Privacy Notice

Last Updated: 22 January 2025

Dear Candidate,

This Privacy Notice outlines the personal data protection policy for job applicants of the following Data Controllers:

1. CIMB Thai Bank Public Company Limited (the "Bank")
2. CIMB Thai Auto Company Limited
3. Worldlease Company Limited
4. Sathorn Asset Management Company Limited

(collectively referred to as the "Data Controllers").

The Bank or companies aforementioned above may provide details regarding personal data protection in addition to what is outlined in this privacy notice. You may review such details through the channels specified by your employer or organization.

The Data Controllers prioritize your privacy and are committed to protecting your personal data ("**Personal Data**") in compliance with the laws of Thailand. You are applying for a job with the Data Controllers, who are determined as the "Data Controllers" according to the Personal Data Protection Act B.E. 2562 (2019) ("Personal Data Protection Law"), wherein each data controller carries separate legal responsibilities under the Personal Data Protection Law. Each party will act as an independent data controller for the collection, use, and/or disclosure of your Personal Data throughout and for the purposes of a recruitment process.

This Privacy Notice explains: -

- What kind of Personal Data does the Data Controllers collect? This includes what you provide to the Data Controllers about yourself ("**you**", "**your**" or "**yourself**") and what the Data Controllers receive through a recruitment process.
- How do the Data Controllers use your Personal Data?
- Who do the Data Controllers disclose the Personal Data to?

- What are the choices the Data Controllers offer, including how to access and update your Personal Data?
- What are your privacy rights and how does the law protect you?

1. Collection of Personal Data

The Data Controllers collect many different kinds of the Personal Data, depending on various circumstances that are relevant to recruitment process.

The Data Controllers collect the Personal Data about you from a variety of sources, including but not limited to: -

- The data collected from you directly during the recruitment process (e.g., application forms online/offline or otherwise, CVs or resumes etc.);
- The data the Data Controllers have received during recruitment process regardless of format, including face-to-face interview, telephone or video call;
- Identification documents such as ID card, passport, driving license, military service certificate or any other documents issued by government agencies, etc.;
- The data the Data Controllers have received when you use the Data Controllers' systems, tools and websites;
- Other forms completed by you at during the recruitment process; and/or
- The correspondences with you through interviews, meetings or other assessments e.g., CCTV, recording equipment, etc.

In some instances, the Data Controllers may collect the Personal Data about you from third parties or publicly available sources, such as the references supplied by your former employers (e.g., period of previous employments, performance during previous employment, etc.), data from employment background check providers, credit bureau and data from criminal record.

Personal data refers to data that can directly or indirectly identify you. The categories of Personal Data about you that the Data Controllers collect, subject to the applicable law, include but not limited to: -

- **Personal data:** Name(s), last name, gender, date of birth, marital status, personal identification number, passport number, other government issued identification number(s) or documents issued by the government agencies for verification purposes, tax identification number, nationality, image of ID card, passport, or driving license, signatures, authentication data, background check data, data provided by you as an answer to the Data Controllers' authentication question, photographs, CCTV images, and recordings of video and audio;
- **Family data:** Family status, relationships with family members, and personal details of family members, such as names, middle names, surnames, ages, and contact data of family members, spouses, and children;
- **Contact data:** Personal contact details, including any data you provide to the Data Controllers to enable them to reach you, such as address, phone number, email, and profile details on social media platforms.

- **Educational data:** The details of educational background, transcript, educational achievements and other additional courses;

- **Professional data:** The details of profession, professional memberships, former employer's feedback, professional qualifications, skills, experience, trainings and employment history, Job responsibilities, organizations, positions, and other personal data related to job performance.

- **Financial data:** The details of your salary and benefits (such as bonus and insurance coverage);

- **Electronic Data:** Any data related to computer systems or technological devices you use to access the Data Controllers' systems, applications, websites, or social media platforms. This includes computer identifiers (IP Address or MAC Address), cookies, or similar technologies, activity logs, identifiable or online tracking data, login data, usage data, browsing history, unique device identifiers, and geolocation data. It also

encompasses other technical data generated during platform and system use throughout the course of employment.

- **CCTV Data:** In certain operational areas, the data controller may implement CCTV systems for security purposes and/or to comply with applicable regulations.
- **Other details:** The data may be received from the interview; and
- **Sensitive Personal Data:** The Personal Data that the law specifically prescribes, including data about your race, ethnic origin, political opinions, religion or philosophical beliefs, sexual behavior, criminal records, health data, disability, labor union membership, biometric data or any other data which affects you in the same way as announced by the Personal Data Protection Committee.

During the recruitment process, the Data Controllers or the aforementioned companies may also collect some Sensitive Personal Data e.g. your criminal record or data relating to health about you to ensure that you are permitted to undertake the role you applied for and to assess and evaluate that you are suitable for employment in the role you applied for and, to ensure that the Data Controllers comply with regulatory obligations placed on the Data Controllers with regard to the Data Controllers' hiring. The Data Controllers will not collect, use and/or disclose this type of Personal Data without your consent unless the law allows the Data Controllers to do so.

2. Use of Personal Data

The Data Controllers may collect and use your Personal Data only if the Data Controllers have proper reasons to do so. This includes sharing it to external party. .

The Data Controllers will rely on one or more of the following lawful bases when collecting, using and/or disclosing your Personal Data: -

- When it is to fulfil a contract the Data Controllers have or will enter into with you (contractual basis) – that is when the Data Controllers need your Personal Data to deliver a contractual service to you or before entering into a contract with you;

- When it is the Data Controllers' legal obligation (legal obligation basis) – that is when the Data Controllers need to collect, use and/or disclose your Personal Data to comply with the law or statutory obligation;
- When it is in the Data Controllers' legitimate interest (legitimate interest) – that is when the Data Controllers collects, uses and/or discloses your Personal Data for the Data Controllers' legitimate interest as permitted under the law, so long as your fundamental rights are not overridden by the Data Controllers' legitimate interest, and/or;
- When you consent to it (consent basis) – that is when you allow the Data Controllers to collect, use and/or disclose your Personal Data for certain purposes.

Under the Personal Data Protection Act B.E. 2562 (PDPA), certain types of personal data are classified as sensitive personal data, which are afforded greater protection. In this regard, the Data Controllers will not purposely collect, use and/or disclose this type of Personal Data without your consent unless the law allows the Data Controllers to do so. If the Data Controllers will collect, use, and/or disclose such sensitive Personal Data, it will only do so upon your consent or only for one of the following purposes: -

- Performance of contractual obligations between you and the Data Controller;
- Legitimate Interests;
- Prevention or suppression of danger to life (vital interest);
- Compliance with legal obligations related to labor protection;
- Establishment, compliance, exercising and/or defending legal claims;

The Data Controllers process personal data in accordance with the purposes and bases established under the Personal Data Protection Law, which govern the collection, use, and/or disclosure of your personal data as outlined below. Please consider the specific purposes based on your relationship with the data controller or employment context on a case-by-case basis.

The purposes for which the Data Controllers may collect, use and/or disclose your Personal Data, subject to the applicable law, and legal basis on which the Data Controllers may perform such collection, use and/or disclose, are : -

Purposes of data collection, use and/or disclosure	Lawful basis for collection, use and/or disclosure
Recruitment Process	
● To carry out any actions related to your job application and other matters as requested by you ● To verify your identity ● To assess your skills, qualifications, and suitability for the role ● To carry out background and reference checks, where applicable ● To communicate with you about the recruitment process and other matters as per your request ● To keep records related to the Data Controllers' hiring process. ● To comply with regulatory requirements	• Contractual basis • Legal obligation basis • Consent basis • Legitimate interest basis

Whether the Data Controllers will consider selecting you to perform in any position or not is considered to be the collection, use, and/or disclosure of Personal Data under the Data Controllers' legitimate interests. Since, such collection, use, and/or disclosure is for the benefit of the Data Controllers in appointing a suitable candidate to each role, the Data Controllers, therefore needs to collect, use and/or disclose your Personal Data to decide whether to enter into a contract with you or not.

The collection, use, and/or disclose of Personal Data may potentially include your sensitive Personal Data. The sensitive Personal Data is not routinely collected from all candidates, it may be collected where the Data Controllers have legal obligations or consents from you to do so, or if you choose to disclose it to the Data Controllers during the period of your relationship with the Data Controllers.

The Data Controllers may collect your CV and the results from any tests you took to decide whether you meet the basic requirements to be shortlisted for the role in question. If you do, the Data Controllers will decide whether your application is suitable to invite you for the interview. If the Data Controllers decides to call you for the interview, the Data Controllers will use the data you provide to the Data Controllers at the interview to decide whether to offer you the role. If the Data Controllers decide to offer you the role, the Data Controllers may then take up the references and/or any other checks before confirming your appointment.

In Case of Failure to Provide Your Personal Data to the Data Controllers

Where the Data Controllers is required by law to collect your Personal Data or need to collect your Personal Data under the terms of contract that the Data Controllers have with you and you fail to provide your Personal Data when requested, the Data Controllers may not be able to perform obligation under the contract the Data Controllers have with you or plan to enter into with you (for example, to process your job application). In this case, the Data Controllers may have to decline to process your job application, but the Data Controllers will notify you if this is the case at the time your Personal Data is collected.

3. Disclosure of Personal Data

The Data Controllers may share your Personal Data internally with the followings: -

- The Data Controllers' employees who would have a managerial responsibility for you or are acting on their behalf;
- The Data Controllers' employees who have the responsibility for recruitment processes or who works in Human Resource and/or employees assigned to undertake the recruitment process (e.g., recruitment, assessment, pre-employment screening, etc.);
- The Data Controllers' employees in the recruitment business unit and/or employees assigned to undertake the recruitment process who will assess and consider you for the interview;

- The Data Controllers' employees in the regulatory compliance unit with the responsibility to investigate the issues of non-compliance with laws and regulations, policies and contractual requirements;
- The Data Controllers' employees in IT department and system owners who manage user access;
- Audit and investigation employees in relation to specific audits/investigations, and/or;
- Security personnel and receptionists of the Data Controllers who are stationed and operating at the Data Controllers' facilities/premises.

The Data Controllers may also need to share your Personal Data with certain external parties including:

- Companies under financial business group of the Bank, or companies listed above, including other companies under business group of the Data Controllers (For further details, please refer to https://www.cimbthai.com/th/personal/who-we-are/about-us.html)
- Your referees;
- Recruitment agency;
- Academic institutions (e.g., universities, colleges, etc.) In validating the data you have provided to the data controllers;
- Suppliers who provide services on the data controllers' behalf; and/or
- External parties who undertake a background screening on the data controllers' behalf and related government authorities (e.g., criminal record, background check, and etc.).
- Regulatory authorities, authorized entities, and legally empowered agencies.
- Third parties that the data controller may intend to transfer rights to, and/or transferees of rights in transactions or mergers and acquisitions involving the data controller.
- Third parties and/or other entities to fulfill the purposes stated in this Privacy Notice.

Except as described in this Privacy Notice, the Data Controllers will not use the Personal Data for any purposes other than the purposes as described to you in this Privacy Notice. Should the Data Controllers intend to collect, use or transfer additional data which are not described in this Privacy Notice, the Data Controllers will notify you and obtain your consent prior to the collection, use and/or disclosure unless the Data Controllers are permitted to do so without your consent under the law. You will also be given the opportunity to consent or to decline approval of such collection, use and/or transfer of your Personal Data.

The Data Controllers will continue to adhere to this Privacy Notice with respect to the data the Data Controllers have in their possession relating to prospective, existing and former candidates.

Cross-border Transfer of Personal Data

Your personal data may be transmitted or transferred to foreign countries and may be collected and/or used overseas (e.g., Malaysia, a country within the Data Controllers' company group), including cloud service provider (Cloud Computing) where the Data Controllers conduct their business or in compliance with legal obligations to fulfill employment purposes or to serve your interests.

The recipient countries may not have data protection measures deemed adequate by the Personal Data Protection Committee under the Personal Data Protection Law. In such case, the Data Controllers will ensure that the transfer or transmission is conducted with appropriate data protection measures and complies with applicable laws. This may include, where necessary, entering into standard contracts (or equivalent measures) with parties outside Thailand. For instance, your personal data may be disclosed to other companies within the Data Controllers' group in accordance with internal policies or Binding Corporate Rules (BCRs), acceptable contractual clauses, or other suitable protective measures. The Data Controllers may need to transmit or transfer personal data to fulfill contractual obligations to which you are a party, to carry out your pre-contractual requests, to comply with legal requirements, to protect the public interest, to benefit you under the agreement between the Data Controllers and the recipient of the personal data, and/or upon obtaining your consent. The Data Controllers will inform you of the inadequacy of data protection standards in the destination country receiving your personal data. Nevertheless, laws in certain countries may mandate the Data Controllers to disclose specific personal data (e.g., to tax-related agency).

In such case, the Data Controllers will disclose the personal data only to those legally entitled to access it.

4. Retention of Personal Data

The Data Controllers will only retain your Personal Data for as long as it is necessary to carry out the purpose for which it was collected only, that is., for the recruitment, employment and legal reasons, or compliance with the applicable laws.

The Data Controllers will keep your Personal Data for the duration of your recruitment and for a period of 3 years from the date the process of recruitment ends. However, in the event of regulatory or technical reasons, the Data Controllers may keep your Personal Data for longer than the recruitment period. If the Data Controllers no longer need to retain the Personal Data beyond the legally required period, the Data Controllers will proceed to destroy, delete or anonymize it (ensuring it can no longer be associated with you)

5. Accuracy of Your Personal Data

The Data Controllers require your assistance to ensure that your Personal Data is current, complete and accurate. Please inform the Data Controllers of any changes to your Personal Data by:

- Contacting the Data Controllers' HR representative at careers@cimbthai.com, or;
- Updating your data at/via Oracle Recruitment Cloud.

The Data Controllers will occasionally request the updates from you to ensure the Personal Data the Data Controllers use to fulfill the purposes of collection, use and/or disclosure are current, accurate and complete.

6. Your Rights as Data Subject

Under certain circumstances, you have rights under data protection law in relation to your Personal Data. It is the Data Controllers' policy to respect your rights and the Data Controllers will act promptly and in accordance with any applicable law, rule or regulation relating to the collection, use and/or disclosure of your data.

Details of your rights are set out below: -

- **Right to Withdraw Consent**: When the Data Controllers collects, uses and/or discloses your Personal Data under your consent, this right enables you to withdraw your consent to the Data Controllers' collection, use and/or disclosure of your Personal Data, which you can do at any time. The Data Controllers may continue to collect, use and/or disclose your Personal Data if the Data Controllers have another basis to do so.

  You have the right to modify your consent provided to the data controller at any time through the channels specified by the Data Controllers in this Privacy Notice and/or any other privacy notices issued by the Data Controllers. This right is subject to legal limitations and/or contractual obligations that benefit the personal data owner.

- **Right to Access:** This enables you to receive a copy of your Personal Data from the Data Controllers.

- **Right to Correct:** This enables you to have any inaccurate, outdated and/or incomplete Personal Data corrected. Please see above in 5. (Accuracy of your Personal Data) for detail of how you can request to have your Personal Data corrected.

- **Right to Erasure:** This enables you to request the Data Controllers to delete, destroy or anonymize your Personal Data where there are no reasonable grounds for the Data Controllers to continue collecting, using and/or disclosing it. This right may be exercised alongside your right to object, as outlined in the subsequent section. However, this does not grant the right to request the deletion of all personal data. The Data Controllers will consider each request carefully in accordance with the requirements of any laws relating to the collection, use and/or disclosure of your Personal Data.

- **Right to Object:** This enables you to object to the collection, use and/or disclosure of your Personal Data where the Data Controllers are relying on the legitimate interest. You also have the right to object where the Data Controllers are collecting, using and/or disclosing your Personal Data for direct marketing purposes and profiling activities.

- **Right to Request Suspension of Personal Data Use:** You have the right to request the Data Controllers to temporarily suspend the collection, use, and/or disclosure of your

personal data. For example, if you want the Data Controllers to verify its accuracy or the reasons for collecting, using and/or disclosing it.

- **Right to Data Portability:** In certain cases, you have the right to request a copy of your personal data in a commonly used electronic format. You also have the right to request the Data Controllers to transmit or transfer your personal data in such a format to another data controller, where feasible by automated means. Additionally, you may request the direct transmission of your personal data from one Data Controller to another, unless it is technically unfeasible. This right only applies to your Personal Data that you have provided to the Data Controllers**.** The right to data portability only applies if the collection, use and**/**or disclosure is based on your consent or if the Personal Data must be collected, used and**/**or disclosed for the performance of obligation under a contract**.**
- **Right to Lodge a Complaint:** This enables you to file the complaint with a related government authority, including but not limited to, the Thailand Personal Data Protection Committee in the case where, in your view, the Data Controllers, the Data Controllers**'** employee or service provider violates or fails to comply with the Personal Data Protection Law or notifications issued thereunder.

You may exercise any of your rights at any time using the contact details set out in 10. (Contact us) below. You will not have to pay a fee to access your data (or to exercise any of the other rights). However, the Data Controllers may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, the Data Controllers may refuse to comply with your request in these circumstances.

The Data Controllers may need to request specific data from you to help the Data Controllers confirm your identity and ensure your right to access your Personal Data (or to exercise any of your other rights). This is a security measure to ensure that your Personal Data is not disclosed to any person who has no right to receive it. The Data Controllers may also contact you to ask you for further data in relation to your request to speed up the Data Controllers' response.

The Data Controllers make an effort to respond to all legitimate requests within 30 days. Occasionally, it may take the Data Controllers longer than 30 days if your request is

particularly complex or you have made a number of requests. In this case, the Data Controllers will notify you and keep you updated.

Handling of Complaints

In the event that you wish to file a complaint regarding how the Data Controllers collect, use and/ or disclose your Personal Data, please contact the Data Controllers at careers@cimbthai. com and the Data Controllers will endeavour to address your request as promptly as possible. This does not prejudice your right to file the complaint with a government authority or the Personal Data Protection Committee.

7. Security of your Personal Data

The Data Controllers place the utmost importance on ensuring the security of your Personal Data. The Data Controllers regularly review and implements up-to-date physical, technical and organizational security measures when collecting, using and/or disclosing your Personal Data. The Data Controllers have internal policies and controls in place to ensure that your Personal Data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by the Data Controllers' employees in the performance of their duties. The Data Controllers' employees are trained to handle the Personal Data securely and with utmost respect, failing which they may be subject to a disciplinary action. In addition, the Data Controllers require their personnel, service providers, and recipients of data from the Data Controllers to maintain the confidentiality of personal data in accordance with the confidentiality measures established by the Data Controllers.

8. Your Responsibilities

You can manage your personal data collected, used, and/ or disclosed by the Data Controllers under this Privacy Notice to ensure its accuracy, completeness, currency, and to prevent any potential misunderstandings. You are responsible for ensuring that the Personal Data you provide, either directly or on your behalf, to the Data Controllers, is accurate and up to date, and you are also required to promptly notify the Data Controllers of any changes or updates to your personal data.

When you have entered into an employment contract with the Data Controllers. You will have some responsibilities under your employment contract to provide the Data Controllers

with the Personal Data in order to exercise your statutory rights. Failing to provide the Personal Data may mean that you are unable to exercise your statutory rights.

Certain Personal Data, such as contact details, and payment details, must be provided to the Data Controllers in order to enable the Data Controllers to enter into the contract of employment with you. If you do not provide such Personal Data, this will hinder the Data Controllers' ability to administer the rights and obligations arising as a result of employment relationship efficiently.

9. Revision of the Data Controllers' Privacy Notice

The Data Controllers keep the Privacy Notice under a regular review which is subject to changes. The date of the most recent revision of the Privacy Notice is indicated at the top of this page.

10. Contact Channels for Data Controllers

If you have any questions in regard to the protection of your Personal Data or if you wish to exercise your rights, please contact**: -**

List of Data Controllers	Contact Channels
CIMB Thai Bank Public Company Limited	• Contact at Recruitment / Human Resources Operations Department, or • Data Protection Officer at dpo@cimbthai.com, or • Human Resources representative at careers@cimbthai.com
CIMB Thai Auto Company Limited	• Contact at Recruitment / Human Resources Operations Department, or • Data Protection Officer at dpo@cimbthaiauto.com, or • Human Resources representative at hris&service@cimbthai.com
WorldLease Company Limited	• Contact at Recruitment / Human Resources Operations Department, or • Data Protection Officer at dpo@worldlease.co.th , or • Human Resources representative at hris&service@cimbthai.com

Sathorn Asset Management Company Limited	• Contact the bank's Recruitment / Human Resources Operations Department, or • Data Protection Officer at DPO-STAMC@sathornamc.com , or • Human Resources representative at careers@cimbthai.com , or hris&service@cimbthai.com