Personal Data Protection Policy

Date / Rev. No.: 29.11.2018 / R01

Türkiye Finans

Participating in life

TABLE OF CONTENTS

1. INTRODUCTION

At Türkiye Finans, we deem confidentiality and privacy of personal data among our most important priorities. While our Bank undertakes to abide by the personal data protection regulations as part of its legal and social responsibilities, it deems personal data protection as one of the pillars of establishing trustworthy business relations and of maintaining its credibility before the public. While our Bank shows utmost sensitivity towards full compliance with the Law on the Protection of Personal Data and the sub-regulations thereof, all our employees assume responsibility in taking and implementing any and all measures necessary in this respect.

2. PURPOSE AND SCOPE

The objective of the Personal Data Protection Policy ("Policy") is to ensure full compliance with the obligations arising from the regulations regarding personal data protection, determining the operational rules and responsibilities within the Bank, and raising the awareness of the Bank's employees in this respect. Another purpose of preparing this Policy is to define the processes of erasure, destruction or anonymization by the Bank (Data Controller) of personal data kept at the Bank when the causes that require the processing of personal data cease to exist, and to ensure that the period required for the storage of personal data of natural persons kept at the Bank does not exceed the period required for the processing thereof, and that appropriate security controls corresponding to the data class have been constituted and maintained throughout the storage of data.
The Personal Data Protection Policy also represents our Bank's "Data Storage and Destruction Policy" within the frame of the Regulation on the Erasure, Destruction or Anonymization of Personal Data. The Personal Data Protection Policy constitutes an integral part of the Information Security Policy.

3. DEFINITIONS AND ABBREVIATIONS

The Bank / TFKB:

Türkiye Finans Katılım Bankası A.Ş.,

Top Management:

TFKB's Chief Executive Officer (CEO) and executives reporting directly to the CEO,

The Law:

Law No. 6698 on the Protection of Personal Data,

Personal Data:

All the information relating to an identified or identifiable natural person,

Data Subject:

The natural person whose personal data is processed, referred as "the data subject" under the Law,

Processing of Personal Data:

Any operation performed on personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means,

Data Controller:

The natural or legal person who is obliged to take any technical and administrative measure necessary to prevent illegal processing of / access to personal data, and to store data under appropriate level of security (for the purposes of this Policy, it refers to our Bank),

Personal Data Protection Management Section:

The section, which maintain the Bank-wide coordination and communication within the scope of the Law on the Protection of Personal Data and the sub-regulations thereof, follow up the already constituted processes and report,

Personal Data Coordination Officer:

The natural person who has been appointed to ensure the coordination of the actions taken and the management of the compliance process related to the Bank's obligations under the Law and secondary regulations to be issued based on the Law. (For the purposes of this Policy it refers to the Finance and Strategy EVP)

Data Protection Officer:

It refers to the real person who is assigned to execute the internal processes related to the PDP, manage/confirm the enterance and verification of data inventory into VERBIS. (For the purposes of this Policy it refers to the Customer Analytics and BI VP)

Contact Person:

Refers to the person who is assigned to be contacted for communication with the Personal Data Protection Authority and who is responsible for the operation related to entering and updating of the data inventory into VERBIS.
(For the purposes of this Policy it refers to the PDP Management AVP)

Data Processor:

The third party natural person or legal entity who process personal data on behalf of the Data Controller and who perform the duties assigned to them by the Bank under law.

Data Controllers Registry Information System (VERBIS):

The information system accessible via internet, which has been created and managed by the Personal Data Protection Authority in order to be used by Data Controllers for applications to the registry, and for other processes related with the registry,

Explicit Consent:

A freely-given, specific and informed consent,

Anonymizing:

Rendering personal data impossible to link with an identified or identifiable person, even though matching them with other data,

Related User:

The persons who process the personal data within the Bank's organization, apart from the person / unit responsible for storing, protecting, and backing-up personal data technically,

Recording Medium:

All kinds of media in which personal data processed completely / partially by automated means, or by an non-automated means which, in this case, should be part of a data registry system, are stored,

Personal Data Processing Inventory:

The inventory which is created by a Bank by correlating the Bank's personal data processing activities carried out as part of its business processes with personal data processing purposes, data categories, the recipient group , and data subject group, and which describes in detail the maximum period required for personal data processing purposes, the personal data required to be transferred to foreign countries, and the measures taken with respect to data protection,

Periodic Destruction:

The processes of erasing, destroying or anonymizing personal data to be performed directly in recurring intervals set out in the policy when all the conditions for processing personal data stipulated under the law cease to exist.

Board:

Personal Data Protection Board,

Authority:

Personal Data Protection Authority,

Data Categories:

The personal data class pertaining to the group(s) of data subjects, in which personal data are grouped by their common features,

ITTD:

IT Technology & Infrastructure Management Department;

EPGD:

Enterprise Project Delivery & Governance Department,

PSOD:

Payment Systems Operation Department,

TRID:

T.R. ID Number.

4. RESPONSIBLE PARTIES

Board of Directors

- Is responsible for formation of management, scope and framework of and regular review of the Personal Data Protection Policy.

Audit Committee

- Oversees compliance with regulations regarding the protection of personal data and the Bank's internal policies and implementation procedures within the scope of personal data protection.
- Provides the Board of Directors with assurance regarding adequacy and effectiveness of the management framework for the protection of personal data.

Top Management

- Is responsible for enforcement of the Personal Data Protection Policy across the Bank.
- They structure management levels and business processes within their responsibility in accordance with the regulations on the protection of personal data.
- With regards to the protection of personal data, they play an active role in ensuring that a culture and working environment is formed and maintained within the Bank.

Personal Data Coordination Officer

- The person ensures coordination of the actions taken at the point of compliance with the law and management of the compliance process.

Data Protection Officer:

- It refers to the real person who is assigned to confirm the data officer during entering data into VERBIS and responsible for the execution of the internal processes related to the PDP.

Contact Person:

- Refers to the person who is assigned to be contacted for communication with the Personal Data Protection Authority and who is responsible for the operation related to entering and updating of the data inventory into VERBIS.

Personal Data Protection Management Section

- Assures coordination and communication throughout the Bank within the scope of the Law on Personal Data Protection and the relevant legislation.
- Fulfills the obligations within the scope of Data Controllers' Register Information System, periodically updates Personal Data Processing Inventory, reports the registry and keep it up to date.
- Deals with the requests transmitted by the data subjects and the issues of data transmission and exchange, carries over to the relevant authorities and / or committees on the basis of the high-level decisions that need to be taken regarding the protection of personal data.
- Manages the processes of periodic destruction of personal data in coordination with the Head Office departments.

- Improves the compliance, accuracy and effectiveness of the personal data protection and management system and conducts studies on continuous improvement and corrective actions.
- Conducts the necessary analysis works in case the personal data are to be transferred to third parties for the purpose of constituting business relations such as support service, supplier / business partner / consultancy etc.
- Monitors and manages the process of fulfillment of explicit consent and disclosure obligations for data subjects.
- Conducts impact analysis studies on new product and service developments, determines the personal data to be processed and checks whether the personal data processing conditions sought under the Law.
- Establishes and maintains internal regulations on the protection of personal data through the participation of relevant departments.
- Informs employees regularly about the measures to be taken for the protection of personal data, and carries out training and awareness activities.
- Advises the Bank on the protection of personal data under the legislation.

PSOD-Customer Satisfaction Section

Records, examines, directs to the Personal Data Management Unit / Service, replies and reports applications filed within scope of the Law and related legislation by individuals whose personal data are stored by our Bank.

Bank Employees

- Shall not disclose personal data to others in breach of the provisions of the Law and other laws, and may not use such data for purposes other than the purpose of processing. This obligation survives the expiry of the employees' duty.

All the activities to be carried out, and all the measures to be taken Bank-wide within the frame of this policy are determined in compliance with the Bank's internal regulations according to the titles, units, and job descriptions of the parties taking part in the personal data storage and destruction processes..

5. PERSONAL DATA MANAGEMENT

5.1 Practice

The Bank's System comprises each of its personal data processing departments serving retail and corporate customers in the banking industry, all the suppliers to which the Bank transfers data, as well as all its employees, and he information security it uses for the protection of its Personal Data Processing Inventory.

5.2 Location Limits

a) Head Office

b) The Service Building where the Data Center is located

c) All regions and branches

5.3 Boundaries of the System

They comprise the systems containing the electronic or physical assets of the Bank in any and all systems where personal data processing activities are performed, or assisted. These include, without limitation:

- Main Banking Application (BYS)
- Ocean
- Humanist
- Inact
- Oracle
- Excel Documents
- Physical Documents
- Pega
- MI4Biz

5.4 Data Subject Categorization

The data subjects falling within the scope of application of the Policy in the frame of the personal data security system and the descriptions thereof are as follows:

Data Subject	*Categorization Description*
Employee Candidates	The natural persons who have applied for a job in TFKB, or those who have rendered their CVs and relevant details accessible to TFKB in any way
Intern Candidates	The natural persons who have applied for internship in TFKB, or those who have rendered their CVs and relevant details accessible to TFKB in any way
Resigned Personnel	The natural persons whose employment at TFKB has been terminated either by their free will, or by TFKB
Employees	All natural persons who work for TFKB either for a definite, or for an indefinite term of service
Customers / Potential Customers	The natural persons, whose personal data of whom have been received due to their business relationships within the scope of the activities performed by TFKB, irrespective of whether there is any contractual relationship or not,
Supplier	A natural person producers who supply TFKB with raw materials, products, etc. in order for the latter to offer a product or service, or a natural person acting as a representative of a legal entity whose personal data is processed by our Bank
Visitors / Guests	Natural persons who have entered in TFKB's physical premises (Head Office, The Service Building where the Data Center is located) for any purpose whatsoever, or those who have visited its websites
Third Persons	Including personal data are processed by guarantor, family members, etc. but not limited to other real persons

6. DATA COLLECTION FLOW AND PROCESSING

6.1 General Principles in the Processing of Personal Data

Our Bank processes the data in compliance with provisions stipulated under the Turkish Constitution, the Law on the Protection of Personal Data, the Banking Law No: 5411, and the applicable legislation it has to abide by within the scope of its operations.

It is mandatory to abide by the following principles in the processing of the personal data:

Compliance with Law and Honesty Rule

Our Bank, as a prudent merchant, acts in compliance with the principles laid down by the legal regulations, and with the general rule of trust and bona fides in the processing of personal data.

Accuracy and Being up to Date, Where Necessary

Our Bank keeps the personal data accurate and up-to-date in consideration of not only the other laws it has to abide by within the scope of its operations, but also the fundamental rights of the data subjects as laid down in the Law on the Protection of Personal Data, and its legitimate interests as well.

Being Processed for Specific, Explicit and Legitimate Purposes

Our Bank determines its legitimate and legal purpose of personal data processing clearly and definitively. In this respect, personal data that are processed are limited to the services being offered or to be offered, and also to the legal obligations. In this respect, the purpose for which the personal data are to be processed is revealed prior to starting to process personal data.

Being Relevant, Limited and Proportionate to the Processing Purposes

Our Bank processes personal data in a way to help attain the specified purposes, while avoiding the processing of any personal data not related with, or not needed for the attainment of the purpose. In this context, the processing of data is limited to operations and legal obligations.

Being retained for the Period of Time Stipulated by Relevant Legislation and for the Processing Purpose

Our Bank stores the personal data only for the period set forth in the relevant regulations it has to abide by, or for such period of time as is necessary for the purpose for which the data are processed.

6.2 Conditions for Processing Personal Data

Protection of personal data is a Constitutional right. Fundamental rights and freedoms may be restricted only by law and due to the causes stipulated in the respective articles of the Constitution without changing their essence. According to the Constitution, personal data may be processed only under such conditions prescribed by law, or with the explicit consent of the respective person. In this respect, our Bank processes the personal data only under the conditions prescribed by law, or with the explicit

consent of the respective person, in accordance with the Constitution. The giving of an explicit consent by the data subject is only one of the legal grounds that render the legal processing of the personal data possible. Apart from the explicit consent, personal data may be processed also in the presence of any one of the following conditions. The grounds of a personal data processing activity may consist of either one, or more than one of the conditions listed below.

6.3 Presence of the Explicit Consent of the Data Subject

One of the requirements for processing personal data is the explicit consent of the data subject. Explicit consent of the data subject should be a freely given, specific and informed consent.

6.4 Conditions under Which Personal Data May Be Processed Without Seeking Explicit Consent

If Clearly Provided by the Law

If clearly provided for by the law, the personal data of the Data Subject may be processed legally without seeking his / her explicit consent.

Failure to Obtain Explicit Consent of the Related Person Due To Incapability

The personal data of the data subject may be processed if it is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid.

Direct Relation with the Conclusion or Fulfillment of a Contract

It is possible to process personal data if processing of personal data belonging to the parties of a contract is necessary provided that it is directly related to the conclusion or fulfillment of that contract.

Legal Obligation

Personal data of a data subject may be processed if processing of data is mandatory for our Bank to be able to perform its legal obligations.

Making Available to Public of Personal Data by the Data Subject Himself

Personal data of a data subject may be processed if the data concerned is made available to the public by the data subject himself.

In Case Data Processing Is Mandatory For the Establishment or Protection of a Right

Personal data of a data subject may be processed if data processing is mandatory for the establishment, exercise or protection of a right.

In Case Data Processing Is Mandatory For the Legitimate Interest of the Bank

Personal data of the data subject may be processed if data processing is mandatory for the legitimate interests of the Bank, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

6.5 Processing of Personal Data of Special Nature

Our Bank is committed to showing sensitivity in abiding by the regulations stipulated under the Law with regard to the processing of personal data designated to be of a "special nature".

According to Article 6 of the Law on the Protection of Personal Data, certain personal data, which, if illegally processed, might result in victimization or discrimination of persons, are designated to be of a "special nature". Such data include race, ethnic origin, political opinion, philosophical belief, religion, sect, or other belief, clothing, membership to associations, foundations, or trade unions, health, sexual life, convictions, and security measures, and the biometric and genetic data.

In compliance with the Law on the Protection of Personal Data, personal data of special nature are processed under the following conditions, provided that the proper measures to be determined by the Board are taken:

In case the explicit consent of the data subject has been received, or

In case the explicit consent of the data subject has not been received;

- Personal data of special nature, excluding those regarding the data subject's health and sexual life, are processed under the conditions stipulated by the laws;
- Personal data of special nature regarding the health and sexual life of the data subject are processed by persons, authorized public institutions and organizations that have confidentiality obligation only for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management healthcare services as well as their financing.

6.6 Obligation to Inform

Our Bank makes disclosures to data subjects with regard to the identity of our Bank, the purpose for which personal data shall be processed, the parties to whom and the purposes for which the processed personal data may be transferred, the method and legal basis for collecting personal data, as well as the rights that the data subject has within the scope of the Article 11 of the Law on the Protection of Personal Data.

7. SAFEGUARDING THE RIGHTS OF THE PERSONAL DATA OWNER

Personal Data Owner is entitled to apply to our Bank, and to:

- Learn whether his personal data is processed or not;
- Request information if his personal data is processed
- Learn the purpose for which his personal data has been processed and whether they are used for intended purposes;
- Know the third parties to whom his personal data is transferred at home and abroad;
- Request for the rectification of the incomplete or inaccurate data, if any, and for the notification of the operations carried out in compliance with this sub-paragraph to third parties, to whom his personal data has been transferred;
- In the event that the reasons which require the processing are to be left in the middle, requesting that personal data be deleted or destroyed and that the process performed in this context be reported to a third parties to whom personal data is transferred, although processed in according to the provisions of the Law and other relevant legislation,

- Object to the processing, exclusively by automatic means, of his personal data, which leads to an unfavorable consequence for the data subject,
- Request for the compensation for any damage arising from the unlawful processing of his Personal Data in accordance with Article 11 of the Law on the Protection of Personal Data.
  Any information request, demand and complaint of data subjects are addressed within the scope of the Bank's internal regulations in such manner and within such periods as stipulated under the applicable regulations.

8. IMPLEMENTATION OF CONTINUOUS IMPROVEMENT AND CORRECTIVE ACTIONS

Our Bank continuously improves the compliance, accuracy, and effectiveness of the personal data protection and management system, and takes all the necessary preventive measures.

Our Bank provides to detect the actual or potential nonconformities, implements if any corrective measures and continuous improvement, and evaluates their effectiveness. Continuous improvements carried out within the scope of the corrective actions are proportionate to the extent of the problem. The aim is to eliminate the root cause(s) of the nonconformity/potential nonconformity.
All employees of the Bank are responsible for the transfer of personal data to the Personal Data Protection Management Section within responsibilities specified in their job descriptions in case of any non-conformities or potential nonconformities related to the security system of personal data.

The Personal Data Protection Management Section is responsible for initiating and following up the respective improvement activities, finding solutions, implementing such solutions, following up their effectiveness, and informing his/her EVP and the Personal Data Coordination Officer accordingly when necessary.

In case the processed personal data are unlawfully seized by others, the Personal Data Protection Management Section is responsible for notifying the relevant data subject and the Board of such situation as soon as possible.

Continuous improvement activities also include training of employees on such topics as avoiding the unlawful disclosure and exchange of personal data, and awareness-raising activities by the Personal Data Protection Management Section The duties and responsibilities of the parties taking part in the operation of the information (including personal data) security management system are clearly defined in the Regulation on Information Security Roles and Responsibilities.

8.1 Assessment of the Effectiveness of the Continuous Improvement and Corrective Actions

The Bank continuously improves the conformity, accuracy, and effectiveness of the access, authorization and security system in respect of the practices of collecting, processing, transferring, storing, and destroying personal data. The information in VERBIS is kept up-to-date by the Personal Data Protection Management Section Effectiveness of the implemented improvement and corrective actions as well as the effect of the implemented activities on the personal data security system is assessed and recorded by the Personal Data Protection Management Section together with related departments when necessary. Where necessary, such assessments are exchanged with the associated EVP, Personal Data Coordination Officer and the relevant committee.

8.2 Keeping the Record of Continuous Improvement and Corrective / Preventive Actions

The records of Continuous Improvement and Corrective / Preventive Actions are kept by the Personal Data Protection Management Section.

Information with regard to the comprehensive corrective and continuous improvement activities concerning more than one unit Bank-wide is submitted to the relevant committee in accordance with the nature and the scope of the subject and the necessary improvement actions necessary are then initiated.

9. DATA ACCESS MANAGEMENT

Technical and administrative measures are taken in order to avoid negligent or unauthorized disclosure of, access to, transfer of, or any other unlawful access to personal data.

10. DATA TRANSMISSION AND EXCHANGE

While our Bank displays maximum diligence and care for the domestic and international exchange of personal data, it carries out its operations in compliance with the applicable regulations.

11. DATA STORAGE AND DESTRUCTION

11.1 Security Principles Regarding the Storage of Data

The personal data provided and to be created by the Bank, which is stored as stipulated in the internal regulations documents are listed in the Personal Data Processing Inventory, and classified within the frame of the rules stipulated by the Law.
In this context, the personal data definitions set forth in the Law have been used as the classification methodology which constitutes the basis of the procedure.

Group 1: Personal data: All the information relating to any identified or identifiable natural person.

Group 2: Personal data of special nature: Data regarding a person's race, ethnic origin, political opinion, philosophical belief, religion, sect, and other belief, clothing, membership to an association, foundation, or trade union , health status, sexual life, conviction, biometric and genetic data;

Group 3: Other: Data not falling within the scope of personal data (i.e. data regarding legal entities).

II.2 Implementation of the Storage Process

There are rules and frameworks in place which have been developed in order to maintain security in the storage of personal data classified in three separate classes within the Bank's organization.

In this context, technical and administrative measures required within the Bank's organization are taken in order to store the data falling within the scope of the 1st and 2nd Groups, entitled Personal Data and Personal Data of Special Nature, respectively.

II.3 Security Principles Regarding the Destruction of Data

The personal data supplied by the Bank within the scope of this Policy, and stored in the manner way as stipulated in the respective internal regulatory documents are destroyed by way of erasure, deletion, or anonymization in view of data confidentiality when the conditions necessitating their processing by the Bank cease to exist. The most critical step taken in the destruction process is the determination of the "Retention Periods". Retention periods for all the data included in the Personal Data Processing Inventory are determined in consideration of the respective regulations. Personal data are retained by taking the required security measures considering all retention periods determined for all personal data stored Bank-wide, and upon expiration of the respective retention periods, the process of proper destruction of data is initiated.

If for any reason retention period has to be exceeded, this is kept under record provided that sufficient reasons are shown.

According to the Regulation on the Erasure, Destruction and Anonymizing of the Personal Data, the table showing the periods of retention and destruction is included in the Personal Data Processing Inventory attached to "Protection, Processing, Retention and Destruction of Personal Data Procedure".

Methods of Destruction:

Erasure of Data: Rendering personal data by no means accessible and usable by the users concerned via the electronic environments on which data reside;

Destruction of Data: Rendering personal data by no means accessible, retrievable, and reusable by anyone; i.e. destroying the written and printed media that contain personal data by means of a shredder, etc., destroying such media as CDs, USBs, expired IT hardware, etc. carrying personal data using methods stipulated under the internal regulatory documents to be drawn up in the Bank;

Anonymizing of Data: Rendering personal data impossible to link with an identified or identifiable person even through matching them with other data such as i.e. using such data as TRID, Name-Surname, etc. in a way that they may by no means be matched with an identified or identifiable natural person.

Personal data are either erased, destroyed, or anonymized during the first periodic destruction process following the date at which the obligation to erase, destroy or anonymize personal data arises. While the interval of the periodic destruction process is 6 (six) months, it is carried out in compliance with the provisions of the respective regulations, notably, those stipulated in Article 42 of the Banking Law. Technical and administrative measures are taken in order to perform the secure storage and lawful destruction of personal data.

12. REVIEW AND AUDIT ACTIVITIES

The Bank carries out internal audit activities by the mediation of the Board of Auditors in line with the Internal Audit Methodology Procedure in order to assess the performance and effectiveness of the management system it has established for the purpose of protecting personal data. The Internal Control Division, on the other hand, performs the control activities required for the personal data protection and management system again in line with the "Internal Control Methodology Procedure". The continuity, applicability, adequacy, and effectiveness of the personal data management system are addressed and reviewed at the Information Security Committee, Operational Risk Committee, Top Management Committee assembled at periodic intervals in accordance with the nature and the scope of the subject.

13. EFFECTIVE DATE

This Personal Data Protection Policy has become effective as of 29.11.2018
This policy is reviewed by the document-owner unit no less than once a year, revised if deemed necessary, and approved by the Board of Directors.