



Privacy Policy for Human Resource

Krung Thai Bank Public Company Limited (the "Bank") recognizes the importance of protecting personal data of the data subjects, including but not limited to job applicants and job interviewers, current employee based in Thailand or abroad or other organizations, former employees, retired employees, temporary employees, contractors, outsource, scholarship student, witnesses and other relevant persons (collectively called "you"). This Privacy Policy ("Privacy Policy") is provided to describe the means which the Bank use in collection, uses, disclosure and/or cross-border transfer of personal data including informing the data subject about their rights under the Personal Data Protection Act. In order for the Bank to act in a transparent manner regarding the Bank's activities of collection, use, disclosure and/or cross-border transfer of personal data of the person specified in this Privacy Policy under the laws governing personal data protection.

The Bank may collect such personal data through various channels, such as the Bank's branches, website, email, during employment exhibitions and events, or when the Bank's representative goes visit you or arrange meetings with you, or from other sources (such as online platforms or other public sources) or through affiliated companies, subsidiaries, business partners, government agencies or third parties and other places and/or other communication channels whereby the Bank collects your personal data. Please read this Privacy Policy together with the terms and conditions of the employment under the employment contract or the employment of related services which might be some difference regarding the collection, use, disclosure and/or cross-border transfer of your personal data.

1. The Bank's procedures for the collection of personal data

1.1 Personal data collected by the Bank

Personal data means any information related to you which can directly or indirectly identify you (excluding the deceased's information) as specified below.

Sensitive personal data means personal data which is classified as sensitive personal data in accordance with the law. The Bank may collect, use, disclose and/or cross-border transfer of your sensitive personal data, only when the Bank receives an explicit consent or as otherwise permitted by law.

1.2 Types of persons and personal data collected by the Bank

The Bank may collect your personal data. The personal data that the Bank may collect shall depend on your current relationship with the Bank or your position, duties and responsibilities towards us and the types of your personal data. The details are as follows;

(1) job applicants and job interviewers, current employee based in Thailand or abroad or other organizations, former employees, retired employees, temporary employees, contractors, outsource, scholarship student, witnesses and other relevant persons.

Personal Data

The Bank may collect your personal data as follows;

1) Personal information, such as title, first name, last name, gender, date of birth, age, blood group, nationality, hometown, signature, marital status, number of children, military service history, Buddhist ordination history, information relating to documents issued by government agencies (e.g., ID card, passport, visa, taxpayer identification number, work permit, house registration number, photograph, evidence of a change of name/surname), airline mileage, vehicle registration number, vehicle color and model, bank account information, credit card number and security number on the back of the credit card, Political tenure history,

collateral information, credit bureau history, proof of tax payment, financial background check (e.g. AML List, Suspect List, Bankruptcy).

2) Contact information, such as residential address on Identity card or house registration, current residential address, work address, phone number, fax number, email address, social media accounts, contact channel through social media and information from social networks, address information of abroad scholarship students.

3) Education information, such as educational qualifications, proof of educational qualifications, educational institution, department, major, graduation year, cumulative grade point average, copy of academic transcript, copy of degree certificate, related training courses/seminars, diploma/special qualifications, training institutions, training period, year of training, information for scholarships administration (e.g. test results used for further study in the country and abroad, acceptance information from foreign educational institutions)

4) Working information, such as employee ID, user ID/default password, employee ID card information, position, group name, department name, department code, working period, working time record, salary, proof of income, previous employment verification letter, investment items/contracts, company/business information you are involved in, stakeholder report of another juristic person, shareholding information of another juristic persons, securities holding report of the Bank, proof of income tax payment, information about your license (e.g. license card number, card issue date and card expiration date, exam history and results), work experience (e.g. workplace (current/previous), occupation, position, salary/monthly income, compensation details, employment start date, employment end date), civil servant information (if any), and other support documents.

5) Information about your salary and benefits, such as salary record (e.g. base salary, salary range, bonus), expenses, compensation, commission, overtime wage, shift pay, medical expenses, off-site work wage, travel expenses, special compensation and welfare, deduction information (e.g. provident funds, taxes, social security), compensation, and pension.

6) Information about surveillance for security, such as internal system access information, building access information, closed-circuit television cameras information, working time record (internet usage log, email, and phone usage data, passcode for information system and the right to access the Bank's information system)

7) Information about operation and disciplinary, such as performance appraisal, job promotion, employee transfer, job rotation and change of position, indicator (disciplinary action information, disciplinary procedures and warnings, detail of complaint consideration and its result, training record)

8) Leave information, such as leave record (e.g. annual leave, sick leave, sterilization leave, personal leave, maternity leave, parental leave, training/study leave, military service leaves)

Sensitive Data collected by the Bank

The Bank will collect your sensitive personal data as follows;

- 1) Sensitive personal data as appeared on identification documents (e.g. religion).
- 2) Nationality
- 3) Race
- 4) Biological data (such as fingerprints, biometric data, biometric face recognition)
- 5) Disability
- 6) Information related to health
- 7) Criminal records
- 8) Information about income

In this respect, the Bank will collect, use, disclose and/or overseas transfer of your sensitive personal data only when the Bank receives an express consent or as legally permissible.

(2) Personal data of third party

If you provide the Bank with personal data of third parties such as your spouse, child, parents, guarantor, chief, co-borrower, reference, or former employer by providing personal data of such person to the Bank, such as first name, last name, detail of home address/office address, occupation, income, telephone number, identification number, passport number, nationality, date of birth, gender, **type of child**, number of child, marriage certificate information (e.g. certificate number, registration date, location of registration office, province, agreement), signature, related company/business information, stakeholder report of another juristic person, shareholding information of another juristic persons, securities holding report of the Bank, collateral information. Please inform this Privacy Policy to such third parties for acknowledgement and request for consent if necessary or as required by law for disclosure of personal data of third parties to the Bank.

(3) Personal data of incompetent persons

The Bank collects personal data relating to a minor, a quasi-incompetent person and an incompetent person only when the Bank receives a consent from a guardian or a curator. The Bank has no intention of collecting personal data from a person aged under 20 years old without a consent of a guardian or a curator, a person taking care of the person as required by laws (as the case may be). In case the Bank was aware that the Bank had unintentionally collected personal data from any person aged under 20 years old without a consent of a guardian or a curator, a person taking care of the person as required by laws (as the case may be), the Bank will immediately delete such personal data or will collect, use, disclose and/or cross-border transfer only on other lawful basis other than a consent or to extent permitted by law.

2. The purpose of collection, use, disclosure and/or cross-border transfer of your personal data by the Bank.

The Bank may collect, use, disclose and/or cross-border transfer the personal data and sensitive personal data for the following purposes:

2.1 The purpose of obtaining your consent

(1) Sensitive Data

The Bank may use your sensitive personal data for the following purposes;

- 1) Sensitive personal data as appeared on identification documents (e.g. religion, race):** for the purpose of your personal identity verification and proof.
- 2) Religion:** for the purpose of hiring and assessing qualification for employment, for visa Preparation and facilitation, and for providing welfare.
- 3) Race:** for the purpose of hiring and assessing qualification for employment, for visa Preparation and facilitation, and for providing welfare.
- 4) Biological data (such as fingerprints, biometric data, biometric face recognition):** for the purpose of your personal identity verification and proof, registration for seminars and meetings, access to the Bank's internal system, access to the building)
- 5) Disability:** for the purpose of hiring and assessing qualification for employment, facilitation, and welfare provision.
- 6) Health information (such as medical history, accident history, health check and medical treatment):** for the purpose of hiring and assessing qualification for employment, for the Bank's consideration

on human resource management such as benefit, leave, and/or disbursement, annual health check, medical expenses.

7) Criminal record: for the purpose of hiring and assessing qualification for employment, for examination or disciplinary investigation.

If the Bank require your consent for collection, use, disclosure and/or cross-border transfer of your personal data, you have the right to withdraw your consent at all times. This can be done by contacting at <https://www.intranet.ktb/intranet/index2.html>

The withdrawal of consent may result the Bank from not able to collect, use, disclose and/or cross-border transfer your personal data for the above-mentioned purposes and the Bank may not able to perform duties or obligations under the employment contract or services contract to you, in whole or in part. Therefore, the withdrawal of consent will not affect the collection, use, disclosure, and/or cross-border transfer of your personal data and sensitive personal data that you had given your consent prior to such withdrawal.

2.2 Other purpose and any applicable law for collection, use, disclosure and/or cross-border transfer of your personal data

The Bank will collect, use, disclose and/or cross-border transfer of your personal data by lawful basis on legitimate interest, by lawful basis on entering into and performing the contract, lawful basis on legal obligation or other lawful basis on permissible personal data protection, as the case may be, depending on the relationship between you and the Bank such as when you enter into an employment contract or service contract with the Bank, for the following purposes, including but not limited to:

(1) For job application and/or employment or outsourcing service management, such as for recording information collected from job applicants as part of the application process, for assessment the suitability and qualification of job applicant, for the recruitment process, screening and checking the applicant's background/status, for decision making on job interview and employment, and enter into a contract, for salary determination and other basic contract information for new employees in a particular position, for data analysis to improve the recruitment process to be more efficient.

(2) For administration, compensation, and welfare, such as for paying salary, wages, expenses, compensations, bonus, commissions, for making disbursement of any expenses and benefits to you, for setting a special interest rate for loan, for funeral money support, for requesting the royal decorations, for providing welfare and insurance, for provident fund management, for scholarships management to employees and scholarship students.

(3) For human resource management and relationship management, such as for proving, identifying, and verifying you or your identity, for recording working information and managing disciplinary matters in order to comply with the Bank's regulations and work regulations, for work-related activities management, for issuance an employee ID card, for your potential development, for providing internal and external training as well as strategy of the Bank, for issuing a certificate of completion of a training or examination, for recording working hours, clock in and out at work [by tracking Internet usage, e-mail, and telephone], for managing general employment, for performance appraisal, for consideration of promotion, salary adjustment and special annual compensation, for managing work permits for foreign employees, for managing the list of employee who abandoned work and the list of serious corrupt employees (Blacklist), for statistical analysis and internal reports, for employee and internal working group management, for management/approval of leave, annual leave and health care management, for employee analysis, performance appraisal and salary adjustment, for support and facilitation the work on requesting licenses, for participation in training and other activities of the Bank, for consideration of adjusting, transferring, rotating, changing position or workplace of an employee including working abroad, or between the Bank and its affiliates, for changing the type of employment contract,



for keeping your information accurate and up-to-date, for debt, interest, and damage collection (if any), for managing and operating related to employment, termination, dismissal, termination of contract and retirement.

(4) For the operation of the Bank and companies in our group, such as for customer service, contacting a partner, making a contact, and for other purposes as determined by the Bank in connection with your employment or service (e.g. to carry out activities or operations for the Bank or on behalf of the Bank) as set out in an employment contract, work rules, or documents related to Human Resources,

(5) For purposes of marketing, sales promotions and communication, such as carrying out activities related to marketing and communication, marketing advertising, sales, special offers, news, public relations, promotion and presentation of the Bank's products and services of financial business group, the Bank's affiliates, business partner and other legal entities, including information of products and services that are directly and indirectly close to your interest or the bank expect you to be interested.

(6) For management of information technology, such as for the purpose of business operations of the Bank, for carrying out public relations within the Bank, including information technology operation, communications system management, information technology security of the Bank, for testing employees' awareness on information technology security systems.

(7) For communication with you, employee, the Bank, other persons and third parties, (such as current and future business partners, sellers, customers, and government officials) this includes communications related to former employees' activities, exit interview prior the employee leaving the Bank, communication with your emergency contact.

(8) For compliance with laws, such as compliance with laws, legal procedures or order of government agencies, and/or in cooperation with courts, regulator, government authorities, and law enforcement, when the Bank has a reason to believe that the laws enforce the Bank to do so. If it is necessary to disclose your personal data in compliance with laws, procedures or government orders, including internal investigation, complaint or claim, crime investigation or crime prevention, fraud, and lawfully establishing legal claims.

(9) For protection of legitimate interests of the Bank, such as for security and the rightfulness of the Bank's business or the Bank's affiliates, for exercising the Bank's right and protecting the Bank's interest or the Bank's affiliates when it is necessary and lawful, for instance, for investigation, protection, and response to complaints, intellectual property infringement complaints or violation of laws, for managing and preventing the loss of assets, for monitoring the compliance with terms and conditions of the Bank, for investigation and prevention of wrongdoing occurred at the Bank's premises, including operating the closed-circuit television (CCTV), for monitoring other situations, for preventing and reporting criminal incidents, for security and legitimacy of the Bank's business, for management, for preparation of reports, internal policies according to the Bank's scope of operations.

(10) For protection of data, confidentiality, and property, such as the protection of customer, employee, and other persons, security of systems and premises of the Bank and its affiliates, or for any other benefits in the protection of data, confidentiality or property of the Bank and its affiliates.

(11) For risks management and right protection, such as management of risks, efficiency monitoring and risks evaluation in order to set risks index, making summary report for risks management in order to evaluate and predict potential risks, including solutions towards the products risk evaluation and giving suggestion in case there are changes and finding solutions for the risk management, protecting property, safety or the operation of the Bank or the Bank's financial business group, you and other person in order to enable the Bank to seek remedies or limit damage that may occur, investigation of breaches of agreements, establishing, exercising or lawfully defending against legal claims, including legal action.

(12) For verification and prevention of the Bank business risks/for fraud detection, such as for your personal verification, for monitoring the compliance with the law and other regulations (for compliance with the money laundering prevention and suppression and corruption prevention regulations), including conducting the monitor and internal record, property management, fraud database, system and control other businesses, for taking any action that may cause fraud, cyber threat, debt default/breach of contract (e.g. bankruptcy Information), as well as collection, use, and/or disclosure of personal data for acceleration in the Bank's operations or legal entities in the same business group with the Bank in prevention, dealing with, reducing or conducting the same manner, conducting disciplinary processes, investigation process and disciplinary action.

(13) For corporate transactions, including the case of business reorganization, merger, sale, purchase, joint venture, assignment, transfer, or dispose of business, property or share, rehabilitation, joint venture, or other similar transaction either partially or all of business, the Bank may disclose your personal data to one or more assignees as a part of such transaction.

(14) For prevention or stop of dangers to lives, bodies or health of persons

In this respect, if you do not provide personal data to the Bank, it may have impact on you, such as the Bank may not proceed its duties or obligations under the employment contract or to provide services to you, such as The Bank may not proceed with your requests; you may experience some inconvenience or do not obtain the performance of agreements and you may receive damage or lose opportunities. In addition, your refusal to provide personal data may affect the compliance with any law that the Bank or you must comply with and may have related penalties as a consequence.

3. Who does the Bank disclose or transfer your personal data to?

The Bank may disclose or transfer your personal data to the following third parties, whereby the collection, use or disclosure and/or cross-border transfer of personal data for purposes under this Privacy Policy. These third parties may live in Thailand or abroad, you can check on the privacy policy of such third parties in order to understand the details regarding the methods of the collection, use and/or disclosure of your personal data, since you are a data subject as specified in the privacy policy of such third parties.

3.1 Affiliates

The Bank may have to disclose your personal data, for the purposes specified in Clause 2 herein, to overseas branches of the Bank, the Bank's financial business group and the Bank's affiliates. The disclosure of your personal data to such financial business group and affiliates will make such other companies be able to use your consent obtained by the Bank in order to collect, use, disclose and/or cross-border transfer of your personal data.

3.2 The Bank's Service providers

The Bank may outsource the Bank's services on behalf of the Bank in order to assist operations and to provide you with products and services, including any procedure for providing you benefits. The Bank may share your personal data to the outsourcing parties, the representative's service providers, including but not limited to (1) internet service providers, software developers, website developers, digital media developers, information technology service providers and service providers of information technology support, (2) logistics and transportation service providers, (3) training providers and its lecturer, (4) event service providers, (5) data storage and cloud storage service providers, (6) auditors, (7) lawyers, legal counsels for the Bank's benefits, including exercising legal claims and defending against legal claims, audits and/or other professionals in assisting the Bank's business operations, (8) document storage and/or disposal service providers, (9) recruitment and Human Resources service provider, (10) telecommunications service providers, (11) outsourcing service providers.

During the provision of such services, the service providers may have the right to access your personal



data, however the Bank will only provide your personal data to the service providers as necessary for the services. The Bank will ensure that the service providers do not use your personal data for any other purposes and they must protect a security of your personal data in compliance with the law.

3.3 The Bank's business alliances

The Bank may transfer your personal data to the Bank's business partner for conducting business and provide services to the Bank's customers and groups of customers who tend to use services from the Bank, including but not limited to educational institution, agency or training service provider or professional training institution, hospital, air ticket company, insurance company, agency [card manufacturing company, printing company, analytics, research, and survey service provider]

3.4 Third parties as specified by laws

In some cases, the Bank may have to disclose your personal data in compliance with the laws, including orders issued by laws which include law enforcement agencies, courts, Legal Execution Department, authorities, government agencies (e.g. the Bank of Thailand, National Health Security Office, Office of the Civil Service Commission, Royal Thai Police, the Revenue Department, Ministry of Finance, State Enterprise Policy Committee, The Securities and Exchange Commission, Territorial Defense Command, Military Recruitment Office, and/or other agencies) or other persons that the Bank believes it is necessary to comply with the laws or to protect the Bank's rights, the rights of third parties or for the security of persons or for inspection, prevention or corruption problem solving, security, safety, including any other risk.

3.5 Associations and clubs

In some cases, the Bank may have to disclose your personal data to relevant institutions, associations or clubs, such as Auditors Association of Thailand, Financial Planners Association, including the Thai Bankers' Association for developing your potential by providing training courses, testing and maintaining status in order to support you to receive special qualifications

3.6 Assignees

In case of a business reorganization, merger and acquisition, entire business or part of business transfer, sale, purchase, joint venture, grant, transfer part or all of business, assets, shares, or other similar transactions, the Bank shall have to disclose your personal data to third parties who have been assigned or wish to be assignees of the Bank such as new employer or who has potential to be a new employer. In this respect, the Bank shall procure that such third parties shall comply at all times with this Privacy Policy when there is a collection, use or disclosure and/or overseas transfer of your personal data.

3.7 Third parties

The Bank may disclose your personal data under the legal basis according to the purposes specified in this Privacy Policy to other third parties, such as customer, other legal references, hotel, as the case may be.

4. Cross-border transfer of your personal data

The Bank may cross-border transfer your personal data to other countries which may have a higher or lower standard of personal data protection than Thailand, such as when the Bank collects your personal data on cloud platforms or server outside Thailand for information technology support.

When it is necessary for the Bank to transfer your personal data to other countries which having a lower standard of personal data protection than Thailand, the Bank shall procure to ensure that there is an appropriate protection measure or personal data protection laws allow the transfer of personal data, e.g., the Bank may have to obtain a confirmation according to the contract from third parties who have access to such personal data that your personal data shall be protected under the same personal data protection standard of Thailand.

5. Duration of personal data storage period

The Bank shall retain your personal data for a necessary period for compliance with the purposes stated in this Privacy Policy. In this respect, for compliance with the law, the Bank may have to retain your personal data as long as it required by laws.

6. Your rights as the Data Subject

Rights stated in this section mean legal rights relating to your personal data whereby you may use these rights with persons required by laws, in this regard, under the conditions stipulated by law and the process of the rights management of the Bank, such rights include the following rights:

(1) Right of access to personal data, you may have the right to access personal data or request for a copy of personal data that the Bank collected, used, disclosed and/or cross-border transferred of your personal data, for your privacy and security, the Bank may request you to verify personal identity before providing you with personal data as requested.

(2) Right to rectification of personal data, you may have the right to rectify your personal data that the Bank collected, used, disclosed and/or cross-border transferred of your personal data if such personal data is incomplete, incorrect, misleading or not up-to-date.

(3) Right to data portability of personal data, you may request the Bank to provide your personal data in electronic format with an explicit structure and to transfer such personal data to other data controllers, whereby this data is (a) your personal data provided to the Bank, (b) the Bank collected, used, disclosed and/or overseas transferred of personal data with your consent or for compliance with the contract between the Bank and you.

(4) Right to object of personal data, you may have the right to object some types of the collection, use, disclosure and/or overseas transfer of personal data, such as objection to direct marketing purpose.

(5) Right to restriction on the use of personal data, you may have the right to restrict the use of your personal data in some cases.

(6) Right to withdraw consent, you may have the right to withdraw your consent at any time for purposes that you gave your consent to the Bank to collect, use, disclose and/or overseas transfer your personal data.

(7) Right to erasure of personal data, you may have the right to request the Bank to erase your personal data or anonymize your personal data, however there is an exemption for the Bank not to take such actions if the Bank must retain such personal data in order to comply with the laws or to lawfully establish legal claims or to lawfully exercise legal claims or to lawfully defend against legal claims.

(8) Right to complaint, you may have the right to complain to the relevant authorities if you believe that the collection, use, disclosure and/or overseas transfer of your personal data was unlawful or violated the law on personal data protection.

If you want to use any right specified in this section, you can do so done by contacting the contact channels specified in "Contact the Bank" section. Request for using any right above may be restricted by the relevant laws, in some cases, the Bank can appropriately and rightfully reject your request, such as when the Bank must comply with the laws or court orders.



If you believe that the collection, use, disclosure and/or overseas transfer of your personal data by the Bank violated personal data protection laws, you have the right to make a complaint to the relevant authorities with respect to personal data protection. However, you may initially inform the Bank of your concern in order for the Bank to consider solving your concern, please contact the Bank through the channels provided in this Privacy Policy.

7. Changes to Privacy Policy

The Bank may make any change to this Privacy Policy from time to time if there is any change in the Bank's practice guidelines on personal data protection due to various possible reasons, e.g., technological or legal change. Changes to this Privacy Policy shall be effective when the Bank publishes on <https://www.krungthai.com>. However, if such change significantly affects your personal data, the Bank will notify you in advance regarding such change prior to the effectiveness.

8. Contact the Bank

If you have any inquiry regarding this Privacy Policy, please contact the Bank or the Bank's personal data protection officer as detailed below:

(1) Krung Thai Bank Public Company Limited

- 35 Sukhumvit Road, Klong Toey Nua Subdistrict, Wattana District Bangkok 10110, Thailand
- Krungthai Contact Center : Telephone number: 02-111-1111
- <https://krungthai.com>

(2) Data Protection Officer (DPO)

Data Protection Department

- 35 Sukhumvit Road, Klong Toey Nua Subdistrict, Wattana District Bangkok 10110, Thailand
- Email: dpo.official@krungthai.com