

OCBC Bank Privacy Notice – California Employees

Effective Date: November 15, 2024

1. Overview and Scope

We comply with the provisions of the California Consumer Privacy Act (“**CCPA**”), as amended by the California Privacy Rights Act (“**CPRA**”), as well as other applicable privacy and/or data protection laws (“**Applicable Law**”) with respect to the Processing of Personal Information. This Privacy Notice applies to all Employees of Overseas-Chinese Banking Corporation Limited, United States (“**OCBC Bank**,” “**we**,” or “**us**”) retained by us from time to time, and summarizes the categories of Personal Information we may collect from time to time and the business purposes for Processing.

This Privacy Notice does not form part of any contract of employment or other contract to provide services, nor does it imply or create any employment relationship, contract of employment, relationship to provide services, or contract to provide services. We may update this Privacy Notice at any time but if we do so, we will provide you with an updated copy of this Privacy Notice as soon as reasonably practical.

2. Definitions

“**Individual**” means any identified or identifiable natural person.

“**Personal Information**” means any information relating to an identified or identifiable Individual.

“**Employee**” means job applicants, employees, owners, directors, officers, interns, consultants, temporary resources and contractors.

“**Process**” “**Processed**,” or “**Processing**” means any operation or operations performed on Personal Information or on sets of Personal Information, whether or not by automated means, including but not limited to use, collection, storage, alteration, disclosure, erasure, or destruction.

3. Purposes for Collecting Your Personal Information

We collect and Process your Personal Information for our businesses purposes, including the following:

1. Assessing your qualifications and/or capability for a particular job, role, or task;
2. Processing background checks;
3. Managing and tracking work and performance relevant to employment or placement decisions;
4. Conducting performance reviews or determining performance requirements;
5. Developing training requirements and/or establishing or conducting training;
6. Gathering evidence for disciplinary action or termination;
7. Managing and tracking the performance of our business;
8. Administering pay and benefits;
9. Processing Employee work-related claims (e.g., workers compensation, insurance claims, etc.);
10. Establishing an emergency contact in the event of an emergency;
11. Complying with applicable labor or employment laws or obligations, including wage and hour laws, tax and withholding obligations, immigration and work authorization laws, or our commitment to equal opportunities, or complying with any other local, state, or federal law;
12. Invoicing and billing our contractors and/or our clients;
13. Monitoring compliance with Company policies;
14. Ensuring the health, safety and security of Employees, facilities, and/or company-held information;
15. Complying with any duties or obligations that we may owe our Employees as an employer or any other third parties; and
16. Other purposes reasonably required by Company.

17. We collect the following types of Sensitive Personal Information. This includes Personal Information that reveals an Employee's:

1. to perform the services or provide the good reasonably expected by an average Employee who requests those goods and services;
2. to prevent, detect and investigate security incidents that compromise the authenticity, integrity, confidentiality of stored or transmitted personal information, provided that the use reasonably necessary and proportionate for this purposes;
3. to resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions, provided that the use of the Employee's personal information is reasonably necessary and proportionate for this purpose;
4. to ensure the physical safety of natural persons, provided that the use of the Employee's personal information is reasonably necessary and proportionate for this purpose;
5. to perform services on behalf of the business, provided that the use of the Employee's personal information is reasonably necessary and proportionate for this purpose; and
6. to verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business, provided that the use of the employee's personal information is reasonably necessary and proportionate for this purpose.-

We will not use the Personal Information we collected for materially different, unrelated, or incompatible purposes without providing you with notice and obtaining your consent.

4. Personal Information We May Collect About You

Throughout the recruitment and hiring process, in the past twelve (12) months and during your time as an Employee of OCBC Bank, the following categories of Personal Information may be collected about you:

#	Category of Personal Information Collected	Collected (Y/N)	Purpose for Using Personal Information Collected
1.	Identifiers such as real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers	Yes	1-17
2.	Personal information categories listed in the California Customer Records statute (Cal. Civ. Code 1798.80(e))	Yes	1-17
3.	Characteristics of protected classifications under California or federal law	Yes	1-6, 8-9, 11, 15-17
4.	Commercial information	Yes	5, 8-12, 16-17
5.	Biometric information	Yes	1, 14, 16-17
6.	Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding Employee interactions with an internet website, application, or advertisement	Yes	3, 6, 13-17
7.	Geolocation data	Yes	1, 14, 17

8.	Audio, electronic, visual, thermal, olfactory, or similar information	Yes	3-6, 13-14, 16-17
9.	Professional or employment-related information	Yes	1-17
10.	Education information (as defined in 20 U.S.C. section 1232g, 43 C.F.R. Part 99)	Yes	1, 4-5, 8, 16
11.	Inferences drawn from any of the information above to create profiles about Employees reflecting Employee preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes	Yes	1-17
12.	Sensitive Personal Information, including, Personal Information that reveals an Employee's: <ul style="list-style-type: none"> A. Gender and emergency contacts. B. Social security, driver's license, federal/state identification card, or passport number. C. Account log-in email with any required security or access code or credentials allowing access to an account. D. Financial/banking account, brokerage account information. E. Precise geolocation. F. The contents of your mail, email and text messages unless OCBC Bank is the intended recipient of the communication. G. The processing of biometric information for the purpose of uniquely identifying an Employee. H. Personal Information collected and analyzed concerning an Employee's vaccination status. 	Yes	1-11, 13-17

We will not collect additional categories of Personal Information other than those categories listed above. If we intend to collect additional categories of Personal Information, we will provide you with a new notice at or before the time of collection.

5. Records Retention

All records of Personal Information listed above in Section 4 are retained for 7 years, in accordance with OCBC Bank's retention policy. We retain your Personal Information for no longer than is needed or permitted in light of the purpose(s) for which it was obtained. The criteria used to determine retention periods include: (i) the length of time we have on an ongoing relationship with you and provide the Services to you; (ii) whether there is a legal obligation to which we are subject; and (iii) whether retention is advisable in light of compliance with laws (such as, in regard to applicable statutes of limitations, litigation or regulatory investigations).

6. Additional Information About Personal Information We Collect

6.1 Other Records

Your file is also likely to contain a variety of other records depending on your position and relationship with us. It is not possible to set out an exhaustive list of the types of records contained in your file, but our policy is to ensure that the Personal Information we Process about you is relevant, accurate, and not excessive.

Access to your file and the Personal Information kept there is restricted to the HR Department and Internal Audit (when reasonably necessary for management purposes).

6.2 Criminal Offenses

If we learn (from any source) that Employee have been convicted of a criminal offense, we may use it as permitted by applicable law in certain employment decisions in situations when it is job-related and consistent with business necessity to do so.

7. How Do We Obtain Your Personal Information?

We collect your Personal Information from the following categories of Sources:

- **Directly from you.** When you provide it to us directly whether online, by email, fax, phone, or in-person, such as during onboarding and annual enrollment.
- **Automatically or indirectly from you.** For example, through logging and analytics tools, cookies, pixel tags, such as Google Analytics.
- **From our Service Providers.** For example, security consultants, and other Service Providers we engage.

8. Under What Circumstances May We Share Your Personal Information?

However, we may share Personal Information with the following categories of third parties:

- **Service Providers.** Companies that provide products and services to OCBC Bank such as payroll administration, pension scheme, benefits providers, human resources services, performance management, training, expense management, IT systems suppliers and support, third parties assisting with equity compensation programs, credit card companies, medical or health practitioners, trade bodies and associations, and other service providers.
- **Contractors and Third Parties.** Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisers in all of the countries in which OCBC Bank operates.
- **Public and Governmental Authorities.** Entities that regulate or have jurisdiction over OCBC Bank such as regulatory authorities, law enforcement, public bodies, and judicial bodies.
- **Our OCBC Group Entities.** Due to the global nature of OCBC Bank operations, we may disclose your Personal information with our Group entities to fulfill the purposes described above. This may include transferring your Personal Information to other countries (including countries other than where you are based that have a different data protection regime). For a full list of our entities and third parties that we may share your Personal Information, please contact us as set out below.

- **Corporate Transaction.** If the OCBC Bank business for which you work may be sold or transferred in whole or in part (or such a sale or transfer is being contemplated), your Personal Information may be transferred to a third party in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of OCBC Bank business, assets or stock (including in connection with any bankruptcy or similar proceedings).

9. **Your Rights and Choices** California residents also have certain rights in their Personal Information. In some cases, a California resident's authorized agent may contact us on their behalf to exercise these rights. The rights include:

- **Data Portability:** You have the right to request a copy of Personal Information we have collected and maintained about you in the past twelve (12) months.
- **Right to Know:** You have the right to request that we disclose certain information to you about the Personal Information we collected, used, disclosed, and sold about you in the past twelve (12) months. This includes a request to know any or all of the following:
 - (i) The categories of Personal Information collected about you;
 - (ii) The categories of Sources from which we collected your Personal Information;
 - (iii) The categories of Personal Information that we have shared, sold or disclosed about you for a business purpose;
 - (iv) The categories of third parties to whom your Personal Information was sold, shared or disclosed for a business purpose;
 - (v) Our business or commercial purpose for collecting, selling or sharing your Personal Information; and
 - (vi) The specific pieces of Personal Information we have collected about you.
- **Right to Deletion:** You have the right to request that we delete the Personal Information we collected from you and maintained, subject to certain exceptions. Please note that if you request deletion of your Personal Information, we may deny your request or may retain certain elements of your Personal Information if it is necessary for us or our service providers to:
 - (i) Complete the transaction for which the Personal Information was collected, provide a good or service requested by you, or reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform a contract between our business and you.
 - (ii) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
 - (iii) Debug to identify and repair errors that impair existing intended functionality.
 - (iv) Exercise free speech, ensure the right of another Employee to exercise his or her right of free speech, or exercise another right provided for by law.
 - (v) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
 - (vi) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the deletion of the information is likely to render impossible or seriously impair the achievement of such research, if you have provided informed consent.
 - (vii) To enable solely internal uses that are reasonably aligned with your expectations based on your relationship with us.
 - (viii) Comply with a legal obligation.
 - (ix) Otherwise use the personal information, internally, in a lawful manner that is compatible with the context in which you provided the information.

- **Right to Non-Discrimination.** We will not discriminate against you for exercising any of your California rights. We will not (i) deny you goods or services, (ii) charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties, (iii) provide you a different level or quality of goods or services, (iv) suggest that you may receive a different price or rate for goods or services or a different level or quality of products or services, and (v) retaliate against an Employee, applicant for employment, or independent contractor, for exercising their rights.
- **Right to Correct.** You have the right to correct inaccurate Personal Information about you. Once we receive and verify your request, we will use commercially reasonable efforts to correct the inaccurate Personal Information about you.
- **Right to Limit.** You have the right to request us to limit the use and disclosure of a certain Sensitive Personal Information. However, we do not Use your Sensitive Personal Information in such a manner under the CCPA that would permit such limitation.

10. Sale or Sharing of Personal Information

The CCPA defines Sale and Sharing broadly. We do not Sell or Share your Personal Information.

11. Submitting a Verified Request

To exercise your rights, you must provide us with sufficient information to allow us to verify your identity, and describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it. Once we receive the information you provide to us, we will review it and determine if more information is necessary to verify your identity as required by law, and we may request additional information in order to do so.

To exercise your California privacy rights described above, please submit a verifiable request to us by:

- Calling us at (888) 320-2609; or
- Emailing us at ContactUSA@ocbc.com.

Only you, or a person authorized by you to act on your behalf, may make a verifiable Employee request related to your Personal Information. You may only make a verifiable Employee request for Right to Know or Data Portability twice within a twelve (12) month period. The verifiable Employee request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected Personal Information or an authorized representative.
- Given the sensitivity of your Personal Information that we collect and retain, we will need to verify your identity with at least two pieces of information, such as your name (first and last) and address.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.
- We may deny your request if we are unable to verify your identity or have reason to believe that the request is fraudulent.
- Request by an Authorized Agent:

If any authorized agent submits a request on your behalf, in order to confirm that person or entity's authority to act on your behalf and verify the authorized agent's identity, we require a call be made to the toll-free number provided above, or an email be sent to ContactUSA@ocbc.com, along with all of the below items:

- To verify your authorization to request on behalf of a California resident, provide one or more of the following: (1) California Secretary of State authorization, (2) written permission from the California resident, or (3) power of attorney.
- To verify your identity, provide: (1) evidence of your identity, and (2) your name (first and last) and address.
- To verify the identity of the California resident for whom the request is being made, provide the Employee's name (first and last) and address.

We may request additional information to verify your identity and/or authority to make the request. We cannot respond to your request or provide you with Personal Information if we cannot verify your identity or authority to make the request and confirm the Personal Information relates to you. We will only use Personal Information provided in a verifiable Employee request to verify the request's identity or authority to make the request.

We will acknowledge receipt of the request within ten (10) business days of its receipt. We will respond to a verifiable request within forty-five (45) days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. Any disclosures we provide will only cover the 12-month period preceding the receipt of the verifiable Employee request. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For Data Portability requests, we will provide the responsive information in a portable and, to the extent technically feasible, in a readily useable format that allows you to transmit the information to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

12. Questions or Complaints

If you have questions or concerns about the way we have Processed your Personal Information, please contact the HR department at ContactUSA@ocbc.com.