DIRECTIVE ON TAKASBANK PERSONAL DATA PROTECTION POLICY

REVISION HISTORY OF THE DOCUMENT				
Ver. No	Date	Prepared/ Revised by	Approved by	Description
V1.0	29/03/2018	Legal Consultancy	Board of Directors	Issuance of Takasbank Personal Data Protection Policy
V2.0	27/11/2019	Legal Consultancy	Board of Directors	Revision
V3.0	07/09/2021	Legal Consultancy	Board of Directors	Periodic review (no revisions)
V4.0	29/07/2022	Legal Consultancy	Board of Directors	Addition of the Data Breach Notification and Crisis Management Plan to the Directive
V5.0	25/11/2022	Legal Consultancy	Board of Directors	It has been updated in accordanc e with the changes made in the B ank's organizational structure.
V6.0	26/03/2025	Legal Consultancy	Board of Directors	An update has been made based on the amendment made in the Personal Data Protection Law No. 6698.

TABLE OF CONTENTS

DIRECTIVE ON
TAKASBANK PERSONAL DATA PROTECTION POLICY

CHAPTER ONE
Purpose, Scope, Basis, Definitions and Abbreviations

ARTICLE 1- Purpose

(1) The purpose of this Directive is to set forth the purposes, methods and the underlying legal reasons of the processing of personal data processed by Takasbank in accordance with the legislation on protection of personal data; to indicate the periods for storage of personal data and the security measures taken for their protection and to lay down the principles regarding the applications to be made by Data Subjects.
(2) Takasbank takes all the necessary measures in order to fulfil the obligations imposed on it under the legislation on protection of personal data and hereby sets forth the principles and procedures regarding such measures to be taken.

ARTICLE 2- Scope

(1) This Directive covers all personal data processed by Takasbank whether by automated means, in part or in whole, or non-automated means that are a part of any data recording system.
(2) Processing of personal data means any operation or set of operations that is performed upon personal data, including, without limitation, any collection, recording, storage, preservation, alteration, revision, disclosure, transfer, acquisition, retrieval, classification or blocking the use of such data.
(3) This Directive contains the explanations for fulfilment of the obligations imposed on the data controller under the legislation on protection of personal data.

ARTICLE 3-Basis

(1) This Directive has been prepared on the basis of the "Law no. 6698 on Protection of Personal Data", the "Regulation on Erasure/Deletion, Destruction or Anonymizing of Personal Data" and the "Regulation on Data Controllers' Registry".

ARTICLE 4- Definitions and abbreviations

(1) For the purposes of this Directive, the following terms used herein shall have the following meanings:

a. **Board:** means the Personal Data Protection Board;
b. **Candidate Personnel:** means the person that has made a job application to Takasbank;
c. **Data Subject:** means the natural person whose personal data are processed;
d. **Destruction Regulation:** means the Regulation on Erasure/Deletion, Destruction or Anonymizing of Personal Data which was published in the Official Gazette no. 30224 dated 28 October 2017;
e. **Inventory:** means Takasbank Personal Data Processing Inventory established and detailed by Takasbank by way of associating its personal data processing activities dependent on their business processes with personal data processing purposes, data categories, recipient groups and data subject groups and elaborating the maximum period of time necessary for the purposes of processing of personal data, the personal data planned to be transferred to foreign countries and the measures taken in relation to data security;
f. **Investor:** means the customers of Takasbank members.
g. **Law:** means the Law no. 6698 on Protection of Personal Data dated 24 March 2016 which was published in the Official Gazette no. 29677 dated 7 April 2016;
h. **Member:** means Takasbank customer executing transactions in the markets served by Takasbank;

i. **Personnel:** means the person that is employed by Takasbank with an employment contract;

j. **Registry Regulation:** means the Regulation on Data Controllers' Registry published in the Official Gazette no. 30286 dated 30 December 2017;

k. **Related User:** means the persons or business units that process personal data within Takasbank's organization or with the authority and direction of Takasbank, except for the person/s or unit/s responsible for the technical storage, protection and backup of data;

l. **REM:** means registered electronic mail;

m. **Supplier:** means the person providing goods and services in accordance with the agreement concluded with Takasbank;

n. **Takasbank:** means İstanbul Takas ve Saklama Bankası A.Ş. (Istanbul Settlement and Custody Bank, Inc.);

o. **Third Person:** means the person that has entered into a legal relationship with Takasbank without establishing a direct contractual relationship.

CHAPTER TWO
Principles and Basic Concepts

ARTICLE 5- Principles

(1) Takasbank processes personal data in compliance with the principles and procedures specified in the legislation on protection of personal data.
(2) Takasbank processes the personal data related with its activities that it conducts in accordance with article 4 of the Law and within the framework of the following principles;

a. Lawfulness and conformity with rules of bona fides;

b. Accuracy and being up to date, where necessary;

c. Being processed for specific, explicit and legitimate purposes;

d. Being relevant with, limited to and proportionate with the purposes for which they are processed;

e. Being retained for the period of time stipulated by the relevant legislation or required for the purpose for which they are processed.

(3) This Directive lays down the principles and procedures regarding the implementation of the aforementioned principles by Takasbank. Takasbank takes the measures necessary for submission of the text of this Directive and the revisions to be made therein to the Data Subjects for information purposes.
(4) Takasbank processes the personal data during its activities within the framework of the principles indicated herein and based on one or more of the reasons specified in article 6 of this Directive.

ARTICLE 6-Conditions for processing of personal data

(1) Takasbank may process personal data without seeking the explicit consent of the Data Subjects within the framework of the lawfulness reasons specified in article 5 of the Law.
(2) Accordingly, Takasbank;

f. shall process personal data in cases where it is clearly provided for by the laws and it is mandatory for the performance of Takasbank's legal obligations, providing that such processing shall be limited with the content specified in the legislation.

g. shall process the personal data that are directly related to the conclusion and fulfilment of the contract.

h. shall process the personal data related with the cases where it is mandatory for protection of legitimate interests of Takasbank, providing that such processing shall not violate the fundamental rights and freedoms of the Data Subjects.

i. may process personal data for the establishment, exercise or protection of any right.

j. shall process the personal data made available to the public by the Data Subject himself/herself.

k. may process personal data within the framework specified in the Law in cases of actual impossibility.

(3) Special personal data cannot be processed except within the scope of Article 6, paragraph 3 of the Law.

ARTICLE 7-Informing the data subjects

(1) It is essential for Takasbank to exactly inform the Data Subjects about the purposes of personal data processing, the purposes of transfer of personal data and the recipient groups, the method and legal reasons of collection of personal data, and the rights of the Data Subject.
(2) The regulations specified herein shall apply for informing of the Data Subjects about the issues specified in the 1st paragraph. In addition, the methods entailing provision of satisfactory information at the time of processing of personal data are also used.
(3) Takasbank provides any and all facilitating means allowing Data Subjects to exercise their rights. Takasbank especially takes the necessary measures in order to provide urgent and satisfactory responses to the applications that will be made by Data Subjects.
(4) Takasbank erases, destroys or anonymizes, ex officio or upon demand, the personal data following disappearance of the reasons which require the processing of such data pursuant to 1st paragraph of article 7 of the Law. The regulations regarding fulfilment of this obligation are provided in the Procedure on Takasbank Personal Data Retention and Destruction Policy.

ARTICLE 8-Purposes of processing of personal data

(1) Personal data are processed by Takasbank for the following purposes within the framework of the conditions in Article 6 herein:

a. Processing of the personal data required and/or needed for the services and subsidiary activities provided and conducted in accordance with the banking legislation, payment and security settlement systems legislation and capital markets legislation;

b. Processing of the personal data required and/or needed in order to conduct the activities;

c. Processing of the personal data required and/or needed in order to conduct the personnel-related processes;

d. Processing of the personal data for the exercise of the rights granted to the personnel;

e. Processing of the personal data for protection of the rights of third persons;

f. Processing of the personal data required by the activities conducted with suppliers and third persons;

g. Processing of the personal data for the purpose of monitoring Takasbank's business processes;

h. Processing of the personal data required and/or needed in order to conduct information security processes;

i. Processing of the personal data required and/or needed for performance of audit and control activities and risk assessments;

j. Processing of personal data in line with the requests of legal authorities and other public institutions;

k. Processing of personal data in order to ensure the security of the physical environment;

l. Processing of personal data for the purpose of protection of the legitimate interests of Takasbank.

(2) Articles 21 and 22 herein set forth the methods and legal reasons of collection of personal data by Takasbank in relation to the purposes listed in this article.

CHAPTER THREE

Categories of Personal Data

ARTICLE 9- Data subject categories

(1) Takasbank classifies the personal data that it processes according to Data Subject groups.
(2) The personal data processed within the organization of Takasbank are classified according to the common properties of natural persons. Accordingly, personal data are classified according to the Data Subject categories such as personnel, trainee, candidate personnel, shareholder, board member, member, investor, supplier, third person, project stakeholders, visitors, etc.

ARTICLE 10-Classification of personal data

(1) Takasbank associates the personal data that it processes within the scope of its activities with the purposes of processing of personal data, data categories, recipient groups and data subject groups; enters into Takasbank Personal Data Processing Inventory the maximum period of time required for the purposes of processing of personal data, the places to which such data are transferred and the measures taken for data security and keeps such Inventory updated.
(2) Takasbank classifies the personal data that it processes within the scope of its activities in detail based on the Inventory.
(3) Personal data are classified according to their properties, privacy levels, data subject groups, purposes of processing and types of activities.
(4) Classification of personal data and ensuring the confidentiality and security of such data according to such classifications are ensured within the framework of Takasbank's relevant internal legislation.

CHAPTER FOUR

Transfer of Personal Data

ARTICLE 11- Transfer of personal data at home and purposes of transfer

(1) Takasbank may transfer the personal data held in its possession to another data controller at home without obtaining explicit consent of the Data Subject in cases specified in article 6 herein.
(2) Takasbank's purposes of transfer of personal data include the fulfilment of the duties defined in the legislation and provision the services and activities rendered and conducted by it in line with the processing purposes specified in Article 8 herein.
(3) In this context, in terms of fulfilment of the duties defined by applicable laws, personal data may be transferred to regulatory – supervisory authorities and other public agencies or institutions providing that such transfer shall be limited with the content specified in the relevant legislation.
(4) In terms of provision of services and conducting of activities, personal data may be transferred to private persons, providing that such transfer shall be limited with such services and activities.
(5) For any other transfers not included within the scope herein, explicit consent of the Data Subject is obtained by Takasbank.

ARTICLE 12-Transfer of personal data abroad and purposes of transfer

(1) Takasbank may transfer the personal data held in its possession to another data controller abroad without explicit consent of the Data Subject in cases specified in article 6 herein.
(2) Takasbank's purposes of transfer of personal data abroad are the provision of its services and the conducting of its activities.

(3) In the absence of an adequacy decision and if any of the appropriate safeguards stipulated in the fourth paragraph of Article 9 of the Law cannot be provided, personal data may be transferred abroad if one of the following situations exists.

a. If the relevant person gives explicit consent to the transfer, provided that he/she is informed about the possible risks.

b. If data transferring is mandatory for the performance of a contract between the relevant person and the data controller or for the implementation of pre-contractual measures taken upon the request of the relevant person.

c. ıf data transffering is mandatory for the establishment or performance of a contract between the data controller and another natural or legal person for the benefit of the relevant person.

d. If data transferring is mandatory for a superior public interest.

e. If data transferring is necessary for the establishment, exercise or protection of any right.

f. If it is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.

g. If Transfer from a registry open to the public or to persons with a legitimate interest, provided that the conditions required for accessing the registry in the relevant legislation are met and the person with a legitimate interest requests it.

(4) While determining the conditions for transfer of personal data abroad, the matters in the third paragraph of Article 9 of the Law and the third paragraph of Article 73 of the Banking Law No. 5411 are taken into consideration.

CHAPTER FIVE

Data Security Measures

ARTICLE 13- Measures to prevent unlawful processing of data

(1) Takasbank defines the business processes in the areas that it serves and operates in and the data to be processed during such processes in a comprehensive and detailed manner using the methods specified in article 21 herein. It takes necessary administrative measures in order to prevent the processing of data beyond such definitions.

(2) Takasbank ensures that necessary technical arrangements are made in this context. To this effect, it employs expert personnel and assures the specialization level of such personnel through continuous improvement processes.

(3) Personal data are processed subject to the aforementioned technical and organizational processes. It is ensured that the minimum amount of personal data required by the activity conducted is processed. The Related Users within the organization of Takasbank may not process personal data except for the specified processes and defined rules.

(4) The processes specified herein in relation to personal data are controlled by the process owners at first level and by IT Information Security and Risk Management Team and Internal Control and Compliance Unit at second level. The third-level control is ensured by the Internal Control Unit considering the Annual Internal Audit Plan and risk analyses.

(5) Takasbank is subject to the audits conducted by BRSA, CMB, CBRT and the other relevant supervisory and regulatory authorities as well as independent audit.

ARTICLE 14-Measures to prevent unlawful access to personal data

(1) Takasbank makes the Related User definitions for its business units and personnel; and identifies their Powers and responsibilities. Takasbank regulates in detail the business processes in the areas that it serves and operates in and the access rights of its business units during such processes. No Related User may have access to any data beyond their authorization.
(2) Takasbank takes the necessary organizational and technical measures to allow every business unit to have access to minimum sufficient data for provision of service/s.
(3) The explanations provided in paragraphs 4, 5, and 6 of article 13 herein shall also apply for this article.

ARTICLE 15-Measures for protection of personal data

(1) At Takasbank, all data are protected within the framework of information security policies. Takasbank takes additional measures for protection of personal data. The issues related to protection of special categories of personal data are regulated in Takasbank Procedure on the Security of Special Categories of Personal Data.
(2) Takasbank takes necessary organizational measures for protection of personal data. In this context, Takasbank;
   a. defines all personal data that it processes in the Inventory and regularly updates it. The roles and responsibilities related with creation of the inventory and keeping it updated are specified with the related procedures.
   b. develops policies for protection of personal data and/or revises the current information security policies properly to incorporate the protection of personal data.
   c. ensures the security of all media used for storage of personal data; and fulfils the legal requirements in this context.
   d. The processes specified herein in relation to personal data are controlled by the process owners at first level and by IT Information Security and Risk Management Team and Internal Control and Compliance Unit at second level. The third-level control is ensured by the Internal Control Unit considering the Annual Internal Audit Plan and risk analyses.
   e. The possible risks that may threaten the protection of personal data and the extent of their impacts are added to the risk definitions that will be entered by the process owners into Takasbank's operational risk database.
   f. defines the communication processes related with protection of personal data.
   g. periodically conducts awareness-raising trainings; and monitors the processes related with protection of personal data in a centralized manner.
   h. fulfills its other obligations arising from the legislation on protection of personal data.

(3) In addition, Takasbank also takes the following measures:
   a. Performs risk analysis related with information systems. The risk analysis is repeated at least once a year or in case of major changes or revisions that can be made in the information systems.
   b. Information systems are subjected to penetration testing performed at least once a year by the natural or legal persons with national or international certification in the field of penetration testing, which do not have any duty regarding the fulfilment of information security requirements.
   c. Information security policies and all responsibilities are reviewed and approved every year.
   d. Incidents related with information security violations are monitored and evaluated every year.
   e. The processes and procedures established for the purpose of management of risks related to information systems are deployed within the organization of Takasbank to ensure their actual functioning and their functionality is supervised and monitored duly.
   f. Information security organization and responsibilities are specified and in place.
   g. Business continuity plan is prepared in order to ensure continuity of all critical business processes according to risk priorities.
   h. All the necessary organizational and technical measures are taken against information security violations.
   i. Control processes are periodically defined.

j. Any and all necessary organizational and technical measures are taken to ensure network security.
k. Any and all necessary organizational and technical measures are taken to ensure the continuity of information systems.

ARTICLE 16-Measures regarding data processors

(1) According to the Law, data processor is the natural or legal person processing the personal data on behalf of the data controller based on the authorization granted by it.
(2) Takasbank does not process personal data except for its personnel-related data and the investor data related with the activities for which a requirement of service is stipulated on an investor basis as well as the services for which it acts as the custodian. Therefore, Takasbank does not establish any data processor relationship.
(3) The content of personal data stored in Takasbank data centers is not accessible by any person or party other than Takasbank.
(4) The information security processes at Takasbank's data centers are audited within the scope of the audits specified under banking, payment systems and capital markets legislation.

ARTICLE 17-Audit processes

(1) Takasbank is subject to various audit processes as required by the laws applicable to it. Such audits also cover the processing of personal data.
(2) The processes specified herein in relation to personal data are controlled by the process owners at first level and by IT Information Security and Risk Management Team and Internal Control and Compliance Unit at second level. The third-level control is ensured by the Internal Control Unit considering the Annual Internal Audit Plan and risk analyses. Continuous improvements are made depending on the results of such audits. In the controls related with the relevant processes, the issues specified in this Directive are taken into consideration and continuous improvement procedures are implemented.
(3) Takasbank is periodically audited by regulatory and supervisory authorities, covering also all of its processing activities related with personal data in line with the banking, payment systems and capital markets legislation. The audits cover the processes specified in paragraph 3 of article 15 herein.

ARTICLE 18-Awareness and confidentiality obligation

(1) Takasbank takes necessary measures in order to inform and train the personnel that it employs within the scope of protection of personal data. It ensures at organizational and technical level that its personnel conduct the activity of processing of personal data within the framework of the principles indicated in article 5 herein. Takasbank raises awareness on the fact that the right to protection of personal data is a fundamental right defined at Constitutional level and on the legal sanctions that may be imposed in case of violation of this right.
(2) Takasbank informs its personnel on the confidentiality obligation in general, and specifically on the obligations arising from the legislation on protection of personal data and collects commitment letters from its personnel within this scope.

ARTICLE 19-Measures to be taken in case of disclosure

(1) Takasbank warrants that in case the personal data processed by Takasbank are unlawfully acquired by others despite all the organizational and technical measures taken; Takasbank shall notify the relevant Data Subject or Data Subjects and the Board of the situation as soon as possible.
(2) Necessary measures are taken in order to ensure immediate actions to be taken in relation to such cases.

CHAPTER SIX

Retention Periods

ARTICLE 20- Periods for retention of personal data

(1) Takasbank is obliged to store the personal data that it processes during the services provided by it in a manner accessible by the related user for a period of 10 years after disappearance of the requirement to

process the personal data processed during the services that it renders under the Banking Law no. 5411 and the capital markets legislation. The Securities physically stored by Takasbank are retained for an unlimited period.

(2) The personal data processed for the reasons arising from any kind of employment contracts are stored for the minimum retention periods specified in the labour legislation.

(3) The personal data processed for any other reasons are stored for the minimum retention periods specified in the related legislation. The proper retention periods for the personal data for which no retention period is specified in the relevant legislation are determined by Takasbank.

(4) The data retention and destruction processes as required by the legislation on protection of personal data are provided in the Procedure on Takasbank Personal Data Retention and Destruction Policy.

CHAPTER SEVEN

Methods and Legal Reasons of Collection of Personal Data

ARTICLE 21- Methods of collection of personal data

(1) Takasbank collects personal data within the framework of the principles specified in article 5 herein. The primary methods for collection of personal data are as follows:

a. Takasbank collects personal data due to the contractual relationships that it establishes. In this context, it enters into the data recording system the personal data that it is obliged to collect as required by applicable laws in relation to its members' representatives, its personnel, its suppliers or the authorized persons of its suppliers.
b. Takasbank enters into the data recording system the personal data that it is required to collect under the applicable laws that it is subject to in terms of provision of its services. This covers the personal data transferred to Takasbank in relation to its members' customers.
c. Takasbank may process personal date for the purpose of protection of its legitimate interests, providing that this processing shall not violate the fundamental rights and freedoms of the Data Subject. This covers the data related with the persons that have submitted job applications to Takasbank, the personal data excluding those processed due to a legal obligation related with the relatives of Takasbank personnel, etc.
d. Takasbank may process personal data in cases where it is mandatory for protection of the rights of Data Subjects.
e. Takasbank enters into the data recording system the personal data contained in the documents sent from public authorities as well as the personal data provided at the time of any applications made to it and stores such data as required by the laws applicable to it.
f. Takasbank collects personal data for the purpose of ensuring physical security of the area that it serves.
g. Takasbank collects personal data for the purpose of ensuring the security of information systems.

(2) The other methods except for Takasbank's primary methods of collection of personal data are indicated in the Inventory.

ARTICLE 22-Legal reasons of collection of personal data

(1) The personal data collected within the framework specified in articles 6 and 21 herein are processed based on the legal reasons specified in the legislation on protection of personal data.

(2) Takasbank processes personal data on the basis of explicit consent of the Data Subject only in relation to any other issues beyond this scope.

CHAPTER EIGHT

Rights of Data Subjects and the Methods to Exercise Such Rights

ARTICLE 23- Rights of data subjects

(1) Takasbank takes any and all facilitating measures to allow Data Subjects to exercise their rights provided for in article 11 of the Law.
(2) Each person has the right to apply to Takasbank through identity verification methods and to raise any requests in relation to the following issues:
   a. To learn whether his/her personal data are processed or not;
   b. To request information about the processing if his/her personal data are processed;
   c. To learn the purpose of processing of his/her personal data and whether such data are used for intended purposes or not;
   d. To know the third persons to whom his/her personal data are transferred at home or abroad;
   e. To request for correction of personal data if they are processed in an incomplete or erroneous manner and for notification of the action taken to the persons to whom his/her personal data have been transferred;
   f. To request for deletion or destruction of his/her personal data in case the reasons necessitating the processing of such personal data cease to exist, and to request for notification of such operations done to the persons to whom personal data have been transferred;
   g. To object to the processing, exclusively by automatic means, of his/her personal data, which leads to an unfavourable consequence for the data subject.
(3) Takasbank runs the necessary processes in order to urgently respond to the request of the Data Subject that suffers a loss or damage due to the unlawful processing of his/her personal data.

ARTICLE 24-Methods to exercise the rights of data subjects

(1) In case of applications made to Takasbank, the applicant has to prove his/her identity without any doubt. This practice is required by the measures taken for protection of personal data.
(2) An application may be filed with Takasbank using the application form enclosed hereto, which may be obtained from the website of www.takasbank.com.tr or upon request, or the letter of application that will be prepared by the Data Subject himself/herself.
(3) The application may be submitted in writing or via the registered electronic mail (REM) or by using the electronic mail address previously notified by the Data Subject to Takasbank and already registered in Takasbank system:
   a. **Application in Person:**
   An application may be submitted in person to the address of İstanbul Takas ve Saklama Bankası A.Ş. Reşitpaşa Mahallesi, Borsa İstanbul Caddesi, No:4 Sarıyer 34467 Istanbul using the originally-signed application form or the letter of application to be prepared to this effect. It is mandatory to verify identity at the time of application. The applicant's representative/attorney may also submit an application to the same address in person. In case of applications filed via an attorney, it is required to present the original power of attorney containing the authorization granted in relation to the personal data request.
   b. **Application via Mail:**
   The applicant may send the originally-signed application form or the letter of application that the applicant will prepare to the address given above. The applicant's attorney may also send an application via mail together with the original power of attorney containing the authorization granted in relation to personal data request. In case of an application via mail, *"KVKK Kapsamında Bilgi Talebi" (Information Request under the Law on Protection of Personal Data)"* must be written on the envelope.
   c. **Application via a Notary:**
   A notification may be sent to the address given above via a notary, or filed in person or by means of an attorney. In case of such an application, the method through which the applicant wants to receive the response to be given by Takasbank must be specified. *"KVKK Kapsamında Bilgi Talebi" (Information*

Request under the Law on Protection of Personal Data)" must be written in the subject field of the notification.

d. **Application via Registered Electronic Mail:**
An e-mail may be sent to the address of takasbank.haberlesme@hs03.kep.tr. If the Data Subject does not request otherwise, the response to be given by Takasbank shall be notified to the applicant's REM (registered electronic mail) address. *"KVKK Kapsamında Bilgi Talebi" (Information Request under the Law on Protection of Personal Data)"* must be written in the subject field of the e-mail sent.

e. Application via Electronic Mail:
If there is an electronic mail address previously notified by the Data Subject to Takasbank and already registered in Takasbank system; application may be sent using such e-mail address. *"KVKK Kapsamında Bilgi Talebi" (Information Request under the Law on Protection of Personal Data)"* must be written in the subject field of the e-mail sent.

(4) Pursuant to paragraph 2 of article 5 of the Communiqué on the Principles and Procedures regarding the Application to the Data Controller as published by the Board, the applications to be made must contain the following information:
   a. Name, surname, and, signature if the application is made in writing;
   b. Turkish identity number for the citizens of the Republic of Turkey, and the nationality, passport numbers or identity numbers, if any, for foreigners;
   c. Place of residence or workplace address as the address for correspondences;
   d. Electronic mail address, telephone and fax number for correspondences, if any;
   e. Subject matter of the request.

   In addition, Takasbank reserves its right to request for additional documents for identity verification.

(5) Out of the issues specified in article 23 herein, the issue or issues that the application is related with must be specified and the request must be clearly described.

(6) The response to be given by Takasbank to the application may be either received by the applicant or his/her attorney against signature at the address specified above or sent to the applicant's address via mail, or to the applicant's REM address, or via electronic mail if the Data Subject's electronic mail address has been previously notified and already recorded in Takasbank system. In case of delivery by hand, the applicant may be informed that the response is ready for delivery via the means of communication preferred by the applicant. The applicant may specify the notification method that s/he prefers in the application form. If no method is specified, the application shall be responded to through the method the application is made. Except for those specified above, no information and documents containing personal data should be provided in the applications unless requested otherwise and as long as it is not mandatory for making the application.

(7) Takasbank reminds that applications must be firstly made to the data controller pursuant to paragraph 2 of article 14 of the Law. The Data Subject has the right to apply to the Board following such application made.

ARTICLE 25-Evaluation of the requests of data subjects

(1) Takasbank may, before responding, request for additional information in order to respond to the application.

(2) Takasbank responds to the application made on the basis of the content in the data recording system and within the framework of article 6 of the Communiqué on the Principles and Procedures regarding the Application to the Data Controller as published by the Board.

(3) Takasbank responds to the application as soon as possible. This period may not exceed 30 days. As a rule, applications are made free of charge; however, if the process requires any additional cost, the fee specified in the tariff determined by the Board may be collected. In case it is understood that the application has resulted from Takasbank's fault, the fee collected is refunded.

ARTICLE 26-Exceptions

(1) In cases specified in article 28 of the Law no. 6698, the applications made to Takasbank are not responded.

(2) In the responses to be given to applications, the cases listed in the aforementioned article are excluded.

(3) The applications that are clearly unrelated with Takasbank and may be characterized as an abuse of right are not responded by Takasbank.

(4) The applications not meeting the conditions for application specified in article 24 herein are not responded.

ARTICLE 27-Enforcement

(1) This Directive shall enter into force on the date it is approved by the Board of Directors.

ARTICLE 28-Execution

(1) The provisions of this Directive shall be executed by the Board of Directors of Takasbank.

ANNEXES

ANNEX-1: Data Subject Application Form

GENERAL INFORMATION

We, as Istanbul Settlement and Custody Bank Inc. İn its capacity as data controller, hereby declare that we have fulfilled our obligations defined in the Law no. 6698 on Protection of Personal Data. Accordingly, personal data are processed based on the methods and legal reasons explained in chapter seven of the Directive on Takasbank Personal Data Protection Policy and for the purposes specified in article 8 therein; and personal data are transferred to the recipient groups indicated in chapter four of the said directive for the purposes set forth again in the same chapter. The rights of Data Subjects and the methods to exercise such rights are explained in detail in chapter eight of the said directive.

Takasbank reminds that it is not possible to directly apply to the Board without making an application to the data controller pursuant to paragraph 2 of article 14 of the Law no. 6698.

We represent that your personal data that you will give us by completing this form must be processed by Takasbank for the reasons specified in article 5 of the Law no. 6698.

Subject Matters of Application

The rights of Data Subjects are set forth in article 11 of the Law no. 6698 on Protection of Personal Data. Accordingly;

ARTICLE 11 - (1) Each person has the right to apply to the data controller and;

a) to learn whether his/her personal data are processed or not;
b) to request information about the processing if his/her personal data are processed;
c) to learn the purpose of processing of his/her personal data and whether such data are used for intended purposes or not;
ç) to know the third persons to whom his/her personal data are transferred at home or abroad;
d) to request for correction of personal data if they are processed in an incomplete or erroneous manner;
e) to request for deletion or destruction of his/her personal data under the conditions stipulated in article 7;
f) to request for notification of the operations executed pursuant to subparagraphs (d) and (e) to third persons to whom his/her personal data have been transferred;
g) to object to the processing, exclusively by automatic means, of his/her personal data, which leads to an unfavourable consequence for the data subject;
h) To request for compensation of the loss or damage arising from the unlawful processing of his/her personal data.

Subject Matters for which No Application can be made

The applications to be made on any issues specified in article 28 of the Law no. 6698 on Protection of Personal Data shall not be responded.

In addition, applications that are clearly unrelated to Takasbank and may be characterized as an abuse of right shall be left unanswered by Takasbank.

The applications made via any method other than the application methods specified below shall not be responded.

Application Methods

This form has been prepared to help Data Subjects exercise their rights. It is not mandatory for Data Subjects to use this form in their applications. In any event, the issues specified herein shall apply with respect to identity verification and the application method.

Data Subjects;

1. may complete and submit this form or the letter of application they have prepared bearing their original signature to the address of **"İstanbul Takas ve Saklama Bankası A.Ş. Reşitpaşa Mahallesi, Borsa İstanbul Caddesi, No:4 Sarıyer 34467 Istanbul"** either in person or through their representatives/attorneys. Identity verification is mandatory at the time of application. In case of applications made through an attorney, it is required to submit the original power of attorney containing the authorization granted in relation to personal data request.
2. may send the originally-signed application form or the letter of application that they will prepare themselves to the address specified in the first article herein by writing **"KVK Kapsamında Bilgi Talebi" (Information Request under the Law on Protection of Personal Data)** on the envelope. The applicant's attorney may also send an application via mail together with the original power of attorney containing the authorization granted in relation to personal data request.
3. may apply via a notary. In case of applications via a notary, the address given above shall be used. **"KVK Kapsamında Bilgi Talebi" (Information Request under the Law on Protection of Personal Data)** must be written in the subject field of the notification made.
4. may use the address of takasbank.haberlesme@hs03.kep.tr in order to send an application via REM. If this method is used, **"KVK Kapsamında Bilgi Talebi" (Information Request under the Law on Protection of Personal Data)** must be written in the subject field of the e-mail sent.
5. If there is an electronic mail address previously notified by the Data Subject to Takasbank and already registered in Takasbank system; application may be sent using such e-mail address. **"KVK Kapsamında Bilgi Talebi" (Information Request under the Law on Protection of Personal Data)** must be written in the subject field of the e-mail sent.

It is essential to collect minimum personal data in the applications. Therefore, no information and document containing personal data other than those specified in article 24 herein must be provided in the applications.

Responding to the Applications

The applications meeting the conditions above are responded by Takasbank as soon as possible. This period may not exceed 30 days. As a rule, applications are made free of charge; however, if the process requires any additional cost, the fee specified in the tariff determined by the Personal Data Protection Board may be collected. However, in case it is understood that the application has resulted from Takasbank's fault, the fee collected shall be refunded. The response to be given by Takasbank may be either received by the Data Subject in person or through his/her attorney against signature or sent to the specified address, REM address, or electronic mail address, if the relevant criterion is met, to prove that the application has been responded. The Data Subject is required to specify the method for communication of the response. If no method is specified, the response shall be given through the method through which the application has been made.

Takasbank reserves the right to request for additional information from the applicant.

APPLICATION DETAILS

Subject Matter of Application/Request

*(Please give information about your application. If the space provided below is insufficient, the field **Additional Explanations** may be used. Explanations on the subject matters of application are provided in the chapter eight of the Directive on Takasbank Personal Data Protection Policy.)*

Preferred Method for Response to the Application
(Please select your preference for response to your application)

Delivery by Hand	
Delivery to Address	
REM (registered electronic mail)	
Electronic Mail[1]	

Data Subject's

Relationship with Takasbank :
Name :
Surname :
Turkish Identity Number :
Nationality[2] *:*
Passport or Identity No.[3] *:*
Address :
Application Date :
Signature :

Additional Explanations:

[1] Only the e-mail addresses previously notified by the data subject and already registered in Takasbank system.
[2] For foreigners.
[3] For foreigners.

ANNEX-2: Data Breach Notification And Crisis Management Plan

1. PURPOSE

According to article 12, paragraph (5) of Law No. 6698 on the Protection of Personal Data, titled "Obligations Concerning Data Security," states, "In case the data processed are obtained by others by unlawful means, the data controller shall communicate the breach to the data subject and notify it to the Board within the shortest time. Where necessary, the Board may announce such breach at its official website or through in any other way it deems appropriate."

In this context, the Data Breach Notification and Crisis Management Plan ("Plan") has been prepared to determine the actions to be adopted and implemented by Takasbank in the event that personal data processed by Istanbul Clearing and Custody Bank Inc. (Takasbank) is obtained by others through illegal means.

2. SCOPE

All personal data processed by Takasbank falls within the scope of this Plan, and the Plan shall be applied to all records containing personal data owned or managed by Takasbank and all activities involving the processing of personal data.

3. DEFINITIONS AND ABBREVIATIONS

The important definitions used in the plan are listed below.

a) **Authority:** means the Personal Data Protection Authority.
b) **Board:** means the Personal Data Protection Board
c) **Data Breach:** means any situation where personal data processed by Takasbank is “unlawfully processed,” “unlawfully accessed,” “unlawfully obtained,” or “unauthorized persons circumvent the technical and administrative measures taken by Takasbank to ensure the protection of personal data and to ensure its level of security.”
d) **Data Controller:** means Takasbank,
e) **Personal Data:** means any information relating to an identified or identifiable natural person,
f) **Processing of Personal Data:** means any operation which is performed on personal data, wholly or partially by automated means or non-automated means which provided that form part of a data filing system, such as collection, recording, storage, protection, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorization, preventing the use thereof.

4. RESPONSIBILITY

All Takasbank employees are responsible for the implementation of the plan. Employees who act contrary to the plan will be subject to the disciplinary provisions of the Takasbank Human Resources Directive.

5. PERSONEL DATA BREACH

A personal data breach occurs in situations such as the unlawful acquisition of personal data, unauthorized access to personal data in violation of the law, or the disclosure, alteration, unlawfully deteled or integrity impairment of personal data to unauthorized persons due to error/intent.

The following situations are generally considered personal data breaches:

- Theft or loss of physical documents or electronic devices containing personal data,

- The transfer of electronic documents containing personal data outside the company through hardware or software,
- The acquisition of personalized user names and passwords by unauthorized persons,
- Inadvertently forwarding or sending emails containing personal data and/or confidential information to unrelated parties outside the company.
- Unlawful access to personal data through viruses or other attacks (e.g., cyberattacks) on Information Technology (IT) equipment, systems, and networks.

6. CRISIS REPONSE TEAM

A Crisis Response Team (Team) will be established, including the following participants, to intervene in the crisis situation that has occurred or may occur in the event of a personal data breach and to fulfill the obligations stipulated under the Law.

- Data Controller Contact Person
- Internal Control Unit
- Information Security Department
- Data Controller (General Principle)
- Unit Manager Where the Violation Occurred

7. CRISIS RESPONDENCE PROCESS

Pursuant tothe Decision No. 2019/10 of the Personal Data Protection Board dated 24.01.2019 (“Decision”) regarding the Procedures and Principles of Notification of Personal Data Breach, the data controller must notify the Board of the personal data breach without delay and within seventy-two (72) hours at the latest, from the date of learning about it, and following the identification of the persons affected by the data breach, the relevant persons must be notified within the shortest reasonable period by appropriate methods such as directly to the contact address of the relevant person if it is accessible, or by publishing it on the website of the data controller if it is not accessible.
In order to fulfill the aforementioned obligations, the following steps must first be followed within Takasbank in the event of a data breach:

a. Preliminary assessment of the crisis,
b. Conducting prevention and recovery efforts,
c. Assessing risks,
d. Notification,
e. Evaluation and Remediation

a) Preliminary Assessment of the Crisis

In the event of a data breach at Takasbank, all relevant employees are obligated to report the situation immediately and without delay to the Information Security Unit and the Data Controller Contact Person.

- The date and time of the personal data breach,
- The date and time of detection of the personal data breach,
- Descriptions relating to the personal data breach event,
- If known, the number of individuals and records affected by the personal data breach,
- Descriptions of the steps taken and measures adopted at the time of personal data breach detection, if any,
- Name and surname of the employee(s) who prepared the report, their contact information, and the report date

The Data Controller's Contact Person performs a preliminary assessment, taking into account the matters specified in the report. When making this assessment, the Internal Control Unit will examine and investigate whether a data breach has actually occurred, the scope of the breach, and its potential impacts, and if necessary, inform the Internal Audit Unit for a comprehensive investigation and the Internal Audit Unit initiates a comprehensive investigation to investigate the data breach.

b) Conducting prevention and recovery efforts

To mitigate the effects of the data breach on Takasbank and data subjects, blocking and recovery efforts are carried out in collaboration with the Internal Control Unit and the Information Security Unit. In this scope, the units/teams that need to be notified of the data breach are first identified, and these individuals are provided with guidance on the steps that should be taken to control the breach, prevent it if possible, and mitigate the damages. Following this, an attempt is made to identify which individuals and records will be affected by the data breach, and if there are any, their contact information is also determined. Concurrently, it is assessed whether there are any other institutions or organizations that need to be notified due to the data breach.

c) Assessing risks

Personal data breaches can have many negative impacts on the affected individuals, such as identity theft, restriction of rights, fraud, financial loss, reputational damage, loss of personal data security, and discrimination. Therefore, it is crucial that the potential consequences of a personal data breach are carefully evaluated by the Takasbank Internal Systems Department and the Personal Data Committee, outlining the risks they may pose to Takasbank and the individuals affected by the breach. When assessing risks, the nature, sensitivity, and volume of personal data affected by the breach, as well as the number of individuals affected, the impact of the data breach on Takasbank's activities and reputation, the measures taken to mitigate the impact of the data breach, and the potential consequences of the breach should be considered separately.

Based on the outcome, a data breach is characterized as "low-risk, medium-risk, or high-risk":

- Low-risk: The breach does not cause any negative impact on the data subjects or the impact remains negligible.
- Medium-risk: The breach may cause negative impacts on the relevant persons, but these impacts are not significant.
- High risk: The breach is causing serious negative impacts on the affected persons.

Regarding data breaches defined as medium and especially high risk, the Data Controller contact officer and the Information Security Unit immediately inform the KVK Committee and Takasbank Senior Management and invite them to a meeting and take part in the coordination of all processes according to the risk assessment reports and the details of the breach.

d) Notification

The data breach may need to be notified to third parties other than Takasbank for purposes such as fulfilling legal obligations, taking measures regarding the data breach, and mitigating its potential impacts.

i. Notification to the Board

The Data Controller's Contact Person is obligated to notify the Board of the personal data breach as soon as they become aware of it, and no later than 72 hours. Therefore, to ensure that Takasbank does not face any sanctions, all employees are required to report any data breach incident to the Data Controller Contact Person without delay. The notification to the Board is made using the Personal Data Breach Application Form published on the KVK website. If the notification cannot be made to the Board within 72 hours for a justifiable reason, the reasons for the delay are also explained to the Board with the notification.

ii. Notification to Persons Affected by the Breach

Following the identification of those affected by the personal data breach, Takasbank must notify the relevant individuals as soon as reasonably possible. Following the identification of those affected by the personal data breach, Takasbank must notify the relevant individuals as soon as reasonably possible. If the relevant person's contact information is accessible, Takasbank must notify them directly, or if not, by appropriate means, such as publishing an announcement on the website.
Such notifications are made by the Data Controller Contact Person with the support of the Team.
Based on the Personal Data Protection Board's Decision No. 2019/271 dated September 18, 2019, regarding the minimum elements that must be included in a data breach notification sent by a data controller to a data subject, Takasbank's breach notification must be made in clear and plain language and must include, at a minimum, the following elements: • When the breach occurred, • Which personal data was affected by the breach based on personal data categories (making a distinction between personal data and special categories of personal data), • The potential consequences of the personal data breach, • Measures taken or proposed to mitigate the negative effects of the data breach, • The names and contact details of contact persons who will enable the data subjects to receive information about the data breach, or the full address of the data controller's website, call center, etc., should be included.

iii. Other Notifications

In addition to the notifications that Takasbank is legally obligated to make, it may also be required to notify third parties as per its contractual obligations, taking into account factors such as the nature and scope of the data breach, and whether the breach constitutes a criminal offense.

e) Assessment and Remediation

Takasbank must record all information regarding personal data breaches, their impact, and the measures taken and make them available for review by the Board.
The KVK Committee, the Information Security Unit, and the Internal Control Unit conduct an assessment to determine whether the steps taken regarding a data breach are appropriate and what aspects could be developed/improved in the event of a potential data breach.
In this scope, it prepares an evaluation and improvement report that includes the following elements.

- What steps should be taken to mitigate the effects of potential personal data breaches
- Whether any policy, procedure, or report needs to be improved due to a personal data breach
- Whether an additional administrative and/or technical measure is required to prevent the recurrence of a personal data breach,
- The necessity of employee awareness training that will prevent the recurrence of the breach,
- Whether additional investment in resources/infrastructure is necessary to mitigate exposures to violations and their cost impacts is evaluated.