Guidelines for Personal Data Protection

KASIKORNBANK PCL.

KASIKORNBANK PCL. ("KBank") recognizes the importance of personal data protection and prioritizes compliance with laws and regulations related to personal data protection and other relevant regulatory requirements as per the following personal data protection guidelines.

1. Personal data must be lawfully processed with fairness and transparency.
2. The collection of personal data shall be limited to what is relevant and necessary for the processing of personal data for lawful purposes; personal data shall not be further processed in the manner that does not correspond to those purposes.
3. In processing personal data, from the process of collection, to use and disclosure, it shall be carried out only to the extent that is necessary, relevant, and limited to the purposes of personal data processing, and the data subject shall be notified of the purposes of data collection, use and disclosure.
4. Personal data which is collected, used, or disclosed must be accurate, complete, and up-to-date.
5. Personal data shall not be retained beyond the appropriate period necessary to achieve the purposes of personal data processing or kept beyond the period prescribed by law. There shall be a process for auditing and deleting or destroying personal data when its retention period has expired.
6. Personal data security measures, including appropriate organizational and technical measures, possibly including necessary physical measures, must be in place to prevent unlawful processing of personal data.

Personal data processing

KBank processes customers' personal data according to the purposes stated in the Bank's personal data protection policy announcement under lawful bases for processing personal data.

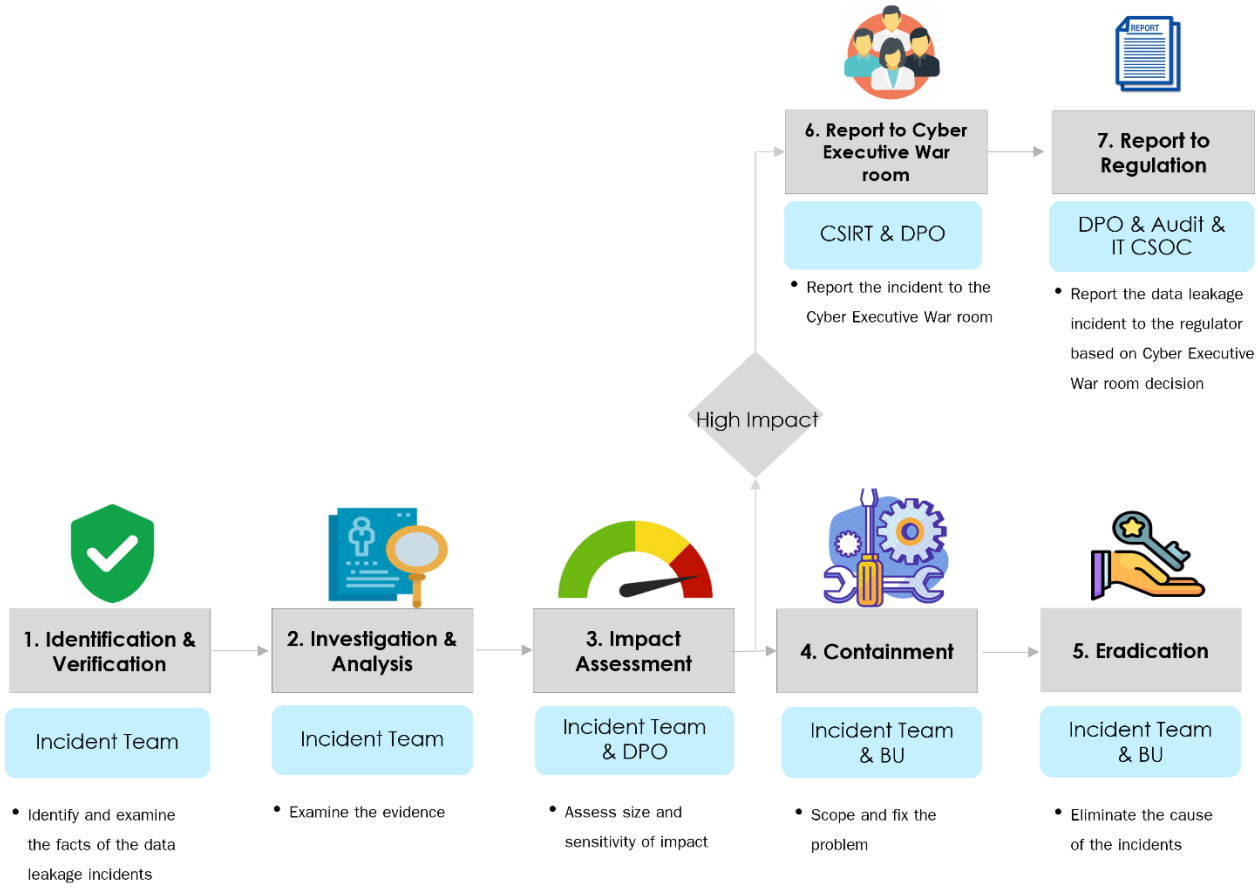
KBank may process customers' personal data for purposes other than delivering the products and services that the customers have applied for, such as analyzing and researching, compiling statistical data, and developing and improving the Bank's products and/or services, as well as marketing activities based on consent. In the event that KBank processes personal data based on legitimate interest, such as processing data for risk management, supervision, audit, internal management, fraud prevention, and IT risk management in order to prevent, manage and mitigate IT risk and cyber threats, KBank shall conduct a three-part test to assess the necessity and proportionality before processing personal data.

In 2023, KBank used customer data for marketing purposes, with consent given by our customers. Data usage proportion represented 70.80 percent of all retail customers.

Data Breach Incident Management (OR)

KBank has established response and report processes for unauthorized or illegal transmission of data (data leakage), which cover loss of, access to, use of, change/amendment to or disclosure of personal data. If KBank has been notified of or found data leakage incidents, KBank shall examine the facts, analyze and assess those incidents, plus related risks and impacts in accordance with internal regulations that have been established by KBank, such as the number of affected owners of personal data, plus volume and sensitivity of personal data. Such incidents and risk assessment results shall be reported to the responsible committees for consideration in establishing recovery, response and relief guidelines, as well as the relevant government agencies in accordance with the laws as the case may be.

If personal data breaches, non-compliance with Personal Data Protection Policy, which is regarded as violation of directives and/or operational procedures of KBank are detected and it is found that there is wrongdoing after and investigation has been completely conducted, KBank may take disciplinary action, such as warning, probation, compensation, wage deduction, demotion and/or salary cut or employment termination, as deemed appropriate.



DPO: Data Protection Officer
CSOC: Cyber Security Operation Center
CSIRT: Computer Security Incident Response Team

Third party verification on personal data protection

KBank has also attached importance to checks and balances in key operations and set out security requirements in all system development processes, from service user screening, solution designs, and operating system development and testing, to system implementation. In 2021, the results of an assessment conducted by a leading consulting firm of our Cyber Risk Maturity, based on the standards of the National Institute of Standards and Technology (NIST*), were on par with those of other leading banks, and KBank has established a continued development plan to achieve Cyber Risk Maturity that is equal to that of world-class banks within 2024. Moreover, KBank has been certified ISO 27001:2013 since 2014, covering important services and applications, Datacenter and Cyber Security Operation Center (CSOC).

**The National Institute of Standards and Technology (NIST) is the United States' agency that determines standards and guidelines of cyber security, which have been globally accepted and are widely used as a reference.*

Internal audit on privacy protection

KBank's internal audit department conducts audit of compliance with the Personal Data Protection Act based on risk-based assessment. The audit scopes include KBank's governance and operational processes related to the data life cycle and data security measures. The audit result was reported to the Audit Committee.