

Personal Data Protection Policy – Vietnam Annex

This Vietnam Annex is read in conjunction with OCBC’s Data Protection Policy, available at <https://www.ocbc.com/business-banking/bank-policies>. In the event of any inconsistency between OCBC’s Data Protection Policy and the variations in this Annex, the variations herein shall prevail.

The purpose of this document (“Data Protection Policy”) is to inform you of how Overseas-Chinese Banking Corporation Ltd – Ho Chi Minh City Branch, and their respective representatives and agents (“Representatives”) (the Companies and Representatives collectively referred to as “OCBC HCM”, “us”, “we” or “our”) process Personal Data.

In this Data Protection Policy, “Data Subject” refers to any of you, each as an individual who can be identified from “Personal Data”.

“Data Protection Regulations” refers to the Law No. 91/2025/QH15 of the National Assembly of Socialist Republic of Vietnam dated 26 June 2025 on personal data protection, as amended and supplemented from time to time (“Personal Data Protection Law” or “PDPL”), or Decree No. 356/2025/ND-CP of the Government dated 31 December 2025 providing instructions and implementation measures on personal data protection, as amended and supplemented from time to time (“Decree 356”), or any other applicable data privacy laws and guidance.

“Processing”, “process” or any other conjugated forms of such term refers to any operations performed on personal data. Common types of personal data processing include (but are not limited to) collecting, analysing, combining, encrypting, decrypting, modifying, deleting, destroying, de-identifying, providing, publicly disclosing, transferring, or similar actions that may be taken on the data, pursuant to Article 2.6 of the PDPL.

The terms “collection, use, disclosure” of personal data or “collect, use, disclose” personal data or any other conjugated forms of such terms, each term as mentioned in the OCBC’s Data Protection Policy, shall express the same meaning as “process”, as defined in the PDPL and Decree 356.

To avoid any doubt, with respect to corporate or institutional Customers, to the extent that you have provided or will provide us with the personal data of your directors, shareholders, employees, authorized representatives, agents and/or other authorized individuals (collectively referred to as the “Data Subjects”), you confirm that you have informed or will inform such Data Subjects that their personal data will be provided to us and that we will process such personal data in accordance with this Data Protection Policy and the agreement(s) between you and us.

In this context, we act as the controller and processor of the personal data that we receive from you or that is obtained during the course of our dealings with you. This means that we determine the purposes and means of processing the personal data, and when acting as a data processor, we will directly process such personal data. For processing activities and purposes that require consent, you undertake and warrant that you have obtained all necessary and valid consents from the Data Subjects to enable us to carry out the processing of such personal data. You agree and acknowledge that we are not be held liable to verify the legality and validity of such consents and you are also responsible for providing evidence of such consent upon our request. Furthermore, you agree to indemnify and hold us harmless from and against any liability, loss, or damage arising from your failure to obtain the required consent, or from any non-compliance by the Data Subjects relating to their personal data, in accordance with this Data Protection Policy.

1. Types of Personal Data we process

In this Data Protection Policy, "Personal Data" that we may collect and process refers to digital data or information in other forms that identifies or helps to identify a particular person, including basic personal data and sensitive personal data. Personal data, after deidentification, is no longer personal data.:

- a. **Basic Personal Data**, which is a type of Personal Data, that reflects common personal and background information frequently used in transactions and social relationships, including:
 1. Your name, including family name, middle name and first name shown in birth registration certificate and other names (if any);
 2. Date of birth; date of death or missing (if any);
 3. Gender;
 4. Place of birth, place of birth registration, place of permanent residence, place of temporary residence, current place of residence, native place, contact address;
 5. Nationality;
 6. Image of the individual;
 7. Telephone number, Citizen identification number; passport number; driver's license numbers, numbers in vehicles' number plates;
 8. Marital status;
 9. Information about family relationships (parents, children, spouses);
 10. Information about digital account of the individual;
 11. Any other information relating to any individuals or leading to the identification of such individuals which you have provided us and which is not classified as Sensitive Personal Data as below.

- b. **Sensitive Personal Data**, which is a type of Personal Data that is associated with an individual's privacy rights, which (if violated) would directly affect entities, organisations and his/her lawful rights and interests, including:
1. Political opinions, religious opinions, beliefs-related views;
 2. Information private life, personal secrets or family secrets;
 3. Health status;
 4. Information relating to racial origin, ethnic origin;
 5. Biometric information, information about the inherited genetic characteristics of the individual;
 6. Information about sex life, sexual orientation of the individual;
 7. Data on crimes and offenses which are collected and stored by law enforcement authorities;
 8. Location data of the individual identified through location services;
 9. Information on usernames and passwords for accessing an individual's electronic identification account; images of identity cards, citizen identity cards, people's identity cards; or other valid identification documents.
 10. Usernames and passwords for accessing bank accounts; bank card information; data on bank account transaction histories; financial and credit information and other information relating to customers' activities and transaction histories in finance, securities, and insurance at credit institutions, foreign bank branches, intermediary payment service providers, securities companies, insurance companies, and other authorized organizations;
 11. Data tracking activities in the use of telecommunications services, social networks, online communication services, and other services in cyberspace;
 12. Other personal data that is required to be kept confidential under the law or subject to strict security measures under law provisions.

2. Purposes for the Processing of your Personal Data

Please refer to Section 3 of the OCBC's Data Protection Policy.

3. Collection of Personal Data

We only collect your Data Subject's Personal Data in lawful manner and when there is a legitimate reason to do so. Providing your Personal Data is entirely voluntary. If you do not provide us with your Data Subject's Personal Data, we may not be able to provide the products and services you request. We collect your Data Subject's Personal Data through the following sources, such as:

- 3.1 when you submit any form, including but not limited to application, declaration, proposal or referral forms;

- 3.2 when you enter into any agreement or provide other documentation or information in respect of your interactions and transactions with us, or when you use our services;
- 3.3 when you interact with our staff, including customer service officers, relationship managers and other representatives, for example, via telephone calls (which may be recorded), letters, fax, face-to-face meetings and email;
- 3.4 when you are in our premises, your images are captured by us via CCTV cameras while you are within our premises, or via photographs or videos taken by us or our representatives when you attend events hosted by us;
- 3.5 when you use our services provided through online and other technology platforms, such as websites and apps, including when you establish any online accounts with us;
- 3.6 when you request that we contact you, be included in an email or other mailing list; or when you respond to our promotions and other initiatives;
- 3.7 when you are contacted by, and respond to, our marketing representatives and agents and other service providers;
- 3.8 when you submit an employment application or when you provide documents or information including your resume and/or curriculum vitae in connection with any appointment as an officer, director, representative or any other position, or when you attend an employment interview with us;
- 3.9 when you interact with us via our websites or use services on our websites;
- 3.10 where permitted by applicable law, when we seek information about you and receive your Personal Data in connection with your relationship with us, including for banking products, insurance policies or job applications, for example, from business partners, public agencies, your ex-employer and the relevant authorities;
- 3.11 when you respond to our request for additional Personal Data;
- 3.12 from third-party sources that you have consented to allow to provide your Personal Data (such as partners within our ecosystem) or in cases where the collection of your Personal Data is necessary to comply with applicable data protection laws;
- 3.13 when you use our Electronic Banking Services, such as OCBC Phone Banking, OCBC ATM, or OCBC Internet Banking. For more details, please refer to the Terms and Conditions governing Business Accounts;
- 3.14 when you use our mobile and digital applications (“Digital Services”);
- 3.15 when you allow us to collect Personal Data from your mobile device (e.g., location information); and
- 3.16 when you submit Personal Data to us for any other reason.

We may collect your Personal Data when you access, browse, or use our website and platforms. Please refer to the “Use of Cookies and Related Technologies” section below for more details. In the event you provide us with any third-party Personal Data

(e.g., information about your customers, spouse, children, parents, and/or employees), you warrant and acknowledge that you have obtained the consent of that third party to provide their Personal Data to us for related purposes.

We may process your Personal Data only after receiving your **consent** (either obtained by us or a relevant third party) in compliance with the **Data Protection Regulations**, unless otherwise an applicable exemption applies.

4. Sharing of Personal Data

Please refer to **Section 4** of the **OCBC's Data Protection Policy** for information on the disclosure of your personal data and parties related to and/or in charge of controlling, controlling and processing of your personal data. We may process your Personal Data only after receiving your **consent** (either obtained by us or a relevant third party) in compliance with the **Data Protection Regulations**, unless otherwise an applicable exemption applies.

5. Potential Unexpected Consequences

We implement security measures to protect your Personal Data when it is processed in our various computer systems (such as our communications, systems, platforms (including physical and electronic systems, and those in cyberspace)). However, please note that security measures are not error-free and may involve transmission via servers and/or systems that are not under our control. Email transmissions may not be secure and are subject to risks. Therefore, each individual must take information security precautions when transmitting information through the internet or cyberspace.

Examples of unexpected incidents and damages that may occur to the Personal Data, include:

- Accidental data loss and/or breaches;
- Unauthorized or unlawful access, use, alteration, correction or disclosure of personal data; and
- Any other unexpected cases as mentioned herein.

If your Sensitive Personal Data directly collected by us has been unauthorizedly disclosed or lost, we will, within 72 hours after such incident is detected, notify you and competent authorities to address and resolve the matter in accordance with the Data Protection Regulations.

6. Retention and start and end time of Personal Data Processing

We will start to process your Personal Data once we receive it from you (together with your consent and authorization for the collection, use, process and disclosure of your Personal Data pursuant to this Data Protection Policy). We will retain your Personal Data for as long as required to perform the purposes for which the Personal Data was collected, unless we are justified by law, or otherwise requested by you (whichever is earlier).

Accordingly, the start and end time of your Personal Data processing will be for (whichever of the following occurs earlier):

- the duration of our relationship with you;
- the period required by applicable laws;
- as long as reasonably necessary and/or in accordance with our internal policies (i) for us to be able to defend ourselves against any complaints, disputes, claims for compensation or other legal obligations; or (ii) for management, administration, operation and maintenance purposes (including, but not limited to, technical systems, security, record-keeping, risk management, audit, inspection, monitoring and/or surveillance measures);
- as long as you withdraw your consent or authorization for the processing of your Personal Data, except where the law provides for continued processing without the data subject's consent.

7. Rights and Obligations of Data Subjects

You may have certain rights in relation to your Personal Data according to Data Protection Regulations, including:

1. To be informed about OCBC's processing of Personal Data;
2. To agree or disagree to the processing by OCBC of the Personal Data;
3. To access, view and edit, or request OCBC to facilitate the access, viewing and editing of the Personal Data;
4. To withdraw your previously provided consent;
5. To delete or request the deletion of your Personal Data;
6. To request restriction on the processing on the Personal Data;
7. To request for the provision of your Personal Data;
8. To object to the processing of your Personal Data, to prevent or limit the disclosure of the Personal Data, or to the use of Personal Data for advertising and marketing purpose;
9. To complain, denounce and initiate lawsuits by law;
10. To request for compensation if there are breaches of Personal Data protection;
11. To defend against any violations of your civil rights related to your Personal Data;

12. To request us and competent authority to implement measures and solutions to protect your Personal Data in accordance with Data Protection Regulations; and
13. Other rights as per the Data Protection Regulations.

Unless otherwise stated by law, you are obliged:

1. To provide complete and accurate Personal Data;
2. To take steps to protect your Personal Data and request that other entities and individuals protect your Personal Data; and
3. Other obligations as per the Data Protection Regulations.

We will facilitate the exercise of your rights as the Data Subject through the following mechanism:

1. In case you wish to **withdraw your consent to, restrict, or object to** the processing of your Personal Data, you may submit a request to us, clearly stating your request, specifying the relevant Personal Data, and indicating the effective date of the request. We will proceed with handling your request as follows:
 - within **02 (two) working days** after receiving your request, we will respond and provide you with adequate procedures regarding the cessation of the processing of your Personal Data;
 - within **15 (fifteen) days** (if the processing cessation does not involve a third party) or **20 (twenty) days** (if the processing cessation involves a third party) after receiving your request, we will complete the handling of your request;
 - depending on the nature and level of complexity, we may extend the time limit for handling your request no more than once, for a period **not exceeding additional 15 (fifteen) days** and we will notify you of the extension and the reasons for it in accordance with the law.
2. In case you wish to **access, rectify, request to rectify, or be provided with** your Personal Data, you may submit a request to us, clearly stating your request, specifying the relevant Personal Data, and indicating the effective date of the request. We will proceed with handling your request as follows:
 - within **02 (two) working days** after receiving your request, we will respond and provide you with adequate procedures regarding your request;
 - within **10 (ten) days** (if the processing cessation does not involve a third party) or **15 (fifteen) days** (if the processing cessation involves a third party) after receiving your request, we will complete the handling of your request;
 - depending on the nature and level of complexity, we may extend the time limit for handling your request no more than once, for a period **not**

exceeding additional 10 (ten) days and we will notify you of the extension and the reasons for it in accordance with the law.

3. In case you wish to **delete your Personal Data**, you may submit a request to us, clearly stating your request, specifying the relevant Personal Data, and indicating the effective date of the request. We will proceed with handling your request as follows:
 - within **02 (two) working days** after receiving your request, we will respond and provide you with adequate procedures to your request;
 - within **20 (twenty) days** (if the processing cessation does not involve a third party) or **30 (thirty) days** (if the processing cessation involves a third party) after receiving your request, we will complete the handling of your request;
 - depending on the nature and level of complexity, we may extend the time limit for handling your request no more than once, for a period **not exceeding additional 20 (twenty) days** and we will notify you of the extension and the reasons for it in accordance with the law.

4. In case you wish to **implement measures and solutions for the protection of your Personal Data**, you may submit a request to us, clearly stating your request, specifying the relevant Personal Data, and indicating the effective date of the request. We will proceed with handling your request as follows:
 - within **02 (two) working days** after receiving your request, we will respond to your request;
 - within **15 (fifteen) days** after receiving your request, we will complete the handling of your request;
 - depending on the nature and level of complexity, we may extend the time limit for handling your request no more than once, for a period **not exceeding additional 15 (fifteen) days** and we will notify you of the extension and the reasons for it in accordance with the law.

8. Other Bases for Processing your Personal Data

OCBC may process your Personal Data without consent as set out in Section 17 of the OCBC Data Protection Policy, and:

1. Where necessary and in urgent cases, to immediately process relevant Personal Data to protect the life, health, honor, dignity, rights, and legitimate interests of the Data Subject or others; in such cases, OCBC and other relevant third parties shall be responsible for proving the necessity and urgency of the processing;
2. to comply with the law;
3. to fulfil your contractual obligations with relevant agencies, organizations and individuals as prescribed by law;

4. to serve the activities of state agencies prescribed by specialized laws; and
5. as required by law.

9. Contacting Us - Feedback, Withdrawal of Consent, Access and Correction of your Personal Data

To contact us regarding your Personal Data or any aspect of our Data Protection Policy (including our reliance on legitimate interests), withdrawing your consent to the use of your Personal Data, or obtaining access and making corrections to your Personal Data records, please contact:

- email: [hcmcom@ocbc.com];
- phone: [028.38232627]; or
- talk to our staff at any of our branches.

10. Governing Law

This Data Protection Policy – Vietnam Annex shall be governed by the laws of Vietnam.