in your job application form
 - When you sign in as a visitor
 - When you register as a participant
 - When you indicate you wish to have follow-up from website
 - When you sign up for a service
 - When you leave your contact details
 - When you respond to a marketing call
 - When you agree to a customer/employee survey
 - Images and videos from CCTV cameras
6. The individual should ensure the Personal Data provided, whether with given consent or not, is true and complete. If the individual provides Personal Data of a third party (e.g. information of the individual’s dependent, spouse, children, parents, proxies, and/or the individual’s company’s Authorised Persons, Directors, Beneficial Owners or Contact Persons, etc.) to UHY LSC, the individual shall be

deemed to have secured the consent of the third party has been obtained for the collection, use and disclosure of the Personal Data for the purposes set out in this Policy.

IV. TYPES OF PERSONAL DATA WE COLLECT ABOUT YOU

7. **If you are a job applicant**, personal data which we may collect includes, without limitation, your:
 - name or alias, gender, NRIC/FIN or passport number, date of birth, nationality, and country and city of birth;
 - mailing address, telephone numbers, email address and other contact details;
 - resume, educational qualifications, professional qualifications and certifications and employment references;
 - employment and training history;
 - work-related health issues and disabilities; and
 - Photographs.
8. **If you are an employee**, personal data which we may collect in the context of your employment with us includes, without, limitation, your:
 - name or alias, gender, NRIC/FIN or passport number, date of birth, nationality, and country and city of birth;
 - mailing address, telephone numbers, email address and other contact details;
 - employment and training history;
 - salary information and bank account details;
 - details of your next-of-kin, spouse and other family members;
 - work-related health issues and disabilities;
 - records on leave of absence from work;
 - photographs and other audio-visual information;
 - performance assessments and disciplinary records; and
 - any additional information provided to us by you as a job applicant (that is, prior to being engaged as an employee).
9. **If you are a customer**, personal data which we may collect includes, without, limitation, your:
 - name or alias, gender, NRIC/FIN or passport number, date of birth, nationality, and country and city of birth;

- mailing address, telephone numbers, email address and other contact details;
- employment details and training history;
- salary information and bank account details;
- details of your next-of-kin, spouse and other family members;
- education & professional qualification
- work-related health issues and disabilities;
- records on leave of absence from work;
- criminal background/past offences
- photographs and other audio-visual information;
- purchase information/history
- customer feedback and survey

V. HOW WE USE YOUR PERSONAL DATA

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 followings purposes:
 - assessing and evaluating your suitability for employment in any current or prospective position within the organization; and
 - 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:
 - performing obligations under or in connection with your contract of employment with us, including payment of remuneration and tax;
 - 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) and developing human resource policies;
 - 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;

- assessing and evaluating your suitability for employment/appointment or continued employment/appointment in any position within our organisation;
- ensuring business continuity for our organisation in the event that your employment with us is or will be terminated;
- performing obligations under or in connection with the provision of our goods or services to our clients;
- facilitating any proposed or confirmed merger, acquisition or business asset transaction involving any part of our organisation, or corporate restructuring process; and
- facilitating our compliance with any laws, customs and regulations which may be applicable to us.

12. **If you are a customer**, we may collect and use your personal data for any or all of followings purposes:

- performing obligations in the course of or in connection with our provision of the goods and/or services requested by you;
- verifying your identity;
- responding to, handling, and processing queries, requests, applications, complaints, and feedback from you;
- managing your relationship with us;
- processing payment or credit transactions;
- complying with any applicable laws, regulations, codes of practice, guidelines, or rules, or to assist in law enforcement and investigations conducted by any governmental and/or regulatory authority;
- any other purposes for which you have provided the information;
- transmitting to any unaffiliated third parties including our third-party service providers and agents, and relevant governmental and/or regulatory authorities, whether in Singapore or abroad, for the aforementioned purposes; and
- any other incidental business purposes related to or in connection with the above.

13. As a customer, 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; or
 - (b) to third party service providers, agents and other organisations we have engaged to perform any of the functions with reference to the above-mentioned purposes.
- 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 a contract with you).

VI. WITHDRAWING YOUR CONSENT

- 15. Before we collect, use or disclose your personal data, we will generally will notify you of the purpose why we are doing so. We will obtain written confirmation from you on your expressed consent. As far as possible, we will not collect more personal data than necessary for the stated purpose. Under certain circumstances, we may assume deemed consent from you when you voluntarily provide your personal data for the stated purpose, e.g. when you enter into a service or employment agreement.
- 16. If you have a one-on-one meeting with us or do a transaction with us on behalf of another individual, you must first obtain consent from that individual in order for us to collect, use or disclose his/her personal data.
- 17. 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.
- 18. If you wish to withdraw your consent, you should give us reasonable advance notice. 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 fourteen (14) business days of receiving it.

19. 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 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 16 above.
20. 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 law.

VII. ACCESSING AND MAKING CORRECTION TO YOUR PERSONAL DATA

21. 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, based on reasonable grounds, at the contact details provided below.
22. 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.
23. We will respond to your request as soon as reasonably possible. In general, our response will be within ten (10) business 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).
24. We are obligated under the PDPA to allow you access to your personal data of the past one (1) year, and to make any correction if there is any error or omission. Before we accede to your request, we may need to verify your identity by checking your NRIC or other legal identification document.

25. 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.

VIII. PROTECTION OF PERSONAL DATA

26. We have implemented an Information Security Policy that governs how personal data and confidential information are protected within our organisation. We will disseminate information to staff holders on implementing measures to secure and protect information such as training of its employees on handling Personal Data with respect to confidentiality, securing individual's data, taking steps to prevent misuse, loss, unauthorised access, and disclosure.
27. We will take the necessary security arrangements to protect your personal data that is under our charge of control to prevent unauthorised access, collection, use, disclosure, or similar risks. All our employees will take reasonable care to ensure that the individual's Personal Data is classified, stored and transmitted adequately.
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, firewalls, strong passwords, 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.

IX. ACCURACY OF PERSONAL DATA

- 30. 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.
- 31. We will take reasonable precautions and verification checks to ensure that the personal data we have collected is accurate and complete, but relies on individual's self-notification of any changes to their personal data that is relevant to us.
- 32. From time to time, we will do a verification exercise for you to update us on any changes to your personal data. If you are a client or customer, it is important that you update us if there are any changes in your personal information such as your home address.

X. RETENTION OF PERSONAL DATA

- 33. 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.
- 34. 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.

XI. TRANSFER OF YOUR PERSONAL DATA

- 35. 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 we 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.

XII. DO-NOT-CALL (DNC) PROVISION AND TELEMARKETING ACTIVITIES

36. We do not make telemarketing call to promote our products or services.

XIII. CONTACTING US

37. You may contact our Data Protection Committee (DPC) liaison personal if you have any enquiries or feedback on our personal data protection policies and procedures, or if you wish to make any request or complaint relating to how we manage your personal data, in the following manner:

Contact No. : +65 6603 6150
Email Address : dpo@uhylsc.com.sg
Address : 6001 Beach Road #14-01,
Golden Mile Tower,
Singapore 199589.

38. Any query or complaint should include, at least, the following details:
- Full name and contact number of the data subject
 - Brief description on the query or complaint

We treat such queries and complaints seriously and will deal with them confidentially and with reasonable time.

XIV. EFFECT OF POLICY AND CHANGES TO POLICY

39. This Policy 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.
40. 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 use of our services constitutes your acknowledgement and acceptance of such changes.

Effective date : 01/07/2020
Last updated : 28/08/2025

XV. REFERENCES

- Personal Data Protection Commission Singapore, 'Advisory Guidelines on Key Concepts in the Personal Data Protection Act, (Issued 23 September 2013, revised 1 February 2021)
- Personal Data Protection Commission Singapore, 'Guide to Notification, (Issued 26 September 2019)
- Personal Data Protection Commission Singapore, 'Data Protection Starter Kit, (Issued 17 October 2017)
- Drew & Napier, 'SME Guild to the Personal Data Protection Act 2012", (Issued 1 December 2015)
- Personal Data Protection Act 2012
- Personal Data Protection Commission (<https://www.pdpc.gov.sg>)

XVI. PDPA CONSENT FORM (SAMPLES)

CONSENT CLAUSE FOR EMPLOYEES

(TO BE INSERTED IN EMPLOYMENT CONTRACT OR OTHER FORM)

You acknowledge that you have read and understand UHY LSC' Personal Data Protection Policy (the "**Policy**"), and consent to the collection, use and disclosure of your personal data by UHY LSC for the purposes set out in the Policy. You may withdraw consent for such collection, use and disclosure, and make an access or correction in respect of your personal data, in accordance with the Policy.

CONSENT CLAUSE FOR JOB APPLICANTS

(TO BE INSERTED IN EMPLOYMENT APPLICATION FORM OR SIMILAR FORM)

By signing this form,

- a) You acknowledge that you have read, understood and agreed to the above Policy, and consent to the collection, use and/or disclosure of your personal data by us for the purposes set out in the Policy; and
- b) In the event that we have received your job application or personal data from any third party pursuant to the purposes set out in the Policy, you warrant that such third party has been duly authorised by you to disclose your personal data to us for the purposes set out in the Policy.

Name: _____

Signature & Date: _____

XVII. DATA PROTECTION COMMITTEE (DPC)

To facilitate the smooth implementation of data protection policies and procedures with accountabilities and responsibility across various perspective related parties, a data protection committee shall be setup with the following structure:

The Data Protection Committee provides governance and oversight by specify the approach responsibilities over the handling of personal data and communicating that throughout the organisation. Key activities carried out by the DPC:

- Appointing the Data Protection Officer (DPO)
- Approving the organisation's Data Protection Policies
- Providing direction to DPO for the handling of major compliants
- Providing direction to DPO for communication and liaison with the Personal Data Protection Commission ("PDPC")

XVIII. ROLES AND RESPOSIBILITY OF THE DPO

The Data Protection Officer (DPO) is responsible for ensuring that the organisation complies with the PDPA and the following key responsibility:

- Ensuring compliance with the PDPA when developing and implementing polices and processes for handling personal data.
- Point of Contact for data security matters within the business unit for staff and customers or other external parties.
- Review and co-ordinate the operation of required data protection policies and procedures within the represented BU.
- Identify and correct missing or inaccurate data protection policies and procedures.
- Integration of defined procedures into daily business routine.
 - Roll out PDPA to respective business units
 - briefing to the staff
 - remind changes/updates to policies
 - ensure information/doc are complete and in order
- Ensure BU compliance with the latest polices
- Alerting DPC on any risks that might arise with regard to personal data handled by the organisation
- Fostering a data protection culture among employees and across various BUs
- Managing personal data protection-related queries and complaints

- Liaising with the PDPC on data protection matter, if necessary