ธนาคารกสิกรไทย
开泰银行 KASIKORNBANK

Personal Data Protection Policy

KBank places importance on personal data protection. KBank therefore has established relevant policies and procedures to ensure that our operations comply with relevant laws and regulatory requirements as follows:

1. **Obtaining Consent from Data Subject:** KBank requires consent to be obtained for the collection, use, or disclosure of personal data in accordance with legal requirements. The purpose of data processing must be clearly communicated, while respecting the data subject's autonomy in granting such consent.

2. **Collection and Deletion of Personal Data:** KBank shall collect personal data lawfully and inform data subjects, prior to or at the time of collection, of the relevant details. KBank also maintains records of processing activities as required by law and ensures that personal data is deleted, destroyed, or anonymized once retention periods expire or when it is no longer necessary for the stated purposes, in accordance with legal requirements.

3. **Access and Use of Personal Data:** KBank limits access to and use of personal data to what is necessary for job performance and in accordance with the access rights defined by KBank.

4. **Disclosure and Receipt of Personal Data:** KBank requires that the disclosure of personal data to third parties, as well as the receipt of personal data from third parties, must be based on the data subject's consent or on a legitimate legal basis.

   For disclosures of personal data to third parties engaged by the Bank to act as data processors on behalf of or under the instructions of the Bank – such as service providers, suppliers, or contractors – the Bank exercises oversight to ensure compliance with the Personal Data Protection Law and KBank's internal policies. This is achieved through a **Data Processing Agreement**, which requires that:

   - Personal data is processed strictly for the purposes defined by KBank.
   - The confidentiality of personal data is strictly maintained.
   - Access to personal data is restricted to authorized personnel only.
   - Appropriate security measures defined by KBank are implemented.
   - Upon contract termination, personal data must be deleted or returned to KBank, with supporting evidence of deletion.
   - Any data breach must be reported to the Bank within the specified timeframe.
   - Cooperation must be provided for investigations and root cause analyses of data breaches.

   In addition, when disclosing personal data to **business partners** or **companies within KBank's financial conglomerate**, KBank ensures proper governance through a **Data Sharing Agreement** which requires that the recipients process the data solely for the agreed purposes and comply with the Personal Data Protection Act.

5. **Transfer of Personal Data to Other Countries:** Personal data may only be transferred to foreign countries or international organizations where appropriate data protection standards are in place and enforceable, or where transfers are made within the Bank's financial group under Binding Corporate Rules (BCRs) approved by the Personal Data Protection

Committee. Transfers under legal exceptions or with appropriate safeguards ensuring enforceable data subject rights and effective legal remedies are also permitted, in compliance with applicable legal requirements.

6. **Security of Personal Data:** Appropriate security measures that are in line with standards prescribed by relevant laws shall be implemented, and they must be reviewed when necessary or there is any technological change to ensure that KBank's security measures are continuously effective.

7. **Rights of Data Subject:** The data subjects can exercise their rights according to PDPA via channels informed in KBank's Personal Data Protection Policy Notice for Customers.

8. **Responsibilities as a Data Controller:** KBank must maintain security measures at a level not lower than the minimum legal standards and review them as needed. When disclosing personal data, KBank takes steps to prevent unauthorized use or disclosure and implements systems for deleting or destroying personal data when retention periods expire or when it is no longer necessary. Data breaches are reported in accordance with legal requirements

9. **Responsibilities as a Data Processor**: When acting as a data processor, KBank collects, uses, or discloses personal data only in accordance with the data controller's instructions, implements appropriate security measures, notifies the data controller of any data breach, and maintains records of processing activities as required by law.

10. **Data Protection Officer (DPO):** KBank appoints a Data Protection Officer who is responsible for duties as specified under applicable data protection laws.

11. **Personal Data Breach:** The breach of personal data shall be reported to the Office of the Personal Data Protection Committee within 72 hours after having become aware of it. If the breach is likely to result in high risk to the rights and freedoms of the data subjects, KBank will notify the data subjects of the breach and remedial measures.

12. **Training:** All employees are required to undergo adequate training on personal data protection to ensure awareness and proper compliance with relevant laws and regulations.