

Privacy Policy for Business Partner

Krung Thai Bank Public Company Limited (the " Bank" or " KTB" or " Krungthai") recognizes the importance of protecting personal data of the data subjects. This Privacy Policy (" Privacy Policy") is provided to describe means which the Bank use in collection, use, 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 personal information that the Bank may collect, use, disclose and/ or cross- border transfer according to Privacy Policy shall be the personal data of individuals who have the connection with the Bank's Business Partners in procurement of goods and/ or services (such as vendors, sales representatives, third- party service providers) (collectively called " Business Partners") , such as corporate representatives, individual shareholders, contact persons, attorney- in- fact, employees, officers, personnel and similar persons of Business Partners (collectively called "you").

This Privacy Policy shall apply to the collection, use, disclosure and/ or cross- border transfer of your personal data. The Bank may collect such personal data through various channels, such as collecting personal data directly from you (e.g. when you, on behalf of the Bank's business partner, offers goods or services to the Bank, including by signing contracts. filling out forms. when you interact with the Bank which includes interacting through the Bank's online platform, website, mobile application, email, telephone, questionnaire, business card, postal mail, during meeting and event, or when the Bank's representative goes visit you), from Business Partners that you work for, act on behalf of, or represent the affiliates or third parties such as other Business Partners of the Bank, from system resources, the Bank's central drive system or transport software systems and/ or electronic files or other communication channels which the Bank use to collect your personal data. However, please read this Privacy Policy together with the terms and conditions of the agreements, contracts and/ or other documents relating to the business relationship between the Bank and its Business Partners, which might be set separately with respect to 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 information relating to an identified or identifiable natural person, directly or indirectly (but not including the information of the deceased person) as follows;

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.

The Bank may collect your personal data. The personal data that the Bank may collect shall depend on your current business relationship with the Bank or the business relationship that might occur in the future between the Bank and you or the Business Partner that you work for, act on behalf of, or represent. The details are as follows;

1) Personal information, such as title, first name, last name, age, gender, photo, video, closed-circuit television cameras (CCTV, geographic coordinates, date of birth, nationality, marital status, financial status (such as financial certificate, credit information, source of income, fixed assets and liabilities) information on the documents issued by government agencies (e.g., ID card, passport, work permit, taxpayer identification number, driver's license number, house registration number, work guarantee (e.g. cash, cashier's check), vehicle information (e.g. chassis number, vehicle registration number), signature (including electronic signature), partner identification number (including type of partner), bank account and payment information (e.g. account holder name, bank account, account type and bank account number, beneficiary account name, payment date, payment method, payment currency and payment account, details of remittances within/ outside of Thailand), other personally identifiable information (e.g. LINE ID, and your land information (e.g. Land Title Deeds).

2) Educational information, such as educational background, educational degree, other qualifications.

3) Work information, such as occupation, position, job description, types of business, types of organization, a period of employment, workplace, information in a job application, resume.

4) Contact information, such as telephone number, mobile number, fax number, address, email, and other similar information.

5) Other information that the Bank collects, uses or discloses in connection with the Bank's relationship with its Business Partners, such as information you provide to the Bank in form of contract, forms or surveys, list of board of directors; list of shareholders, power of attorney, terms of reference (TOR), computer record data.

6) Sensitive Data, such as sensitive information obtained from the identification card (e.g. religion). The Bank shall 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 Personal data of the third party

If you provide the Bank with personal data of third parties such as an information which can identify your spouse or child, an information of the Bank employees related to you, and any other person that you have relationship with respect to your relationship with the Bank. Please inform this Privacy Policy to such third parties for acknowledgement and request for consent if necessary or legal basis for disclosure of personal data of third parties to the Bank.

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

The Bank may use your sensitive personal data as appeared on identification documents (such as religion) only for the purpose of identification and verification.

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 the customer contact channels specified in Clause 8 or as specified by the Bank. The withdrawal of consent will not affect the collection, use and disclosure 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, and/or disclose of your personal data by lawful basis on the legal basis of legitimate interest, the performance of a contract, legal obligation or other legal basis under personal data protection laws, as the case may be, depending on the relationship between you and the Bank, for the following purposes;

(1) For communication such as any communication in connection with product and service, project of the Bank or Business Partners, e.g. submitting documents, answering questions, responding to requests or reporting on progress.

(2) For the selection of Business Partners such as the assessment of your suitability and qualification and Business Partners', your identification and verification and Business Partners status, due diligence or other forms of background checks or risk assessments for you and Business Partners (including checking with law enforcement agencies for publicly available information and/or information on the blacklist) request for bid issuance and bidding, entering into a contract with you or Business Partners, assessment for your management and Business Partners.

(3) For data management of Business Partners such as a creating business partner account, recording data into the system, maintaining and updating business partner lists/ directories (including your personal data), collecting and managing contracts and related documents that may contain your name.

(4) For management of relationship with you such as plan, execution, management of relationship and rights (contractual) with Business Partners, e.g. appointing, terminating or authorizing Business Partners to carry out transactions, procurement, payment processing, account-related activities, audit, invoice issuance and money collection, arrangement of transportation and delivery, support services.

(5) For business analysis and improvement such as research, data analysis, assessment, survey, and report on product and service of Business Partners as well as and your performance or Business Partners.

(6) For system management and information technology support such as Information technology support and helpdesk, access management for any system to which the Bank has granted access rights to customers, deletion of inactive accounts, implementation of business control measures to enable business operations and to identify and solve problems in the

Bank's information technology system, as well as to maintain security in the Bank's system, develop, deploy, operate and maintain information technology systems.

(7) For monitoring security and system such as authentication and role-based access control in respect to monitoring and maintenance of the systems, equipment, and internet, information technology security, prevention and solution of crime, including risk management and fraud prevention, accident report.

(8) For dispute resolution management such as dispute resolution, contract enforcement, legal claims, including establishment, exercise, or defense of legal claims, and power of attorney.

(9) For management and communication between internal departments in the organization such as hosting public relations activities within the organization and complying with the appropriate business requirements, including but not limited to procurement, disbursement, internal management, training, auditing, reporting, delivering or managing documents, data processing, controlling or managing risk, analyzing and planning statistics, trends and other similar or related activities.

(10) For compliance with laws such as compliance with laws, legal procedures or orders of government agencies, including orders of government agencies outside Thailand and/or in cooperation with courts, authorities, government authorities, and law enforcement agencies, when the Bank has a reason to believe that the laws enforce the Bank to do so. Suppose that it is necessary to disclose personal data in compliance with laws, procedures, or government orders in order to comply with regulations, rules, and guidelines (e.g. obtaining a license to operate a business as required by law) , including coordination and communication with relevant government agencies, courts or relevant institutions (such as the Revenue Department, the Royal Thai Police and the Office of the Auditor General) , including investigation, complaints and/or crime or fraud prevention.

(11) For prevention or stopping of dangers to lives, bodies or health of persons

(12) For corporate social and environmental responsibility

In this respect, if you do not provide personal data to the Bank, it may have an impact on you, such as the Bank may not proceed with your Business Partner's or your request. Business Partner or you may experience some inconvenience or do not obtain the performance under contracts, and you or your Business Partner may receive damage or lose opportunities. In addition, the refusal to provide personal

data may affect the compliance with any law that the Bank or Business Partner or you must comply with and it may have related penalties.

3. The party that the Bank may 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 within Thailand or overseas; 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, to the Bank's financial business groups and the Bank's affiliates. The disclosure of your personal data to such financial business groups and affiliates will enable other companies to use your consent obtained by the Bank.

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. The Bank may share your personal data to the outsourcing parties or the service providers including but not limited to (1) internet and software service providers, website and digital media developers, information technology service providers and the information technology support service providers, (2) logistics and transportation service providers, (3) payment and payment system service providers, (4) research service providers, (5) analytics service providers, (6) survey service providers, (7) auditors, (8) customers services hotlines, (9) marketing, advertising, design, creative and communication service providers, (10) event, campaign, marketing and customer relationship management service providers, (11) telecommunications service providers, (12) administrative service providers, (13) cloud storage service providers, (14) printing service providers, (15) 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, (16) document storage and/or disposal service providers and (17) debt collection 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 when necessary. The Bank will ensure that the service

providers must protect the security of your personal data in compliance with the laws.

3.3 The Bank's business alliances

The Bank may transfer your personal data to the Bank's business alliances 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 card issuers, companies that provide printing services, credit card companies, companies that provide payment services for products and services, analytics service providers, market analysis service providers and financial transaction service providers, and other service providers that support the bank's business operations

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 Office of the Auditor General of Thailand, the Revenue Department 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.

In this regard, the Bank may have to disclose your personal data to the Office of Insurance Commission for supervision and promotion of insurance business under the law of the Insurance Commission, including the law on life insurance and non-life insurance according to the Privacy Policy of the Office at <https://www.oic.or.th>

3.5 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. In this respect, the Bank shall procure that such third parties comply at all times with this Privacy Policy when there is a collection, use, or disclosure and/or cross-border transfer of your personal data.

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 servers located outside Thailand for information technology support.

When the Bank has to transfer your personal data to other countries which have 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 permit the cross-border transfer of personal data, e.g., the Bank may have to obtain a confirmation in the term of contract from third parties who have access to such personal data that your personal data shall be protected under the same standard level of the personal data protection in Thailand.

5. Duration of the personal data storage period

The Bank shall retain your personal data for a necessary period of time to comply with the purposes stated in this Privacy Policy. In this respect, to comply with the laws, the Bank may have to retain your personal data as long as laws require.

6. Your rights as the Data Subject

Rights stated in this section mean the legal rights relating to your personal data whereby you may exercise these rights with persons required by law under the conditions stipulated by law and the process of the rights management of the Bank, such rights are set as follows;

(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. In order that protect your privacy and security, the Bank may request you to verify your 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 cross-border 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 to some types of the collection, use, disclosure and/or cross-border 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 cross-border 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 action if the Bank must retain such personal to comply with the laws, establish legal claims lawfully, exercise legal claims lawfully, or defend against legal claims lawfully.

(8) Right to complain, you may have the right to complain to the relevant authorities if you believe that the collection, use, disclosure and/or cross-border 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 contact the Bank through the customer contact channels specified in the “Contact Bank” section. The relevant laws may restrict the request for using any right above; in some cases, the Bank can appropriately and rightfully reject your requests, such as when the Bank must comply with the laws or court orders. If you believe that the collection, use, disclosure and/or cross-border transfer of your personal data by the Bank violated personal data protection laws, you have the right to complain to the relevant authorities concerning personal data protection. However, you may initially inform the Bank of your concern in order for the Bank to solve your concern; please contact the Bank through the channels provided in this Privacy Policy.

7. Changes to Privacy Policy

The Bank may make change to this Privacy Policy occasionally, 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. If there is any change made to this Privacy Policy, changes 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 its effectiveness.

8. Contact the Bank

If you have any inquiries 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