COMPLIANCE DEPARTMENT

TÜRKİYE HALK BANKASI A.Ş.
PERSONAL DATA RETENTION AND DISPOSAL POLICY

HALKBANK

HALKBANK

TABLE OF CONTENTS

1. INTRODUCTION 2

1.1. Objective and Scope 2

1.2. Definitions 2

2. DISTRIBUTION OF RESPONSIBILITIES AND TASKS 4

3. RECORDING ENVIRONMENTS 4

4. EXPLANATIONS ON RETENTION AND DISPOSAL 5

4.1 Explanations on Retention 5

4.1.1 Legal Grounds Requiring Retention 5

4.1.2 Processing Purposes that Require Retention 5

4.2 Reasons for Disposal 6

5. TECHNICAL AND ADMINISTRATIVE MEASURES 6

5.1. Technical Measures 6

5.2. Administrative Measures 7

6. PERSONAL DATA DISPOSAL TECHNIQUES 8

6.1. Deletion of Personal Data 8

6.2. Disposal of Personal Data 8

6.3. Anonymization of Personal Data 8

7. PERSONAL DATA RETENTION AND DISPOSAL PERIODS 8

8. EFFECTIVENESS 9

HALKBANK

1. INTRODUCTION

1.1. Objective and Scope

This Policy has been prepared in order to determine the basic principles of the process to be followed in order to fulfill the Bank's obligations regarding the retention and disposal of personal data in accordance with the Law No. 6698 on the Protection of Personal Data and the "Regulation on the Deletion, Destruction or Anonymization of Personal Data" issued based on this Law. This Personal Data Retention and Disposal Policy ("Policy") is based on nationally recognized basic principles regarding the protection, processing and destruction of personal data within the framework of applicable legislation and regulations.

This Policy covers personal data defined by the Law and special categories of personal data held by the Bank.

The works and transactions regarding the storage and destruction of personal data are carried out in accordance with the Policy prepared by our Bank in this direction.

1.2. Definitions

Express Consent: Consent to a particular subject matter, based on information and freely given,

Recipient Group: The category of natural or legal person to whom personal data is transferred by the data controller,

Banking Activities: Activities that banks can perform as specified in the Banking Law No. 5411,

EBYS: Electronic Document Management System,

Electronic Environment: Environments where personal data can be created, read, changed and written with electronic devices,

Non-Electronic Environment: All written, printed, visual, etc. media other than electronic environments,

Service Provider/Supplier: A natural or legal person who provides goods and/or services to our Bank under a specific contract,

Contact Person: The natural person whose personal data is processed,

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

Disposal: Deletion, disposal or anonymization of personal data,

Contact Person: The natural person notified to the Registry by the data controller for natural and legal persons resident in Türkiye and by the representative of the data controller for natural and legal persons not resident in Türkiye, in order to ensure communication with the Authority regarding their obligations under the Law and the secondary regulations to be issued based on this Law,

Transaction Owner: A natural person who benefits from the products and/or services offered by the Bank within the framework of the banking activities carried out by the Bank, either on his/her own behalf and account or on behalf and account of someone else,

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

Registration Environment: Any medium containing personal data that is fully or partially automated or processed by non-automated means, provided that it is part of any data recording system,

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

Personal Data Processing Inventory: The inventory that our Bank creates by associating the personal data processing activities that it carries out depending on the business processes of our Bank with the channels of obtaining personal data, the purposes and legal reason for processing personal data, the data category, the transferred recipient group and the data subject group, and details the maximum retention period required for the purposes for which personal data are processed, the personal data foreseen to be transferred to foreign countries and the measures taken regarding data security,

Anonymization of Personal Data: Rendering personal data impossible to be associated with an identified or identifiable natural person even if it is matched with other data,

Processing of Personal Data: All kinds of operations performed on personal data, such as obtaining, recording, storing, retaining, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic means or by non-automatic means provided that they are part of any data recording system,

Deletion of Personal Data: The process of making personal data inaccessible and non-reusable by the relevant users in any way,

Disposal of Personal Data: The process of making personal data inaccessible, irretrievable and non-reusable by anyone in any way,

Board: Personal Data Protection Board,

Institution: Personal Data Protection Institution,

KVK Committee: Within the scope of Law No. 6698 on the Protection of Personal Data (KVKK), Türkiye Halk Bankası A.Ş., as the data controller, determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system. (Bank) "Türkiye Halk Bankası A.Ş. Personal Data Protection Committee" to be assigned by the Board of Directors to fulfill its obligations under the PDPL and secondary regulations,

Masking: Erasing, crossing out, coloring and starring certain areas of personal data in such a way that they cannot be associated with an identified or identifiable natural person,

Sensitive Personal Data: Data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data,

Periodic Disposal: The deletion, destruction or anonymization process to be carried out officially at recurring intervals specified in the Personal Data Retention and Disposal Policy in the event that all of the conditions for processing personal data specified in the Law disappear,

Policy: Personal Data Retention and Disposal Policy,

Data Processor: A natural or legal person who processes personal data on behalf of the Data Controller based on the authorization granted by the Data Controller,

Data Recording System: A recording system where personal data is structured and processed according to certain criteria,

Data Controllers Registry Information System (VERBIS): The information system created and managed by the Presidency of the Personal Data Protection Authority, accessible over the internet, which data controllers will use in the application to the Registry and other related transactions related to the Registry,

Data Controller: Türkiye Halk Bankası A.Ş. as the legal entity that determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system,

Regulation: Regulation on Deletion, Destruction or Anonymization of Personal Data

2. DISTRIBUTION OF RESPONSIBILITIES AND TASKS

The distribution of the titles, units and job descriptions of those involved in the storage and destruction of personal data is given in Table-1.

Table-1: Retention and Disposal Processes Task Distribution Table

UNIT/COMMITTEE	TASK
Personal Data Protection Committee	• It is responsible for determining the methods of destruction and storage within the scope of this Regulation and deciding on periodic destruction processes.
Branch Operations Department	• Establishing policies in accordance with the KVKK and ensuring coordination with the relevant units regarding the preparation, development and execution of the Policy, • Responsible for determining the technical measures included in the policy.
Departments of Information Technologies	• Taking technical measures for the storage and destruction of bank data, • Responsible for providing technical solutions needed for the implementation of the policy.
Internal Control Department	• Responsible for reviewing the compliance of the controls established for retention and destruction processes with internal and external legislation.
Related Departments	• It is responsible for taking the necessary measures regarding the processing, storage and destruction of personal data in order to comply with the PDPL in relation to its own business processes.

3. RECORDING ENVIRONMENTS

Personal data are securely stored by our Bank in accordance with the law in the environments listed in Table-2.

Table-2: Personal Data Retention Environments Table

• Servers (web server, database, file sharing, domain, backup, e-mail, etc.) • Software (Banking service software, auxiliary in-house process management software, office software, portal, EBYS) • Information security devices (firewall, intrusion detection and prevention, log file, antivirus, etc.) • Personal computers (desktop, laptop) • Mobile devices (phones, tablets, etc.) • Optical disks (CD, DVD, etc.) • Removable memories (USB, memory card, etc., tape cartridges) • Printer, scanner, copier	• Paper • Manual data recording systems (survey forms, visitor logbook) • Other written, printed and visual media in locked storerooms, rooms, safes, cabinets or desk drawers in headquarters, branches or centers specially prepared for storage purposes

4. EXPLANATIONS ON RETENTION AND DISPOSAL

4.1 Explanations on Retention

4.1.1 Legal Grounds Requiring Retention

Personal data processed within the framework of our Bank's activities are subject to the Law No. 6698 on the Protection of Personal Data, Banking Law No. 5411, Law No. 5549 on the Prevention of Laundering Proceeds of Crime, Turkish Code of Obligations No. 6098, Turkish Commercial Code No. 6102, Labor Law No. 4857, Social Insurance and General Health Insurance Law No. 5510, Occupational Health and Safety Law No. 6361, Law No. 4208 on the Prevention of Money Laundering, Capital Markets Law No. 6362, Law No. 4982 on the Right to Information, Law No. 3071 on the Exercise of the Right to Petition, Tax Procedure Law No. 213, Bank Cards and Credit Cards Law No. 5464, Law No. 6502 on Consumer Protection, Check Law No. 5941, other relevant laws, regulations, communiqués, international agreements and other provisions of legal legislation and in order to comply with the processing, storage, reporting and other obligations stipulated by the relevant legislation.

4.1.2 Processing Purposes that Require Retention

Personal data of the Bank's customers and special categories of personal data;

- Use in all kinds of products and services within the framework of banking activities,
- Realization of banking services in accordance with the legislation,
- Ensuring the Bank's property rights and security,
- Ensuring that legal obligations are fulfilled,
- Fulfillment of the burden of proof as evidence in legal disputes,
- Execution of human resources processes and ensuring corporate communication,
- Responding to complaints, questions and requests of relevant persons,
- Recording the identity, address and other necessary information in order to identify and confirm the identity of the transaction owner; issuing all records and documents that will be the basis of the transaction to be carried out electronically or in writing,
- Compliance with the submission, information retention, reporting and information obligations stipulated by official institutions such as BRSA, MASAK, CBRT, CMB, Revenue Administration, VDK and organizations such as KKB, BKM,
- To provide other Bank products and services requested and to ensure the establishment or performance of the banking services agreement and other loan and/or product service agreements and all other agreements,

Personal data and special categories of personal data relating to third parties other than the customer;

- Within the scope of all legal rights and legitimate interests of the Bank arising directly or indirectly from banking activities,

Personal data relating to the employee and sensitive personal data;

- In order to prove the employment relationship, to record wage and wage-related information, to make legal notifications to the Republic of Türkiye Ministry of Treasury and Finance, Social Security Institution and other institutions, to implement occupational health and safety principles, to fulfill the obligations arising from the law and to determine working conditions,

Personal data and sensitive personal data obtained within the scope of contracts concluded with support services companies and companies from which products/services are purchased;

- In order to execute the contracts signed with support services companies and suppliers and to fulfill their obligations

In addition, it is processed in order to realize other purposes stipulated in the relevant legislation.

4.2 Reasons for Disposal

Personal data shall be destroyed in the event that

- the provisions of the relevant legislation that constitute the basis for its processing are changed or abolished, the purpose requiring its processing or retention disappears,
- in cases where the processing of personal data takes place only on the basis of explicit consent, the person concerned withdraws his/her express consent,
- the application made by the person concerned regarding the deletion and destruction of his/her personal data is accepted by our Bank,
- the decision given by the Board is implemented,
- the maximum period of time requiring the storage of personal data has expired.

5. TECHNICAL AND ADMINISTRATIVE MEASURES

5.1. Technical Measures

Necessary arrangements are made for the secure storage of personal data and sensitive personal data, secure access to these data and prevention of unauthorized access. Adequate measures are also taken for the processing of special categories of personal data within the framework of the decisions of the Board.

The technical measures taken by our Bank regarding the personal data it processes are listed below:

- Network security and application security are ensured.
- Closed system network is used for personal data transfers through the network.
- Key management is applied.
- Security measures are taken within the scope of procurement, development and maintenance o information technology systems.
- Access logs are kept regularly.
- Data masking measures are applied when necessary.
- Up-to-date anti-virus systems are used.
- Firewalls are used.
- Personal data is backed up and the security of backed up personal data is also ensured.
- User account management and authorization control system are implemented and monitored.
- Log records are kept without user intervention.
- Intrusion detection and prevention systems are used.
- Penetration test is applied.
- Encryption is performed.
- Data loss prevention software is used.
- Extra security measures are taken for personal data transferred via paper and the relevant document is sent in the format of a confidential document.
- Necessary security measures are taken regarding entry and exit to physical environments containing personal data.
- Physical environments that include personal data must be secured against outer risk. (fire, flood, etc.)
- Security of environments containing personal data is ensured.
- Secure encryption/cryptographic keys are used for sensitive personal data and managed by different units.
- Sensitive personal data transferred on portable memory sticks, CDs and DVDs are encrypted.
- Authorization access matrix is created for employees.
- Employees who are reassigned or leave their jobs are no longer authorized in this area.

5.2. Administrative Measures

The administrative measures taken by our Bank regarding the personal data it processes are listed below:

- Personal data security is monitored.
- Existing risks and threats are identified.
- If sensitive personal data is to be sent via electronic mail, it is sent encrypted and using a KEP or corporate mail account.
- Cyber security measures have been taken and their implementation is constantly monitored.
- There are disciplinary regulations for employees that include data security provisions.
- Training and awareness raising activities on data security are carried out at regular intervals for employees.
- Corporate policies on access, information security, use, storage and disposal have been prepared and implemented.
- Confidentiality commitments are made.
- The signed contracts contain data security provisions.
- Personal data security policies and procedures have been determined.
- Personal data security issues are reported quickly.
- Internal periodic and/or random audits are conducted and commissioned.
- Protocols and procedures for the security of sensitive personal data have been determined and implemented.
- Data processing service providers are periodically audited on data security.
- Awareness of data processing service providers on data security is ensured.
- Personal data is minimized as much as possible.
- Before starting to process personal data, the Bank fulfills its obligation to inform the relevant persons.
- Personal data processing inventory has been prepared and is updated periodically.

6. PERSONAL DATA DISPOSAL TECHNIQUES

At the end of the period stipulated in the relevant legislation or the retention period required for the purpose for which they are processed, personal data are destroyed by our Bank in accordance with the provisions of the relevant legislation, either ex officio or upon the application of the person concerned. The disposal of personal data can be done in three different ways: deletion, destruction or anonymization of the data. In the disposal processes of personal data, the process-based maximum retention periods in the personal data processing inventory are taken into consideration.

6.1.Deletion of Personal Data

Deletion of personal data is making it inaccessible and non-reusable in any way for the relevant users, except for authorized persons with limited access.

After determining the data to be deleted, the relevant users using the data are identified using authorization management applications. These users' authorizations and methods such as access, retrieval, reuse are closed or eliminated.

6.2. Disposal of Personal Data

Disposal of personal data is the process of making personal data inaccessible, unrecoverable and unusable by anyone in any way.

Where data is processed on physical recording media, disposal is carried out in such a way that it cannot be retrieved.

6.3. Anonymization of Personal Data

Anonymization is the process of making personal data impossible to associate with an identified or identifiable natural person, even if such data is matched with other data, in cases where personal data is processed in whole or in part by automated means.

By removing or modifying all direct and/or indirect identifiers in the relevant dataset, the identity of the person concerned is prevented, its distinguishability within the dataset is eliminated, and it is made impossible to associate it with a real person.

7. PERSONAL DATA RETENTION AND DISPOSAL PERIODS

Personal data are stored for the maximum retention period stipulated in the legislation or required for the purpose for which they are processed. When determining the maximum retention period;

- The period that must be kept within the framework of legal obligation,
- The period during which the legal relationship that requires the processing of personal data will continue,
- The period during which the legitimate interest will be observed in accordance with the law and the rules of honesty,
- The period during which the risks, costs and responsibilities to be created by storage will continue legally,
- The period that is suitable for keeping the data accurate and up-to-date when necessary,
- The statute of limitations determined for the assertion of a right based on personal data,
- Whether there is a legal dispute,
- The general customs of the sector

  are taken into account.

- The Bank is obliged to provide all kinds of information and documents required by the Banking Law and the Banking Regulation and Supervision Agency and Capital Markets regulations, to submit books and documents and to keep them ready for inspection, and to keep all information and documents related to banking transactions for 10 years from the date of the last transaction.

- However, since receivables are subject to a 10-year statute of limitations pursuant to Article 146 of the Turkish Code of Obligations No. 6098 and documents are required to be kept for 10 years pursuant to Article 82 of the Turkish Commercial Code No. 6102, personal data are kept for 10 years from the date of the last transaction in order to enable our Bank, as the data controller, to fulfill its legal obligation, to protect its legitimate interests and to enable the documents to be submitted to judicial authorities if necessary.

- Personal data obtained from support service companies and supplier companies are kept for 10 years from the date of the last transaction in order to enable the Bank, which is the data controller, to fulfill its legal obligation, to protect its legitimate interests and to enable the documents to be submitted to the judicial authorities in case of need, since the receivables are subject to a 10-year statute of limitations pursuant to Article 146 of the Turkish Code of Obligations No. 6098 and the documents are required to be kept for 10 years pursuant to Article 82 of the Turkish Commercial Code No. 6102.

Personal and sensitive personal data are disposed of by taking into account the periods specified in Table-3. The "Personal Data Retention and Disposal Periods Table" may be updated with the decision of the PDP Committee.

Table-3: Personal Data Retention and Disposal Periods Table

RELATED PERSON	EXPLANATION	RETENTION PERIOD (*)	DISPOSAL PERIOD
Direct or indirect parties to banking transactions	Personal data	10 years	At the first periodic destruction following the end of the retention period
Direct or indirect parties to banking transactions	Sensitive personal data	10 years	At the first periodic destruction following the end of the retention period
Support Service Provider/Supplier	Personal data	10 years	At the first periodic destruction following the end of the retention period
Other 3rd Parties	Personal data	10 years	At the first periodic destruction following the end of the retention period

*Terms start from the date of the last processing date / all processing conditions are no longer applicable.

In accordance with Article 11 of the Regulation, the Bank has determined the periodic destruction period as six-month periods.

All transactions regarding the deletion, destruction or anonymization of personal data and sensitive personal data are recorded and such records are kept for at least three years, excluding other legal obligations.

8. EFFECTIVENESS

8.1. This Policy was adopted by the Board of Directors Decision dated 17.10.2023 and numbered 38/26.

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

8.3. With the entry into force of this Policy, the Personal Data Retention and Disposal Policy of Türkiye Halk Bankası A.Ş. adopted by the Board of Directors Decision dated 01/10/2019 and numbered 41/19 is abrogated.