TÜRKİYE HALK BANKASI A.Ş.

PERSONAL DATA STORAGE AND DISPOSAL POLICY

CONTENTS

1. PURPOSE AND SCOPE

This Policy has been prepared to determine the main principles of the process to be followed to enable the Bank in fulfilling its obligations with regard to the storage and disposal of personal data as required by the Law on the Protection of Personal Data No. 6698 and the "By-Law on Deletion, Disposal or Anonymization of Personal Data" issued based on this Law.

The Policy implicates the personal data and sensitive/special category personal data retained by the Bank and defined by the Law.

As outlined by the law, personal data contained in systems where data is processed fully or partially through automatic means or through non-automatic means, provided that the process is part of any data registry system, is within the scope of this Policy.

2. DEFINITIONS

Law: Law on the Protection of Personal Data No. 6698,

Personal Data: Any information relating to an identified or identifiable natural person,

Sensitive/Special Category Personal Data: Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations or trade-unions, information relating to health, sexual life, convictions and security measures and the biometric and genetic data,

Processing of Personal Data: Any operation carried out on personal data such as acquiring, recording, storing, retention, alteration, re-organization, disclosure, transfer, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or through non-automatic means provided that the process is part of any data registry system,

Board: Personal Data Protection Board,

Authority: Personal Data Protection Authority,

Data Controllers' Registry Information System (VERBİS): An online information system that is established and managed by the Personal Data Protection Authority, where data controllers will be registered to and will use for other processes related to Registry,

Data Controller: The legal person Türkiye Halk Bankası A.Ş., who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data filing system,

The Personal Data Protection Committee: Türkiye Halk Bankası A.Ş. Personal Data Protection Committee who determines the purposes and means of processing personal data as data controller and is responsible for the establishment and management of the data filing system, within the scope of the Law on the Protection of Personal Data (LPPD) No. 6698 and to be appointed to fulfill their obligations under LPPD and the secondary legislation by Türkiye Halk Bankası A.Ş. (The Bank) Board of Directors,

Contact Person: The natural person named during the Registry entry process for establishing communication with the Authority in respect of the mentioned natural and legal persons' obligations under the Law and secondary legislations to be issued based on this Law, by the data controller in case of natural and legal persons resident in Turkey and by the representative of the data controller in case of non-resident natural and legal persons,

Relevant User: The employee who processes personal data within the data controller organization, except for the individual or unit responsible for the technical storage, protection and backup of the data,

Data Subject: Natural person whose personal data is processed,

Data Registry System: The registry system through which personal data are processed by structuring according to specific criteria,

Registry Environment: Any environment in which personal data are processed fully or partially through automatic means or through non-automatic means provided that the process is part of any data registry system,

Personal Data Processing Inventory: The inventory that elaborates the personal data processing activities, the channels used to acquire personal data, the purposes and legal justification for the processing of personal data, the data category, the maximum retention period of personal data created by associating the recipient group to whom such data is transferred and the data subject individuals group and the period required for the purposes for which it is processed, the personal data foreseen to be transferred abroad and the measures taken related to data security, carried out by the Bank subject to its business processes,

Data Processor: Natural or legal person who processes personal data based on the authority granted by and on behalf of the data controller,

Processing Requirement: The legal reason, the processing of personal data and sensitive/special category personal data stipulated in Articles 5 and 6 of the Law is based on,

Disposal: Deletion, destruction or anonymization of personal data,

Deletion of Personal Data: The process of rendering personal data inaccessible and unusable for all relevant users,

Destruction: The process of rendering personal data inaccessible, irretrievable and unusable for any person,

Anonymization: Rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data,

Periodic Disposal: The process of deleting, destruction or anonymization which is determined in the personal data storage and disposal policy and to be carried out periodically ex officio, in the event that all of the conditions for processing laid down in the Law no longer exist,

Banking Activities: The activities that Banks can carry out as specified in the Banking Law No. 5411,

Transaction Owner: The natural person who benefits from the products and/or services offered by the Bank within the framework of the Banking Activities, either on his/her own behalf or on behalf of a third party,

By-Law: By-Law on Deleting, Destruction or Anonymization of Personal Data.

3. GENERAL SCOPE AND LEGAL BASIS

3.1 Legal, Technical or Other Reasons Requiring Storage of Personal Data

Concerning the Law on the Protection of Personal Data No.6698, personal data and sensitive/special category personal data shall be recorded, stored, updated or, where permitted by the legislation, transferred, disclosed, transmitted to domestic or foreign 3. parties, classified and processed as listed in LPPD, for the purpose of conducting Banking activities, within the framework explained below.

3.1.1 Personal data and sensitive/special category personal data related to bank customers;

- Using in all kinds of products and services within the framework of Banking activities under the provisions of the Banking Law No. 5411 Law No. 5549 on Prevention of Laundering Proceeds of Crime, Law No. 4208 on the Prevention of Money Laundering, Capital Market Law No. 6362, Turkish Code of Obligations No. 6098, Turkish Commercial Code No. 6102 and other laws, by-laws, communiqués, international agreements, and other legal legislations,

- Recording the identity, address and other information required to identify and verify the personal identifying information of the transaction owner, preparing all records and documents that will form the basis for the transaction to be carried out electronically or in written form,

- Complying with the submission, information storage, reporting and notifying obligations stipulated by official institutions such as BRSA, MASAK, CBRT, CMB, RA, TTIB and organizations such as KKB and BKM,

- Banking practices to offer requested products and services of other Banks and for enabling banking service contracts and other credit and/or product service contracts to

be drawn up or performed,

- Personal data and sensitive/special category personal data of third parties other than the customer are processed within the scope of all legal rights and legitimate interests of the Bank, arising directly or indirectly from banking activities.

3.1.2 Personal data and sensitive/special category personal data of the employees are processed to prove the business relationship, to record remunerations and information on remuneration, to ensure that legal notifications are made to the Ministry of Finance, the Social Security Institution and other institutions, to implement occupational health and safety principles, to ensure that the legal liabilities are fulfilled and to determine the working conditions.

3.1.3 Personal data and sensitive/special category personal data acquired within the scope of contracts concluded with support services companies and companies from which products/services are purchased, are processed to ensure the performance and fulfillment of obligations of the contracts signed with support services companies and suppliers.

3.2 Technical and Administrative Measures Taken for the Legal Disposal of Personal Data, Actions to Be Taken In Case the Conditions for Processing of Personal Data No Longer Exist

3.2.1 The PDP Committee shall ensure the biannual review of whether or not the conditions related to the processing of personal data and sensitive/special category personal data included in the Personal Data Processing Inventory of the Bank still exist.

3.2.2 As a consequence of periodic reviews, the PDP Committee shall decide on the deletion, destruction, or anonymization of personal data and sensitive/special category personal data, determined to no longer exist in the relevant articles of the Law on the processing of personal data and/or sensitive/special category personal data, under this policy.

3.2.3 The PDP Committee shall ensure the immediate implementation of the warrants or decisions issued by the Board or the court, or evaluate legal actions taken regarding this warrant or decisions, such as objection and appeal and shall act according to the outcome.

3.2.4 Although the processing conditions regulated in the relevant articles of the Law regarding the processing of personal data no longer exist, in case there is an interim injunction, caution, custody and/or confiscation decision given in a lawsuit, or a lawsuit filed despite the absence of such a decision, or if there is a criminal/administrative investigation and this case or investigation is notified to the Bank, the PDP Committee stops the process of deletion, destruction or anonymization of personal data until the end of the trial/investigation, to prevent the destruction of the evidence.

3.2.5 The process of deleting personal data and sensitive/special category personal data, the processing conditions of which no longer exist, is ensured as disabling the access of any other institution, organization and/or person by rendering the data inaccessible and unusable for all relevant users. By taking necessary technical and administrative measures, it is ensured that personal data and sensitive/special category personal data can only be accessed by the employee or unit responsible for the storage, protection and backup of such data. To carry out these transactions, the Bank uses software and other technical tools and equipment performing such functions, thus executing the process of deleting personal data and sensitive/special category personal data.

3.2.6 If approved by the PDP Committee and there is a final Board or court decision concerning the request for disposal of the personal data and sensitive/special category personal data of the relevant person, access of relevant users to personal data and sensitive/special category personal data is blocked in recording media where they are stored and rendered unusable.

3.2.7 Requests of relevant persons for the deletion or destruction of their personal data are evaluated within the framework of availability of personal data processing conditions and legal regulations.

3.2.8 All transactions concerning the deletion, destruction or anonymization of personal data and sensitive/special category personal data are recorded and the subject records are kept for at least three years, excluding other legal obligations.

3.3 Secure Storage of Personal Data and Sensitive/Special Category Personal Data and Administrative and Technical Measures Taken to Prevent Unlawful Processing and Access to This Data

3.3.1 Necessary arrangements are made in such issues as the secure storage of personal data and sensitive/special category personal data, secure access to such data and prevention of unauthorized access. For the processing of sensitive/special category personal data, adequate measures within the framework of decisions of the Board, are also taken.

3.3.2 All Bank employees are informed, necessary trainings are provided and important developments are announced before the Bank, within the scope of LPPD compliance studies. This Policy is posted on the Bank portal, accessible to all personnel.

3.3.3 The PDP Committee shall carry out monitoring to see whether the requirements of the Policy are being fulfilled. When a breach of the Policy is identified, the subject matter shall be referred to the Unit Manager of the employee concerned and the Human Resources Department and the Unit Manager shall take necessary actions to rectify such breach. The provisions of the Bank Disciplinary Directive shall be applicable to any employee found to have violated the Policy.

3.3.4 The Bank shall engage any software/systems/applications needed for the fulfilment of requirements of the Policy and the PDP Committee shall follow amendments in legislation, changes in Institution recommendations and any changes that may occur due to Council decisions made and notified to the Bank by the Council or courts and shall ensure that necessary actions are taken.

3.4 Duties and Responsibilities of Individuals Involved in Personal Data Storage and Disposal Processes

3.4.1 The Personal Data Protection Committee

The PDP Committee is responsible for performing the following duties:

3.4.1.1 Ensuring and monitoring the implementation of this Policy,

3.4.1.2 Monitoring circumstances such as changes that may occur in the legislation and regulatory procedures and decisions of the Board, as well as court decisions, changes in the technical infrastructure,

3.4.1.3 Keeping track and reviewing the work programs carried out regarding data storage and disposal and checking whether the work performed within the framework of the work programs is in compliance with such Policy and in case of any discrepancy, ensuring that these are brought into conformity with this Policy,

3.4.1.4 Fulfilling any other duty as specified in this Policy.

3.4.2 Contact Person

Within the scope of this Policy, the Contact Person has the following duties and responsibilities;

3.4.2.1 Providing the required coordination to duly respond to the applications of the relevant persons in their capacity as data controller to the Bank,

3.4.2.2 Receiving or accepting notifications or correspondence from the Board in the name of the data controller,

3.4.2.3 Accepting the requests made by the Board to the data controller in the name of the data controller and transmitting the relevant responses to the Authority,

3.4.2.4 Fulfilling the duties assigned to him by the PDP Committee

4. PERSONAL DATA STORAGE AND DISPOSAL PERIODS

4.1 The Bank is obliged to provide all kinds of information and documents that will be requested in the audits, to submit the books and documents and to keep these ready for inspection and to keep all information and documents related to banking transactions for 10 years as of the date of the last transaction, within the framework of the Banking Law and Banking Regulation and Supervision Agency and Capital Market regulations.

4.2 Nonetheless, since the receivables are subject to a 10-year statute of limitations period according to Article 146 of the Turkish Code of Obligations No. 6098 and the obligation to keep documents for 10 years according to Article 82 of the Turkish Commercial Code No. 6102, personal data are stored for 10 years as of the date of the last transaction, to enable the Bank as a data controller to fulfill its legal obligation, protect its legitimate interests and to submit the documents to the judicial authorities as may be required.

4.3 In accordance with the provision of the Occupational Health and Safety Services Regulation, article 7/1-b, health and safety records of the Bank personnel shall be kept for 15 years. Additionally, in accordance with the relevant articles of the Social Security and General Health Insurance Law No. 5510, personal data other than the health and safety records of the Bank personnel are stored for 10 years following the termination of the employment contract.

4.4 Because the receivables are subject to a 10-year statute of limitations period according to Article 146 of the Turkish Code of Obligations No. 6098 and the obligation to keep documents for 10 years according to Article 82 of the Turkish Commercial Code No. 6102, the personal data acquired from support service companies and supplier companies are stored for 10 years from the date of the last transaction, to enable the Bank as the data controller to fulfill its legal obligation, protect its legitimate interests and to submit the documents to the judicial authorities as may be required.

4.5 In case the conditions for processing personal data no longer exist and the personal data subject to the request are transferred to third parties, the data controller shall notify such situation to the third party. The data controller shall ensure that the required procedures are carried out in the presence of the third person, within the scope of this Policy and By-Law.

4.6 The "Personal Data Storage and Disposal Periods Table" included in the Policy annex can be updated with the decision of the PDP Committee.

4.7 Access of relevant users to personal data is blocked and deleted at periodic disposal time intervals of six months as of the end of the periods in the attached Table.

5. EFFECT

5.1 This Policy has been accepted by the Board of Directors Decision No. 41/19 and dated 01/10/2019.

5.2 The Personal Data Protection Committee executes the provisions of this Policy.

5.3 The entry into force of this Policy supersedes the Policy on the Protection and Processing of Personal Data adopted by Türkiye Halk Bankası A.Ş. by a Resolution of the Board of Directors dated 17.04.2018 and numbered 14/42, effective as of 31.12.2017.

Personal Data Storage and Disposal Periods Table

Data Subject	Description	Storage/Disposal period (*)
Direct or indirect parties to banking transactions	Personal data	10 years
Direct or indirect parties to banking transactions	Sensitive/special category personal data	10 years
Employee	Personal data	10 years
Employee	Sensitive/special category personal data	15 years
Support Service Provider/Supplier	Personal data	10 years

*Periods start as of the date of the last transaction.