PERSONAL DATA PROTECTION POLICY

Objectives of the Personal Data Protection System

The objective of the Personal Data Protection System is ensuring the establishment and implementation by the Bank of its own standards in the management of personal data; identification and support of organizational targets and obligations; establishment of control mechanisms in line with the Bank's acceptable risk level; fulfillment of the Bank's obligations under international law in the field of protection of personal data, the Constitution, laws, contracts and professional rules, and the protection of the interests of individuals in the best way.

The Bank complies with the legislation on the protection of personal data and data protection principles. The data protection principles adopted by the Bank are as follows:

a. To process personal data only if it is clearly necessary for legitimate corporate purposes,
b. To process the personal data on the minimum scale necessary for these purposes and avoid processing data more than what is required,
c. To provide individuals with clear information about who used personal data and how they were used,
d. To process only relevant and appropriate personal data,
e. To process personal data in accordance with fairness and the law,
f. To keep a personal data inventory as stated in the legislation,
g. To set up mechanisms to ensure that personal data inventory is accurate and up-to-date,
h. To retain personal data in compliance with the terms determined under the methodology indicated in the "Retention and Disposal Policy",
i. To create the policy on the retention and disposal of personal data, structure the processes in line with this policy, and ensure that the policy is reflected in the practice,
j. To be respectful of the individuals' rights relating to personal data, including the right to access,
k. To ensure the safety of all personal data,
l. To transfer personal data (customer information / employee information) abroad in accordance with the article 4.8. only if sufficient protection exists,
m. To transfer data abroad only to safe countries determined by the PDP Agency or, in the absence of adequate protection, in the event that data officers in Turkey and the relevant foreign countries pledge an adequate protection in writing and if allowed by the Agency and the BRSA regulations are not violated,
n. To implement the exceptions allowed under the legislation,
o. To establish and implement a personal data protection system for the implementation of the policy,
p. To determine, when necessary, the internal and external stakeholders who are part of the personal data protection system and the extent to which they are involved in the Bank's personal data protection system,
q. To identify the staff with special powers and responsibilities related to the system of personal data protection.

Notification and Access

The Bank shall notify the Personal Data Protection Board ("PDP Board") in case it is the data officer and if information is requested on what personal data categories it has processed in this capacity. The bank identifies all personal data categories it processes in the personal data inventory.

Notification is made in accordance with the procedure and method to be established by the PDP Board and a copy of the notification is kept by the Bank's Personal Data Protection Committee (PDP Committee).

The notifications are repeated periodically if deemed necessary by the relevant legislation or the PDP Board.

The Information Security Management Committee reviews the Bank's data processing activities and amendments thereto annually to identify potential changes that may occur in the reporting made to the PDP Board and informs the LPPD Board if necessary.

This policy covers all units of the Bank, employees of the firms providing support services, trainees and contracted staff. Any action that violates the LPPD or this policy will be subject to the Bank's disciplinary rules and, if the violation in question constitutes a crime or a misdemeanor, the situation is notified to the relevant authorities as soon as possible.

Solution partners of the Bank that have access or are likely to have access to the personal data and all third parties working with the Bank are invited to read and abide by this policy. No third party may have access to personal data processed by the Bank without conclusion of a written confidentiality agreement which has at least as strong standards as the Bank does with regard to the protection of personal data and which includes the obligations and the right to audit by the Bank relating thereto.

Risk Assessment

The purpose of the risk assessment is to be aware of the risks associated with the Bank's processing of certain types of personal data.

The Bank establishes methods to assess the risks that the processing of personal data may create for the individuals. This assessment is performed by also taking into account the third parties that process the data on behalf of the Bank. The Bank manages the risks identified as a result of the assessment in a way that they do not create conflicts with this policy.

If a particular type of data processing activity is likely to pose a high risk to individual rights and freedoms in line with its structure, context and purpose, the unit related to the activity performs an impact analysis prior to the Bank's data processing activity by getting the approval of the Risk Management and manages the potential risks. A single assessment may be relied upon for multiple data processing activities containing similar risks.

If it is found at the end of the impact analysis that the Bank is about to start a data-processing activity that may create a high risk over the personal rights and freedoms, the ISM Committee approval on this issue is sought. The ISM Committee receives opinion from the PDP Board if it deems necessary.

In risk management, the systems and controls applied pursuant to the Operational Risk Procedure which the Bank has already adopted pursuant to the Information Security Policy are implemented.

Data Protection Principles

It is essential that all personal data processing activities are carried out in accordance with the following data protection principles. The Bank's policies and procedures aim at ensuring compliance with these principles:

- Compliance with the law and rules of honesty.
- Accurate and up-to-date when needed.
- Processing for specific, clear and legitimate purposes.
- Being connected with the purpose they are processed for, limited and measured.
- Retention for the time required for the purpose prescribed in the relevant legislation or for which they are processed.

Personal data are processed in accordance with the law and rule of honesty and in a transparent manner.
In this respect, the Bank includes confidentiality notices in data collection channels and related forms regarding the personal data processing activities performed by the Bank. The ISM Committee determines the areas where these notices, in which clear and understandable information is contained about which data about whom are processed by the Bank for which purposes, will be included and announced. These notices include the following::

- Identity and contact information of the Bank as the data officer,
- The ISM Committee and contact information,
- Types of personal data that are processed (Personal Data or Private Personal Data),
- Data types that are considered as personal data are sorted as printed and electronic data,
- Purposes of processing personal data,
- Retention time stipulated for personal data,
- Data owner's rights,
- Third parties the data may be shared with.

Personal data can only be processed for specific, clear and legitimate purposes.
The reasons/purposes for the processing of personal data are determined in the personal data inventory and the personal data cannot be used for purposes other than the stated purpose without any other legal justification or explicit consent of the data owner.

In the event of the occurrence of the conditions that require the use of personal data for purposes other than those specified in the personal data inventory, this situation is communicated to the ISM Committee by the relevant staff/unit. The ISM Committee checks the suitability of the new objective and, if necessary, ensures that the data owner is informed of the new objective and of the new data-processing activity.

The activity of processing of personal data must be carried out in a manner that is suitable for its purpose, relevant, and limited.

The ISM Committee is obliged to ensure that no personal data that are not explicitly required for the purposes of processing are collected and processed.

The approval of the ISM Committee is sought for a new personal data processing process other than those specified in the inventory.

The ISM Committee audits that the processed data are appropriate and relevant, based on the personal data inventory, which is reviewed at least every six months.

The ISM Committee checks that all data processing methods are appropriate and relevant through the internal audit/external audit that it will perform/get performed on an annual basis.

The ISM Committee is responsible, in respect of personal data which it has found to be inappropriate or not relevant or more than it was required for the purpose of processing, for stopping the data processing activity and ensuring that the data that have been processed are processed in accordance with the retention and disposal policy by taking account the provisions of the legislation that may be relevant.

Personal data must be accurate and up-to-date.
The Human Resources and Administrative Affairs Unit is responsible for creating an awareness as to the collection and retention of all staff data in an accurate and up-to-date manner and for coordinating training activities.

The correctness and timeliness of the data that are kept relating to the staff are the responsibility of the relevant personnel.

Employees/customers and other relevant persons must inform the Bank of the updating of the personal data that are processed. It is the responsibility of the relevant unit to correct/update the record in question upon delivery of such a notification and to update the changes in data categories through the data inventory.

The ISM Committee may instruct the relevant unit for a review of the accuracy or timeliness of certain data through an assessment it would make over the data inventory as to the type, storage period, and amount of the processed data, also taking into account the provisions of the legislation that may be relevant.

1. Personal data should be processed in a way that the person concerned may be identified only if it is necessary for data processing purposes.

1.1 In the event that personal data are retained beyond the required term due to requirements such as backup, etc., it is essential that personal data be processed in accordance with the Retention and Disposal Policy in order to protect the rights and freedoms of individuals in case of data security weaknesses. Where necessary, the approval of the ISM Committee is obtained.

1.2 The processing of personal data after the periods that have been specified is subject to the written approval of the ISM Committee.

Data Owners' Rights

The data owners have the following rights as to the data processing activities and records about them at the Bank:

- To know whether his/her personal data were processed,
- If his/her personal data have been processed, requesting information about it,
- To know the purpose of processing personal data and whether they have been used in a way that was appropriate for their purpose,
- Requesting to know the domestic or foreign third parties to which personal data were transmitted,
- In the event that personal data have been processed incompletely or incorrectly, requesting correction thereof,

- Requesting the deletion or removal of personal data for which there was no legitimate justification or basis for processing under LPPD or this policy,
- Requesting the notification of the correction or deletion actions taken upon his/her request to the third parties to which personal data were transferred,
- Objecting to the emergence of a consequence against the person himself/herself due to the analysis of the processed data exclusively through automated systems,
- Demanding that the damage be eliminated in the event that he/she suffered damage due to the unlawful processing of personal data.

Data owners may request access to their personal data and exercise the rights mentioned above. These requests are forwarded to the 'Liaison Officer'. The ISM Committee, informed by the Liaison Officer, ensures that the necessary actions are performed within 30 days at the latest. All kinds of communication with the data owners are provided through the Liaison Officer.
The processes of receiving, transmitting and finalizing requests are carried out under the rules that have been defined for data owner's access.
The data owners' right to access the ISM Committee and the contact information of the Committee is included in the privacy statements and on the website of the Bank so that data owners can direct their requests.
Regardless of the job description, all employees of the Bank are obliged to forward to the Legal and Legislative Unit the access requests by the data owners and the Legal and Legislative Unit is obliged to submit these requests to the ISM Committee as soon as possible. The Bank's staff should be informed and trained by the ISM Committee on how they should act as to the requests that would be made by data owners.

Obtaining Explicit Consent

The consent which is based on information and expressed by free will through written/oral declaration or clear confirming action that reveals the willingness to have personal data to be processed is considered by the Bank as the explicit consent by the data owner for specific data processing activities. Explicit consent for sensitive data is always obtained in writing. Explicit consent can always be withdrawn by the data owner.

An explicit consent may be obtained by getting the template for explicit consent form signed by the data owner or through an agreement to be concluded with the data owner or by including in the electronic form the elements contained in this template. Explicit consent with respect to the personal data routinely processed relating to the employees, prospective employees, and customers is obtained through the relevant standard agreements or forms.

In the event that the data processing activity based on explicit data is to be continuous or repeated, a record of the persons with explicit consent given is kept in a single list by the unit concerned. The timeliness and the accuracy of these records are the responsibility of the relevant unit. Explicit consent forms or other relevant means of proofing for data processing activity based on explicit consent are kept by the relevant unit.

Data Security

The staff is obliged to ensure that the data processed by the Bank and held under their responsibility are kept secure and not disclosed to any third party unless a confidentiality agreement is signed.

Personal data are accessible only by those who need access to them. Access is provided in accordance with established rules.

Data security is provided in accordance with the Bank's Information Security Policy and related documents.

As a statutory obligation, the information security events concerning personal data are notified by the ISM Committee to the PDP Board and the person concerned as soon as possible.

Data Sharing

1. Personal data may only be shared with third parties in accordance with law and fairness. Accordingly, the existence of one of the following conditions is sought in order for personal data to be shared:
    - An explicit consent received from the data owner.
    - Explicit prescription by law.
    - It must be mandatory to protect the life or bodily integrity of someone else or the person himself/herself who is unable to express his/her consent due to actual impossibility or whose consent is not legally valid.
    - If the processing of personal data belonging to the parties to the agreement is required, provided that it is directly related to the conclusion or performance of an agreement to which the Bank is or will be a party.
    - If it is compulsory for the bank to fulfill its legal obligation.
    - If already publicized by the relevant person himself/herself.
    - Data processing is mandatory for the establishment, exercise or protection of the Bank's rights.
    - Data processing is mandatory for the Bank's legitimate interests, provided that it does not damage the fundamental rights and freedoms of the person concerned.
2. Personal data may only be transferred abroad provided that the above conditions are met, there is adequate protection in the target country, and the data owner's explicit consent is obtained about this transfer.

When transferring personal data abroad, the list of countries with sufficient protection established by the PDP Board is taken into account.

In the case of the transfer of personal data abroad, the ISM Committee provides the necessary permits and notifications to the PDP Board pursuant to the LPPD and related legislation.

3. All transactions relating to the sharing of personal data must be recorded in writing together with their justifications. These records are audited at specific periods by the ISM Committee.

4. In the case of a regular data-sharing relationship without a legal basis or legal obligation, a data-sharing agreement is set up with the party concerned that specifies the conditions for data sharing. The data-sharing agreement includes, at a minimum, the following:
    - Purpose or purposes of sharing;
    - Potential third-party recipients or recipient types and conditions of access right;
    - Data to be shared (they should be kept at a minimum level for your purposes);
    - General principles concerning the processing of data;

- Data security measures are assessed according to the information assets confidentiality class. Confidentiality classes of information assets are Confidential, Limited Access, Agency-specific, and Public;
- Retention period of shared data;
- Data owner's rights, access requests, procedures for responding to applications and complaints;
- Review of termination of the enforcement of the sharing agreement
- Liability and sanctions for non-compliance with the agreement or individual breach by the staff
- Data-sharing agreements are submitted to the ISM Committee for approval after the approval of the Legal and Legislative Unit.

Management of Records

Personal data cannot be kept longer than necessary for the purposes of processing. Classification of the records containing personal data and their retention periods are determined pursuant to the Asset Identification and Classification Procedure that has been prepared in accordance with the relevant legislation.

Personal data with the time required for processing purposes already expired or that can be destroyed under the legitimate request of the data owner is anonymized, deleted or destroyed in accordance with the Retention and Disposal Policy.

Audit

PDP audits are carried out by the Internal Audit or a third-party firm within the company. The internal and external audit results are reviewed by the ISM Committee periodically at evaluation meetings.