HALKBANK

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

## CONTENTS

1. PURPOSE AND BASIS……2
2. SCOPE……..……2
3. DEFINITIONS……..2
4. PROCEDURES FOR PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA.....3
5. ACTIONS ON EMPLOYEES INVOLVED IN THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA.....4
6. ACTIONS ON ENVIRONMENTS WHERE SPECIAL CATEGORIES OF PERSONAL DATA IS PROCESSED, MAINTAINED AND/OR ACCESSED....5
7. ACTIONS REQUIRED TO BE TAKEN FOR THE TRANSFER OF SPECIAL CATEGORIES OF PERSONAL DATA.....7
8. MISCELLANEOUS ....……..8
9. EFFECT ……....8

ANNEX 1: Necessity Test
ANNEX-2: Form of Authorization Access Matrix for Employees Accessing Sensitive Personal Data (Authorization Access Matrix)

## 1. PURPOSE AND BASIS

The purpose of the policy is to lay down procedures and guidelines for establishing and implementing technical and administrative actions for the processing of sensitive personal data as defined in article 6/1 of the Law numbered 6698 on the Protection of Personal Data (LPPD) and ensuring the appropriate level of safety for its processing.

This policy has been formulated based on the LPPD and secondary legislation for LPPD, including the decisions of the Board for Protection of Personal Data concerning the processing of sensitive personal data.

## 2. SCOPE

This Policy applies to sensitive personal data related to all Bank employees, prospective employees, service providers, visitors, customers, prospective customers, and other third parties and systems, applications, services, and processes whereby such data is processed.

This Policy applies to the processing of sensitive personal data for which the Bank is the data controller.

## 3. DEFINITIONS

**Bank:** Türkiye Halk Bankası A.Ş.,

**PDP 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,

**Account:** Cookies used for accessing the Bank's systems, resources, software, databases, and applications,

**Data Subject:** Natural person whose personal data is processed,

**User:** Any person or persons who have an account,

**Process Owner:** The unit that establishes and manages the process whereby the personal data is processed,

**Decision:** The Board's decision entitled "Adequate Actions Required To Be Taken by Data Controllers for Processing of Sensitive Personal Data" which was promulgated in the Official Gazette on 31.01.2018 with Decision number 2018/10,

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

**Sensitive 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,

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

**Policy:** Sensitive Personal Data Protection and Processing Policy of Türkiye Halk Bankası A.Ş.

**Role:** Identification data provided for obtaining additional functions for applications

## 4. PROCEDURES FOR PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

The Bank may process sensitive personal data under the fundamental guidelines outlined in the LPPD and based on legal reasons outlined in the LPDD and secondary regulations.

### 4.1 Fundamental Guidelines for the Processing of Sensitive Personal Data

**4.1.1** Sensitive personal data may only be processed for a specific, explicit, and legitimate purpose. Thus, the first thing that should be done is to define the purpose for which sensitive personal data will be processed.

**4.1.2** The processing of sensitive personal data shall be related to the defined purpose and be limited and proportional. It must be necessary to process such sensitive personal data for attaining the purpose identified. The processing of sensitive personal data which is not related to the achievement of the purposes or not needed in that context must be avoided.

**4.1.3** The principle of compliance with the law and integrity that should be taken as a basis for any action to be taken concerning sensitive personal data includes, but is not limited to, the following:

- The processing of sensitive personal data must be based on a legitimate ground,
- Sensitive personal data should not be used in a manner leading to adverse effects on individuals without a legitimate ground,
- Sensitive personal data should be processed transparently and individuals should be informed accordingly,
- Sensitive personal data should be processed in line with the reasonable expectations and predictions of individuals

among other examples.

Processed sensitive personal data should be accurate and current if necessary. Channels that will ensure that data related to the data subject is accurate and current will be established and kept open based on that principle.

Sensitive personal data that is no longer current and accurate shall be treated under the procedures and guidelines of the Bank's Policy on Storage and Destruction of Personal Data and the Regulation on Deletion, Destruction, or Anonymization of Personal Data.

**4.1.4** Sensitive personal data should be stored for a period defined in the applicable legislation or required for the purpose for which it has been processed. If there is a period stipulated in the applicable legislation for the storage of data, such period should be observed. If there is no such period, data shall be stored for a period required for the purpose for which it is processed. The period needed for processing will be fixed by the process owner and specified in the Inventory for Processing Personal Data.

## 4.2 Legal Reasons for the Processing of Sensitive Personal Data

### 4.2.1 Processing due to the provisions of the legislation

On the condition that adequate measures determined by the Board have been taken, in cases stipulated by the legal legislation, the special categories of personal data of the data subject other than those related to health and sexual life may be processed without the explicit consent of the data subject following LPPD provisions. In this case, the data processing activities to be performed by Halkbank are limited to the requirements of the provisions of the reference legislation.

### 4.2.2 Processing of sensitive personal data related to health and sexual life;

As a requirement of the PDPL, the data processing of special categories of personal data related to health and sexual life is subject to explicit consent. In the event of no such explicit consent being granted, it is regulated that such personal data may be processed only by those under a confidentiality obligation or authorized agencies and institutions and only for the protection of public health, executing preventive medicine, medical diagnosis, treatment and care services, the planning and management of health services, and their financing.

In cases covered by the confidentiality obligation in line with the provisions of the applicable legislation, the special categories of personal data regarding the health of the persons may be processed by the Bank to the extent required by the provisions of this legislation.

### 4.2.3 With the explicit consent of the data subject.

If any of the above-mentioned special categories of personal data processing conditions are not available for the processing of the special categories of personal data, the explicit consent of the data subject may be requested by Halkbank. In such cases, the special categories of personal data of the data subject may be processed by Halkbank after informing (of the need for the person's explicit consent) and obtaining his/her explicit consent (limited to this issue).

### 4.2.4 Sufficient measures must have been taken in the processing of sensitive personal data

Taking the steps determined by the Board as a requirement of the PDPL is obligatory related to the sensitive personal data to be processed. Halkbank shall process sensitive personal data in line with the measures determined by the Board. The monitoring of the security measures to be determined by the Board within this scope, and the inclusion of these measures in Halkbank's business processes, is carried out by the PPD Committee.

## 5. ACTIONS ON EMPLOYEES INVOLVED IN THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

### 5.1 Training for Employees and Awareness Raising Activities

Halk Academy Department will ensure that the employees receive regular training on LPPD and related legislation on security of sensitive personal data based on coordination/decisions of the PPD Committee.

### 5.2 Confidentiality Agreements

The manager of the unit to whom the user reports will sign confidentiality agreements with employees who are/will be involved in the processing of sensitive personal data based on coordination/decisions of the PPD Committee and notify them to the Human Resources Department.

### 5.3 Scope, Term, and Supervision of Authorization to Access Sensitive Personal Data

**5.3.1** The scope and term of the authorization to access sensitive personal data, which should be limited to the operations carried out by users under their job descriptions should be expressly defined and limited according to the Policy on Protection and Processing of Personal Data of T. Halk Bankası A.Ş. and other applicable legislation. User accounts/roles/authorization will be defined for defining authorization and responsibilities based on such restrictions and coordination/decisions of the PPD Committee and authorizations are subjected to periodical controls. An authorization granted to any employee who has been transferred to another position or resigned and/or discharged because of any reason should be promptly withdrawn and items in the inventory containing sensitive personal data should be returned.

The Internal Control Department and the Inspection Board will verify if user accounts/role/authorization definitions conform with the Bank's job descriptions.

**5.3.2** A Necessity Test (ANNEX-1) will be conducted in line with requirements for processing to ensure that sensitive personal data is processed under LPPD, the Bank's Policy on Protection and Processing of Personal Data, and other applicable legislation and each processing activity will be assessed by the process owner(s). Necessary actions will be taken after the assessment.

**5.3.3** Sensitive personal data laid down in the Policy will be processed by employees authorized to access sensitive personal data subject to coordination by the PPD Committee and following access and authorization processes applicable to access to the Bank's applications, software and hardware, networks, and the Internet. (ANNEX-2 Form for Access Authorization Matrix)

## 6. ACTIONS ON ENVIRONMENTS WHERE SPECIAL CATEGORIES OF PERSONAL DATA IS PROCESSED, KEPT AND/OR ACCESSED.

### 6.1 Electronic Media

**6.1.1 Storage of sensitive personal data by using cryptographic methods:**

Responsibility for the safeguarding of electronic media whereby sensitive personal data is processed, stored, and/or accessed

- by using cryptographic methods conforming with the Bank's Data Security Standards

- rests with the Infrastructure Operation and Management Department if the encryption method suited to the Service is provided via technical infrastructure,
- If the appropriate method is based on software, responsibility for developing and managing codes and related software within the Bank, for software developed outside of the Bank, responsibility for providing coordination rests with the Software Development Department or the Department for Management of Technological Architecture.

- If sensitive personal data is required to be transferred to a cloud environment according to the applicable Banking Legislation, the Department for Operation and Management of Infrastructure will be establishing a technical infrastructure and providing support for the encryption and transfer of sensitive personal data.

- The encryption process in question should be established by the Department for the Operation and Management of Infrastructure if the encryption is provided through technical infrastructure or by the Software Development Department if it is provided in the form of software and the responsibility for providing coordination for ensuring continuity and necessary arrangements will rest with the Information Technologies Departments involved in the operation of the process.

**6.1.2** **Cryptographic keys:** The Department for the Operation and Management of Infrastructure will separately determine cryptographic encryption keys to be created as a result of cryptographic encryption in each location, store them in safe and different media, ensure their safety, and control and regulate them and the Information Technologies Departments involved in the operation of the process will provide coordination to ensure that they are used in a manner consistent with the process and their continuity and necessary regulations are achieved.

**6.1.3** **Log records:** The Information Technologies Departments involved in the operation of the process will ensure that all actions taken concerning sensitive personal data in electronic media or systems whereby sensitive personal data is processed, stored, and/or accessed are logged properly and the Department for the Operation and Management of Infrastructure will be responsible for their safe storage; and the Information Technologies Departments involved in the operation of the process will provide coordination for ensuring the continuity of the logging processes in question and their storage.

**6.1.4** **Safety updates, tests, and records for the media containing data:** The Department for the Operation and Management of Infrastructure will constantly monitor security updates for the media containing sensitive personal data and regularly perform necessary security tests. The providers of information technology services are responsible for requesting security tests after major structural modifications or new commissioning of services and addressing all information security findings regarding the services.

**6.1.5** **Accessing data through a software:** If a software is used for accessing sensitive personal data stored in electronic media or systems whereby sensitive personal data is processed, stored and/or accessed;

- The unit charged with granting authorization will grant authorization to the users of such software with coordination provided by the process owner(s) and the Internal Control Department and the Inspection Board will check if the authorizations are in conformity with the Bank's job descriptions.

- The Department for Operation and Management of Infrastructure is responsible for providing coordination to ensure that the security tests for such software are regularly conducted and necessary controls and arrangements are made for such security tests.

- The Department for Operation and Management of Infrastructure is responsible for providing coordination to ensure that the results of the security tests for the software are recorded, controlled and necessary arrangements are made.

**6.1.6 Remote access to data:** If remote access to sensitive personal data stored in electronic media whereby sensitive personal data is processed, stored, and/or accessed is necessary, the Department for Operation and Management of Infrastructure shall provide an identity verification system consisting of at least two stages and provide coordination for controlling the identity verification system and making necessary arrangements.

### 6.2 Physical Environments

**6.2.1 Security precautions to be taken depending on the nature of the environment where sensitive personal data is maintained:** The Department for Support and Procurement Services is responsible for taking adequate security measures against electric leakage, fire, inundation, and burglary depending on the nature of the environment where sensitive personal data is processed, stored and/or accessed.

**6.2.2 Ensuring physical security of environments where sensitive personal data is maintained and prevention of unauthorized access:** The Department for Support and Procurement Services is responsible for ensuring the physical security of the physical environments where sensitive personal data is processed, stored, and/or accessed and preventing unauthorized access.

## 7. ACTIONS REQUIRED TO BE TAKEN FOR THE TRANSFER OF SPECIAL CATEGORIES OF PERSONAL DATA

### 7.1 Transfer via Email

If sensitive personal data needs to be transferred via email, it must be encrypted and transferred via an organizational email address or Registered Electronic Mail (REM).

The Department for the Operation and Management of Infrastructure is responsible for the provision of technical infrastructure for transferring sensitive personal data via email and the process owner(s) will be responsible for transferring them by using the technical infrastructure.

### 7.2 Transfer via External Memory Storage Products

If sensitive personal data needs to be transferred via media such as portable memory (USB, etc.), external disks, CDs, and DVDs, they must be encrypted by using cryptographic methods.

The business unit which has developed data is responsible for encrypting sensitive personal data by using cryptographic methods and the Department for the Operation and Management of Infrastructure will provide the encryption infrastructure.

When sensitive personal data is transferred via media such as portable memory (USB, etc.), external disks, CDs, and DVDs, cryptographic keys used for encrypting them by employing cryptographic methods should be kept in different media.

Keeping cryptographic keys used for encrypting them by employing cryptographic methods in different media is a responsibility assigned to the Department for the Operation and Management of Infrastructure.

### 7.3 Transfer between Servers

If sensitive personal data is transferred between servers in different physical environments, data should be transferred by establishing a VPN between the servers or using sFTP method. Responsibility for providing infrastructure and support for data transfer rests with the Department for the Operation and Management of Infrastructure and the process owner(s) is responsible for transferring data through that infrastructure.

### 7.4 Transfer on Paper

If sensitive personal data needs to be transferred on paper, necessary precautions should be taken against risks such as the theft or loss of paper or access by unauthorized persons and the document must be sent in the format of "classified document".

The process owner(s) must ensure that sensitive personal data is sent to the Department for Support and Procurement Services so that it can be forwarded to the party concerned and the Department for Support and Procurement Services is responsible for forwarding the documents.

## 8. MISCELLANEOUS

The PPD Committee must ensure that the updated version of the policy is communicated/notified to the Bank's employees, which will be coordinated by the Branch Operations Department/Department for Coordinating Consumer Relations.

The Bank shall engage any software/systems/applications needed for the fulfilment of requirements of the Policy and the PPD 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.

The Internal Control Department and the Inspection Board are responsible for verifying that the requirements outlined in this policy have been met as per the Policy.

## 9. EFFECT

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

**9.2** This Policy shall enter into effect upon the date of its adoption by the Board of Directors.

**9.3** Implementation of the Policy shall be coordinated by the top management of the Bank's service units and the PPD Committee.

**9.4** The provisions of this Policy shall be executed by the Branch Operations Department/Department for Coordinating Consumer Relations and the PPD Committee.

ANNEX-1

**Whit is the objective intended to be achieved in the process involving processing of personal data?**

## OBJECTIVE

**Is it legally permitted to achieve the intended objective?**

**YES**

Is it necessary to process personal data to reach the intended objective?

**NO**

Stop the processing of personal data*

**IT IS NECESSARY**

What groups of people and data categories are necessary?

**IT IS NOT NECESSARY**

Stop the processing of data*

**AFTER IT HAS BEEN DETERMINED**

Is the quantity of personal data processed higher than that necessary for achieving the intended objective?

**YES**

Stop the data processing activity for unnecessary data.*

**NO**

Is there a reason for the lawfulness of the processing of personal data?**

**YES**

The necessity test has been completed.

**NO**

Stop the processing of data*

ANNEX-1

* If the processing of personal data has been stopped according to the necessity test, such personal data shall be subjected to destruction for that specific process.

**** Reasons for the lawfulness of the processing of personal data;**

- Explicitly envisaged in the Laws,
- It is necessary for the protection of the life or bodily integrity of a person or other who is unable to give his or her consent or whose consent is legally invalid,
- It is 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
- Necessary for compliance with a legal obligation to which the data controller is subject
- When the relevant information is revealed to the public by the data subject herself/himself
- When necessary for the institution, usage or protection of a right
- It is necessary to process data for the sake of the legitimate interests of the data controller provided that it is not prejudicial to the fundamental rights and freedoms of the data subject.
- With the explicit consent of the data subject.

**Reasons for the lawfulness of processing of sensitive personal data;**

Sensitive data except for health and sexual life;

- Explicitly envisaged in the Laws,
- With the explicit consent of the data subject.

Data of special nature related to health and sexual life;

- Processing by authorized institutions and organizations and by persons under obligations to keep such information confidential for planning and managing protection of public health, preventive medicine, medical diagnosis, the carrying out of treatment and care services and their funding.
- With the explicit consent of the data subject.

**Form of Authorization Access Matrix for Employees Accessing Sensitive Personal Data** ANNEX-2

| Item no | ORGANIZATIONAL UNIT / System/Implementation Environment/Data Subject/Personal Data Used | THE DEPARTMENT FOR MANAGEMENT OF ASSETS AND LIABILITIES | THE DEPARTMENT FOR THE OPERATION AND MANAGEMENT OF INFRASTRUCTURE | THE DEPARTMENT FOR INDIVIDUAL MARKETING | THE BUDGET AND REPORTING DEPARTMENT | … |
|---|---|---|---|---|---|---|
| 1 | CUSTOMER - IDENTITY DETAILS in ALPERA | Not accessing | Not accessing | Not accessing | Not accessing | … |
| 2 | EMPLOYEE - ADDRESS DATA in HALKPORTAL | Not accessing | Not accessing | Not accessing | Not accessing | … |
| 3 | EMPLOYEE - FINANCIAL DATA in VEHICLE TRACKING SYSTEM | Not accessing | Not accessing | Not accessing | Accessing | … |
| 4 | CUSTOMER - CUSTOMER DATA in APPRAISAL APPLICATIONS | Not accessing | Not accessing | Accessing | Not accessing | … |
| 5 | CUSTOMER - IDENTITY DETAILS in CRM | Not accessing | Not accessing | Not accessing | Not accessing | … |
| 6 | EMPLOYEE, CUSTOMER - IDENTITY DATA in File Server | Not accessing | Not accessing | Not accessing | Not accessing | … |
| 7 | CUSTOMER - CARD DATA in Banksoft (DEBITCARD) | Not accessing | Not accessing | Not accessing | Not accessing | … |
| 8 | EMPLOYEE - HEALTH DATA, SENSITIVE PERSONAL DATA in archive | Not accessing | Not accessing | Not accessing | Not accessing | … |
| 9 | CUSTOMER - COMMUNICATION DATA in BDDK WEB SERVICE | Not accessing | Not accessing | Not accessing | Not accessing | … |
| 10 | NON-CUSTOMER NATURAL PERSON - IDENTITY DATA in FINDEKS | Not accessing | Not accessing | Not accessing | Not accessing | … |
| 11 | CUSTOMER - ACCOUNT DATA in Batch (PVDSI560-561-601) | Not accessing | Not accessing | Not accessing | Not accessing | … |
| 12 | SURETY - FINANCIAL DATA in other media | Not accessing | Not accessing | Accessing | Not accessing | … |
| 13 | … | … | … | … | … | … |
| 14 | … | … | … | … | … | … |
| 15 | … | … | … | … | … | … |

(*) Information on units and data is given as an example