

**TÜRKİYE HALK BANKASI A.Ş.**  
POLICY ON THE PROTECTION AND  
PROCESSING OF PERSONAL DATA

## TABLE OF CONTENT

1. PURPOSE AND SCOPE .....	2
2. BASIS .....	2
3. TERMS .....	2
4. DUTIES, AUTHORITIES AND RESPONSIBILITIES .....	4
5. PRINCIPLES OF PERSONAL DATA PROCESSING.....	5
6. CONDITIONS FOR PROCESSING PERSONAL DATA.....	6
7. CONDITIONS OF PROCESSING THE SENSITIVE PERSONAL DATA .....	7
8. TRANSFER OF PERSONAL DATA.....	7
9. DESTRUCTION OF PERSONAL DATA.....	8
10. OUR OBLIGATIONS.....	8
11. RIGHTS OF THE DATA SUBJECT .....	10
12. OTHER ISSUES .....	11
13. ENFORCEMENT .....	11

## **1. PURPOSE AND SCOPE**

This Policy has been established to ensure the compliance of our Bank with the Personal Data Protection Law No. 6698 (PDPL) and its secondary regulations which are issued to protect fundamental rights and freedoms of people, the right to privacy, with respect to processing of personal data and to set forth liabilities, procedures and principles to be abode by the natural or legal persons who process personal data.

The compliance of all its internal operations with the PDPL, secondary regulations, advices of the Personal Data Protection Agency (Agency), decisions and regulations of the Personal Data Protection Board (Board), final court orders and other relevant legislation, in line with the principles adopted by the Bank namely, superior service quality, respecting the rights of individuals, transparency and honesty; is a prior issue for our Bank.

This Policy aims the efficient implementation of the regulations to be introduced in accordance with the basic principles mentioned above for compliance with the PDPL in the Bank.

Activities for the processing and protection of personal/special categories of personal data of our Bank's customers, business partners, shareholders, executives/officials, employees, consultants, advisors, solution partners, guests, institutions and organizations with which it has cooperation and business relations, and their employees, shareholders, officials and third parties are handled within the scope of PDPL and this Policy.

Within the scope of the fundamental regulations of this Policy, necessary technical and administrative measures are taken in the processing and protection of personal data within the Bank's operations; the required internal procedures are established; appropriate training is provided to raise the awareness, all necessary measures are taken to ensure compliance with the processes of the PDPL among employees; technological infrastructure, as well as administrative and legal systems have been established together with the appropriate and effective control mechanisms in line with the basic regulations projected by the Policy.

The Policy governs the principles to be regarded during all of these processes and issues required as per the regulations introduced by the PDPL. The employees of our Bank and to the extent that they come into in contact with the personal data in the possession of our Bank, our affiliates, subsidiaries, business partners and third parties from which our Bank has purchased products and/or services, and their personnel, and, if applicable, their third parties, are obliged to comply with the legislation on the protection of personal data, in particular with this Policy and the PDPL, and with Personal Data Protection Agency recommendations, resolutions of the Personal Data Protection Board and other legislative provisions.

## **2. BASIS**

This Policy has been prepared based on Personal Data Protection Law No. 6698 (PDPL) and its secondary regulations.

## **3. TERMS**

### **3.1. Explicit Consent**

It refers to the consent that relates to a specified issue, declared by free will and based on information.

The burden of proof that the relevant person has been informed and enlightened is on the data controller, and the storage and protection of the relevant person's explicit consent and information records are carried out in accordance with the Bank's internal regulations.

### 3.2. Recipient Group

It refers to the category of natural or legal person to whom personal data is transferred by the data controller.

### 3.3. Relevant Person

It refers to the natural person whose personal data is processed.

### 3.4. Contact Person

It refers to natural persons named (by the data controller in the case of natural and legal persons based in Turkey, and by the representative of the data controller in the case of natural and legal persons not resident in Turkey) during the Registry entry process to serve as a point of contact for establishing communication with the Institution regarding the mentioned natural and legal persons' obligations under the Law and any secondary legislation to be issued on the basis of the Law.

### 3.5. Personal Data

Personal data refers to any kind of information relating to an identified or identifiable natural person.

All information that makes a person identifiable is considered personal data. Examples include such information as Turkish Republic identification number (TRID No), full name, address, e-mail address, phone number, birth date and bank account number.

### 3.6. Personal Data Processing Inventory

It refers to the documentation that explains in detail the personal data processing activities carried out by Halkbank as part of its business operations; the channels used to obtain personal data; the purposes and legal justification for the processing of personal data; the data category; the maximum storage period for the purposes that it constitutes by associating with the transferred recipient group and the data subject group, and for which the personal data is processed; the personal data foreseen to be transferred to foreign countries; and the measures taken related to data security.

### 3.7. Destruction of Personal Data

Destruction means the erasure, eradication or anonymization of personal data.

**Erasure:** This is the process of making the personal data, which has been processed automatically or semi-automatically, absolutely inaccessible and non-retrievable by relevant users.

**Removal:** This is the process of making the personal data definitely inaccessible, irretrievable and not usable by any person.

**Anonymization:** Rendering personal data, which in no way may be associated with an identified or identifiable natural person by no means, even when paired with other data.

### 3.8. Processing of Personal Data

The processing of personal data refers to any process such as the acquisition of personal data and the saving, storage, preservation, alteration, rearrangement, disclosure, transferring, being taken over, making acquirable, categorization or prevention of use which are carried out on the data in a fully or partially automated or non-automated manner as part of a data recording system.

### **3.9. PDP Committee**

Within the scope of the Personal Data Protection Law No. 6698 (PDPL), it refers to the “Türkiye Halk Bankası A.Ş. Personal Data Protection Committee” to be assigned by the Board of Directors of Türkiye Halk Bankası A.Ş., which determines the purposes and means of processing personal data as a data controller within the scope of the Personal Data Protection Law No. 6698 (PDPL), and is responsible for the installation and management of the data recording system, to fulfill its obligations under the PDPL and secondary regulations.

### **3.10. Sensitive Personal Data**

Sensitive Personal Data means the data that is related to people’s race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, appearance and mode of dress, membership to associations, foundations or unions, health, sexual life, criminal conviction and security measures, and biometric and genetic information.

### **3.11. Data Processor**

It refers to a natural person or legal entity that processes personal data on behalf of the data controller based on the authority granted by the data controller.

### **3.12. Data Category**

It refers to the personal data belonging to sets or data subject sets that are grouped according to common characteristics of personal data.

### **3.13. Data Subject Group**

It refers to the data subject category for which the data controller is processing personal data.

### **3.14. Data Controllers’ Registry Information System (DCRIS/VERBIS)**

It refers to an online information system that is established and managed by the Department, and used by the data controller for application to Registry and other transactions regarding Registry.

### **3.15. Data Controller**

It refers to our Bank which determines the purposes and means of personal data processing and is responsible for setting up and managing the data recording system.

## **4. DUTIES, AUTHORITIES AND RESPONSIBILITIES**

**4.1.** Our Bank, in its capacity as the Data Controller, is responsible for implementation of this Policy for regulation of all its internal operations and processes. “The Türkiye Halk Bankası A.Ş. Personal Data Protection Committee” has been established to ensure that all obligations imposed by the legislation are fulfilled by our Bank. The Bank fulfills these responsibilities through the Personal Data Protection Committee.

**4.2.** The Personal Data Protection Committee is responsible for implementation of the internal regulations drafted in accordance with the Policy and training activities in line therewith within the Bank.

**4.3.** Our Bank’s employees are obliged to cooperate with the Personal Data Protection Committee and Personal Data Protection Unit Supervisors in the fulfillment of legal liabilities and in the prevention of risks and hazards that may arise due to the provisions of the relevant legislation and pertaining to the compliance with the Policy.

**4.4.** All service units and organs of the Bank and related employees thereof are obliged to act in accordance with the Policy and to ensure compliance with the provisions of the Policy.

**4.5.** This Policy is retained in our Bank's intranet system as a policy and available at any time. This Policy is also published on our Bank's website. Future changes to the Policy shall be livingly reflected on our Bank's website and intranet system, thus keeping the data owner informed by accessing the principles stipulated in the Policy.

**4.6.** The Personal Data Protection (PDP) Committee shall carry out monitoring to see whether the requirements of the policy are being fulfilled. When a violation of the policy has been identified, the matter shall be referred to the Unit Manager of the employee concerned and the Human Resources Department, and the Unit Manager shall take the necessary actions to rectify the violation. The provisions of the Bank's Disciplinary Directive shall be applicable to any employee found to have violated the policy.

**4.7.** The Bank shall put into operation any software/systems/applications required for the fulfilment of the requirements of the Policy, and the PDP Committee shall keep abreast of amendments in legislation, announced changes in Institution recommendations, Council decisions, and any decisions made by the Council or courts that are notified to the Bank, and shall ensure that the necessary actions are taken.

## **5. PRINCIPLES OF PERSONAL DATA PROCESSING**

The principles that govern our Bank's personal data processing are as follows:

### **5.1. Conformity with the law and the rule of good faith**

All personal data-processing activities are carried out by our Bank primarily in accordance with Banking legislation and legislation related to the Protection of Personal Data, as well as in accordance with the provisions of all legislations to which our Bank is subject to, and in accordance with the rule of good faith as stipulated in Article 2 of the Civil Code.

### **5.2. Accuracy and up-to date information where necessary**

Our Bank attaches great importance to keep the personal data accurate and up-to-date. Channels are made available to ensure that information regarding the data subject is accurate and up-to-date; and measures are taken to ensure that the personal data is accurate and up-to-date. Administrative and technical mechanisms are also in operation for the assessment of requests coming from a data subject who contacts the Bank acting as the Data Controller, or for the correction or inspection of the accuracy of personal data found to be inaccurate or out of date, in cases where the Bank may deem it necessary.

### **5.3. Processing for specific, explicit, and legitimate purposes**

Personal data is processed primarily in accordance with banking legislation and legislation related to the Protection of Personal Data within the scope of the legislation to which our Bank is subject, limited to the products and/or services offered or presented by our Bank. The purpose of personal data processing is determined clearly and precisely prior to the processing of the intended data.

### **5.4. Being relevant, limited and proportionate to the purposes for which data is processed**

Personal data is processed by our Bank only in connection with, and limited to, the purposes of processing, and where necessary for the purpose of accomplishment of this purpose. In addition, the processing of personal data that is not related to and required for the real purpose of processing the data, is avoided.

## **5.5. Storing the data for the time stipulated by the relevant legislation or not more than the time required for its intended processing purpose**

Personal data is processed during the allowed time stipulated by the provisions of the relevant legislation, and not more than the time required for its purpose. When the justification for the processing of personal data is no longer available, or when the allowed time is over as stipulated by the legislation, personal data is destroyed by a method (deletion, destruction or anonymization) deemed appropriate by our Bank.

However, if there is a legal obligation for the storage of such data, even in the event of the justification for the use of such personal data is no longer available, the data shall be processed only for the purpose of fulfilling the legal obligation. Necessary technical and administrative measures are taken to prevent the processing of personal data at the end of the required period.

## **6. CONDITIONS FOR PROCESSING PERSONAL DATA**

The legal grounds determined as per legislation regarding personal data processing are listed below.

The personal data-processing activities carried out by our Bank may be based on one or more of the following legal grounds.

### **6.1. Where expressly permitted by laws**

Where explicitly stipulated in the provisions of legislation, data processing activities may be carried out without the consent of the data subject, provided that the activities do not exceed legislative limits. For example, our Bank within the limits stipulated by legislative provisions, where the Law on the Restructuring of the Debts to the Financial Sector No. 4743, the Banking Law No. 5411 and other related legislation stipulate the processing of personal data, processes personal data.

### **6.2. Where necessary, in order to protect the life or physical integrity of the data subject or another person in the event of the data subject is physically incapable of giving consent or his/her consent is not acknowledged as valid in the legal sense**

As a requirement of the PDPL, the processing of personal data is only possible when personal data processing is obligatory for the protection of the life or bodily integrity of the person, or someone else who is effectively unable to disclose his/her consent, or whose consent is not acknowledged as valid in the legal sense. In cases that suits this regulation, our Bank has the right to process personal data.

### **6.3. When necessary to process the personal data of parties to a contract, provided that the processing is related directly to the execution or performance of the contract**

The personal data, required for the fulfillment of obligations within the scope of execution or performance of a contract, may be processed without the explicit consent of the data subject within the scope of the PDPL. This also includes data processing activities related to the establishment phase of the contractual relationship between the data subject and our Bank.

For example, in the process of establishing a loan contract, there is no need to obtain the explicit consent of the person to carry out a credibility check by obtaining salary payroll, abstract of title or documentary evidence of no debt or for such necessary information as identity or contact information, which are the essential elements of the contract.

#### **6.4. When mandatory for the data controller to fulfill its legal obligation**

Personal data is processed by our Bank, which acts as a Data controller according to PDPL requirements, to fulfill its obligations arising from legislative provisions, in such a way as to be bound by the limits of the relevant obligation. For example, there is no need to obtain the explicit consent of the data subject for processing personal data to fulfill the obligations of the Bank in accordance with the relevant legislation on the Prevention of Laundering of the Crime Revenues.

#### **6.5. In the event of public disclosure by the data subject himself/herself**

In case the personal data made public by the data subject himself/herself, such personal data may be processed by our Bank in accordance with the purposes of publicity.

#### **6.6. When mandatory for the institution, usage or protection of a right**

Personal data may be processed by our Bank to the extent that it is mandatory for the institution, usage or protection of a right.

#### **6.7. Where mandatory for the legitimate interests of the data controller**

Personal data may be processed in line with the legitimate interests of our Bank, provided that the fundamental rights and freedoms of the data subject are not damaged. The "legitimate interests of our Bank", however, may not contradict in any way to the principles set forth by the PDPL, the purpose of processing of the personal data, and may not be implemented as an intervention into the essence of the right guaranteed by the Constitution.

#### **6.8. With the explicit consent of the data subject**

If any of the aforementioned personal data processing conditions are not covered in the processing of personal data, the explicit consent of the data subject may be requested by our Bank. In such cases, the personal data of the data subject may be processed by our Bank by informing (the data subject on the issue requiring his/her explicit consent) and obtaining his/her explicit consent (limited to this issue).

### **7. CONDITIONS OF PROCESSING THE SENSITIVE PERSONAL DATA**

In the processing of special personal data, the provisions of the Policy on the Protection and Processing of Special Personal Data adopted by Türkiye Halk Bankası A.Ş. shall be applicable in addition to the guidelines set forth in this Policy.

## **8. TRANSFER OF PERSONAL DATA**

### **8.1. Transfer of Personal Data Domestically**

#### **8.1.1. The transfer of personal data without obtaining the consent of the data owner, on the condition that the requirements related to the processing of personal data are fulfilled**

It is possible to transfer personal data to the groups of recipients specified in the personal data processing inventory in line with the conditions set out in clause 3 of Article 6 and clause 5 of Article 2 of the PDPL, and Articles 6.1, 6.2., 6.3., 6.4., 6.5., 6.6., 6.7., 6.8. of this Policy regarding data processing requirements for the processing of personal data.

In the transfers made by our Bank, as the data controller, to our Bank's data processors, care is taken to ensure that the data processors take the necessary technical and administrative actions provided for in the PDPL related to data security.



### **8.1.2. Providing the relevant conditions for the sensitive personal data and the transfer of personal data on the condition that the legislative provisions have been fulfilled**

In the transfer of special personal data, the provisions of the Policy on the Protection and Processing of Special Personal Data adopted by our Bank shall be applicable.

### **8.1.3. Existence of the explicit consent of the data subject for data transfer**

In the lack of aforementioned conditions for the transfer of personal data and/or sensitive personal data, the explicit consent of data subject may be requested by our Bank. In this case, the transfer of personal data may be made by informing data subject on the issue requiring his/her explicit consent and after obtaining his/her explicit consent, limited to this issue.

## **8.2. Transfer of Personal Data Abroad**

### **8.2.1. Transfer of personal data on the condition that the requirements for the processing of personal data are fulfilled**

Under the conditions set out in clause 3 of article 6 and clause 5 of article 2 of PDPL, and Articles 6.1, 6.2., 6.3., 6.4., 6.5., 6.6., 6.7., 6.8. and 7. of this Policy regarding data processing requirements for the processing of personal data and sensitive personal data, personal data may be transferred abroad, taking into account the conditions regarding the Transfer of Personal Data Abroad in Article 9 of the PDPL.

## **9. DESTRUCTION OF PERSONAL DATA**

Our Bank will delete, destroy or anonymize personal data in accordance with the Policy on the Storage and Destruction of Personal Data adopted by Türkiye Halk Bankası A.Ş.

## **10. OUR OBLIGATIONS**

### **10.1. Obligation to inform**

Our bank will inform the person concerned while the personal data is obtained directly from the data owner by our Bank,

If the personal data was not obtained from the data owner;

- a) within a reasonable period of time after the personal data is obtained,
- b) when the first communication is established, if the personal data is to be used for communications with the data owner,
- c) if personal data is to be transferred, when the first transfer of personal data is to be performed.

Informational texts to be used for specific business processes and/or for groups of persons as a means of fulfilling the obligation to inform shall be drafted and released by the PDP Committee in line with our Bank's Personal Data Processing Inventory.

### **10.2. The obligation to ensure the protection of personal data**

Technical and administrative measures are taken by our Bank in order to prevent unlawful processing and access to personal data and to ensure the protection of personal data, related systems are established, and such systems are monitored and inspected by our Bank.

### **10.2.1. Technical Measures**

The technical measures taken by our Bank regarding the personal data it processes are as follows:

- Network security and application security are ensured.
- Closed system network is used in personal data transfers through the network.
- Key management is applied.
- Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
- Access logs are kept on a regular basis.
- When necessary, data masking measures are applied.
- 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 is implemented and monitored.
- Log records are kept with no user intervention.
- Attack detection and prevention systems are used.
- Penetration testing is applied.
- Encryption is practiced.
- Data loss prevention software is used.
- Additional security measures are taken for personal data transferred by paper and the related document is sent in a classified document format.
- Necessary security measures are taken for entering and leaving physical environments containing personal data.
- Physical environments containing personal data are secured against external risks (such as fire, flood, etc.).
- Security of environments containing personal data is ensured.
- Secure encryption/cryptographic keys are used for sensitive personal data and they are managed by different departments.
- Sensitive personal data transferred in portable memory, CD, DVD media are encrypted.
- An authorization access matrix is created for employees.
- The authorizations of employees who have a change of duty or leave their jobs are removed in this area.

### **10.2.2. Administrative Measures**

The administrative measures taken by our Bank regarding the personal data it processes are as follows:

- The security of personal data is monitored.
- Existing risks and threats are identified.
- If any sensitive personal data needs to be sent by e-mail, they must be sent in encrypted form and using KEP (registered e-mail) or corporate mail account.
- Cyber security measures are taken and their implementation is continuously monitored.
- There are disciplinary regulations that include data security provisions for employees.
- Training and awareness raising activities regarding data security are periodically carried out for employees.
- Corporate policies on access, information security, use, storage and destruction have been prepared and implemented.
- Confidentiality undertakings are made.

- Data security provisions are included in the contracts signed.
- Personal data security policies and procedures have been determined.
- Personal data security issues are reported promptly.
- Periodic and/or random internal audits are conducted and commissioned.
- Protocols and procedures for sensitive personal data security are been defined and implemented.
- Data processing service providers are periodically audited on data security.
- Awareness of data processing service providers regarding data security is ensured.
- Personal data is mitigated as much as possible.
- The Bank fulfills its obligation to inform the related persons before initiating personal data processing.
- Personal data processing inventory is prepared and periodically updated.

### **10.2.3. Carrying out the necessary inspections/having the necessary inspections carried out**

Our Bank is devising systems to carry out the necessary inspections or having it carried out regarding the functioning of technical and administrative measures taken to fulfill its legal obligations. Audit results are reported to the relevant parties within the scope of the internal operation of the Bank, and the necessary activities are carried out to improve the measures taken.

According to Article 12 of the PDPL, our Bank is also responsible for the third parties to whom the Bank transfers personal data, to fulfill their obligations of lawful processing, protection of data and lawful access to data as per the provisions of this Policy and the PDPL. Therefore, our Bank includes undertakings, to ensure these conditions and grant the Bank the authority to audit, in the agreements and all kind of arrangements to be executed whilst transferring the data to third parties. Our Bank also informs its employees on their responsibilities arising from the transfer processes of personal data to third parties.

## **11. RIGHTS OF THE DATA SUBJECT**

According to Article 11 of the PDPL, the data subject has the following rights against our Bank acting as the Data Controller.

- a. To be informed whether or not personal data is being processed
- b. If the data subject's personal data has been processed, to request information about the nature of the processing
- c. To be informed on the reason of personal data processing, and whether it is used in accordance with the defined purpose
- d. To be informed on the third parties to whom personal data is transferred domestically or abroad
- e. To request the correction of personal data in case of incomplete or incorrect processing
- f. To request that personal data be deleted or destroyed if the conditions which anticipated in Article 11 of the PDPL are realized
- g. To request the transfer of the transactions made pursuant to subparagraphs (e) and (f) to third parties to which personal data are transferred
- h. To object the occurrence of a result against himself/herself by analyzing the processed data exclusively through automatic systems
- i. To request the recovery of damages in the event of loss resulting from the unlawful processing of personal data

In the event of data subjects sending requests to our Bank related to the aforementioned rights, depending on the nature of the request, the request is concluded free of charge within the shortest period of time, or within a maximum of thirty days. Depending on the nature of the reply, however, a fee determined by the Board may be charged. If it is understood that the reason for application is arising from the fault of the Bank, the fee may be returned to the data subject.

The result of the application regarding his/her request shall be communicated to the data subject in writing or via electronic environment depending on the preference of the data subject.

Depending on the nature of the request, the Bank may reject the request by giving justifications, or may accept it. If the application is accepted, the requirements of the request shall be fulfilled by our Bank without delay.

Our Bank sends necessary warnings to and informs our employees on the fact that the data subject has a right to petition to the Board within thirty days if the application of data subject is rejected, he/she finds the answer inadequate or the application is not duly responded.

## **12. OTHER ISSUES**

The amendments to the Policy and the necessary works to put such changes into effect are carried out in accordance with the resolutions of the Personal Data Protection Committee, and amendments shall be put into effect by the resolutions of the Board of Directors of our Bank.

The Policy shall be reviewed regularly once a year. However, if necessary, our Bank reserves the right to review, update, modify or abrogate this Policy and create a new policy, in a shorter period of time.

The Board of Directors of our Bank has the authority to decide on the abolition of the Policy.

## **13. ENFORCEMENT**

**13.1.** This Policy has been adopted by the Board of Directors decision dated 25/12/2024 and numbered 43/41.

**13.2.** The Personal Data Protection Committee executes the provisions of this Policy on behalf of the Board of Directors.

**13.3.** With the enforcement of this Policy, Türkiye Halk Bankası A.Ş. Personal Data Protection and Processing Policy adopted by the Decision of the Board of Directors dated 17/10/2023 and numbered 38/26 is hereby revoked.