TÜRKİYE WEALTH FUND INC.

PERSONAL DATA PROTECTION POLICY

1. INTRODUCTION

1.1. Generally

Ensuring the confidentiality and security of personal data and compliance with the relevant legal regulations are among the most important priorities of our Company, Türkiye Wealth Fund Inc., ("Company"), and intense care is shown in this regard. In this context, the process and targeted purpose managed by this Personal Data Protection Policy ("Policy") and other written policies within the Company regarding the processing and protection of personal data; informing our customers, potential customers, employees, employee candidates, visitors and other third parties about the legal processing, storage and protection of their personal data, and reflecting our corporate culture.

In the preparation of this Policy; Our Company has been guided by the provisions of the Constitution of the Republic of Turkey and the Law on the Protection of Personal Data No. 6698 ("PDPL"), the relevant legal norms regarding the protection of personal data and the decisions of the Personal Data Protection Board.

In this Policy, explanations will be made regarding the following basic principles adopted by our Company for the processing of personal data:

- Processing personal data in accordance with the law,
- Keeping personal data accurate and up-to-date when necessary,
- Processing personal data for specific, explicit and legitimate purposes,
- Personal data must be connected, limited and measured for the purpose for which they are processed,
- Keeping personal data for as long as required by the relevant legislation or for the purpose for which they are processed,
- Informing data subjects,
- Establishing the necessary processes for the data subjects concerned to exercise their rights,
- Taking the necessary measures in the processing and protection of personal data,
- Transferring personal data to third parties in line with the requirements of the processing purpose,
- Showing the necessary care in the processing and protection of special categories of personal data,
- Erasure, destruction or anonymization of personal data whose processing purpose has ended.

1.2. Purpose of the Policy

The main purpose of this Policy is to provide transparency by informing the data subjects about the personal data processing activity carried out by our Company in accordance with the law and the procedures adopted for the protection of personal data.

In addition, this Policy and other written policies aim to make our principle of compliance with the PDPL and other relevant legal regulations regarding personal data security sustainable.

1.3. Scope of the Policy

The scope of this Policy is for data subjects whose personal data is processed automated means or non-automated means which provided that form part of a data filing system. The Internal Directive on the Protection of Personal Data has been established within the scope of this Policy.

1.4. Implementation of the Policy and Related Legislation

This Policy has been drawn up within the framework of the principles set forth by the relevant legislation. Our company undertakes and accepts that in case of inconsistency between the legislation in force and this Policy, the legislation will be implemented.

1.5. Enforcement of the Policy

This policy comes into force after being approved by our Company's board of directors. It is published on the (https://www.tvf.com.tr) website and made available to the data subjects in this way.

2. DEFINITIONS AND ABBREVIATIONS

Explicit Consent	Freely given, specific and informed consent
Anonymization	Rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data
Employee	Employee of the Türkiye Wealth Fund
Employee Candidate	Persons who have applied for a job or submitted their CV and related information to our Company for review by any means.
Data Subject	The natural person, whose personal data are processed

Personal Data	Any information relating to an identified or identifiable natural person
Processing of Personal Data	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
Board	The Personal Data Protection Board
Authority	The Personal Data Protection Authority
Policy	Personal Data Protection Policy
PDPL	Law on the Protection of Personal Data No. 6698
Special Categories of Personal Data	Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data
Periodic Disposal Process	In case of termination of personal data processing purposes, erasure, destruction or anonymization to be carried out at regular intervals
Potential Customer	Persons who have requested or are considered to use our services
Company	Türkiye Wealth Fund Inc.
Data Processor	The natural or legal person who processes personal data on behalf of the data controller upon its authorization,
Data Filing System	Registration system where personal data is processed and structured according to certain criteria
Data Controller	The natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data filing system

Data Subject Application Form	The application form to be used by data subjects when using their applications regarding their rights in Article 11 of the PDPL
Erasure	Making personal data inaccessible and non-reusable for the relevant users.
Destruction	Making personal data inaccessible, irretrievable and reusable by anyone in any way.
Guest	People visiting physical premises owned by the company

3. PRINCIPLES OF PROCESSING PERSONAL DATA

3.1. Processing of Personal Data in Compliance with the Principles in the Legislation

3.1.1. Lawfulness and Fairness

Our Company has adopted the principle of being lawful and fair in all transactions to be carried out on personal data. In this context, by adopting the principle of transparency, it informs the data subjects about the purpose of use of the personal data collected through this Policy and other texts.

3.1.2. Being Accurate and Kept Up To Date Where Necessary

Our Company has a system and process to ensure the accuracy and up-to-dateness of the personal data it processes while processing personal data. In this context, data subjects may make it possible to keep their personal data accurate and up-to-date by applying to our Company.

3.1.3. Being Processed for Specified, Explicit and Legitimate Purposes

Our Company clearly determines the purpose of processing personal data within legitimate and legal limits and presents it to the data subjects before the personal data processing activity begins, through this Policy and other texts.

3.1.4. Being Relevant, Limited and Proportionate to the Purposes For Which They Are Processed

Our Company processes personal data within the scope of the necessary purposes for the execution of the activity in a way that is related and proportional to the field of activity. In this context, while carrying out data processing activities, it carefully avoids processing personal data that is not related to the realization of the purpose and is not needed at the moment or in the future.

3.1.5. Being Stored for the Period Laid Down by Relevant Legislation or The Period Required for The Purpose for Which the Personal Data Are Processed

Our Company retains personal data only for the period specified in the relevant legislation or for the period required for the purpose for which they are processed. In this context, first of all, it is determined whether a period is determined in the relevant legislation for the storage of personal data, and if a period is determined, action is taken in accordance with this period. If a specific period is not determined, the period required for the purpose for which each personal data is processed is determined and kept for this period.

In this context, our Company implements policies for the erasure, destruction or anonymization of personal data.

3.2. Compliance with Personal Data Processing Conditions

Our Company processes personal data only on the basis of the explicit consent of the data subject or in accordance with the situations in which explicit consent is not required in the PDPL.

3.2.1. Explicit Consent

Explicit consent means freely given, specific and informed consent. Our Company respects and complies with the explicit consent of the data subject, if necessary for personal data processing.

3.2.2. Circumstances Where Explicit Consent is Not Required

In some cases, the processing of personal data without the explicit consent of the data subject is accepted in the PDPL. Since obtaining explicit consent from the person concerned in the presence of one of the specified conditions will be considered as misleading the data subject, our Company does not apply for explicit consent in the following conditions.

- It is expressly provided for by the laws.
- 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.
- Processing of personal data of the parties of a contract is necessary, provided that it is directly related to the establishment or performance of the contract.
- It is necessary for compliance with a legal obligation to which the data controller is subject.
- Personal data have been made public by the data subject himself/herself.
- Data processing is necessary for the establishment, exercise or protection of any right.
- Processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

3.3. Processing of Special Categories of Personal Data

Our company shows maximum sensitivity to the processing and protection of personal data determined as special categories of personal data by PDPL.

It is prohibited to process special categories of personal data without explicit consent of the data subject. By our Company, special categories of personal data can be processed in the following cases, provided that adequate measures to be determined by the Board are taken, if the person concerned does not have explicit consent.

- Personal data, except for data concerning health and sexual life, listed in the first paragraph may be processed without seeking explicit consent of the data subject, in the cases provided for by laws.
- Personal data concerning health and sexual life may only be processed, without seeking explicit consent of the data subject, by the persons subject to secrecy obligation or competent public institutions and organizations, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

Our Company has determined additional measures regarding the processing and access of sensitive personal data. In this framework, the environments where special categories of personal data are stored and protected with secondary locks and secondary passwords, and they can only be processed by authorized persons within the framework of the authorization matrix.

3.4. Transfer of Personal Data

Personal data may be shared with the following persons in order to fulfill the purposes specified in this Policy;

- to supervisory organizations within the framework of audit activities,
- to the auditing institutions, in accordance with the Turkish Commercial Code and other relevant legal regulations,
- to our shareholders,
- to legally authorized public institutions and organizations,
- to our domestic and/or foreign suppliers and business partners,
- to natural and legal persons to whom services are provided or to third parties to whom services are provided in the country and abroad.

4. PRINCIPLES ON THE DATA PROTECTION OF PERSONAL DATA

4.1. Technical and Organizational Measures Taken by Our Company Regarding the Security of Personal Data

4.1.1. Technical Measures

The main technical measures taken by our Company to ensure that personal data are processed in accordance with the law and to prevent unlawful access to personal data are as follows:

- Personal data processing activities carried out within our Company are audited by established technical systems.
- Experienced personnel in technical matters are employed.
- Relevant departments on technical issues have been established.
- The technical measures taken are periodically reported to the authorized unit in accordance with the internal audit mechanism.
- In order to ensure the safe storage of personal data, a backup program is used in accordance with the law.
- New technological developments are followed and technical measures are taken on systems, especially in the field of cyber security, and the measures taken are periodically updated and renewed.
- Access and authorization technical measures are used within the framework of legal compliance requirements determined for each department within our Company.
- Access authorizations are limited, authorizations are regularly reviewed, and accounts of former employees are closed.
- Software and hardware including virus protection systems and firewalls are used.
- The use of counterfeit software and hardware is strongly avoided.
- All of our products we use are original and licensed.

In this framework, our Company is constantly working on the following technical measures determined by the Board:

- Authority Matrix
- Authority Control
- Access Logs
- User Account Management
- Network Security
- Application Security
- Encryption
- Penetration Test
- Intrusion Detection and Prevention Systems
- Log Records
- Data Masking
- Data Loss Prevention Software
- Backup
- Firewalls
- Anti-Virus Systems
- Erasure, Destruction, or Anonymization
- Key Management

4.1.2. Organizational Measures

The main organizational measures taken by our Company to ensure that personal data are processed in accordance with the law and to prevent unlawful access to personal data are as follows:

- Our employees are informed and trained about the law of protection of personal data and the processing of personal data in accordance with the law.
- The requirements to be fulfilled in order to ensure the legality of the personal data processing activities carried out by the business units of our Company are examined for each business unit and the activity carried out.
- Contracts and documents between our Company and employees set records that impose an obligation not to disclose and use personal data. In addition, awareness of the employees is increased in this regard.
- In order to keep the sensitivity towards data protection at a high level, necessary organizational measures are implemented with internal policies and trainings.
- Access to personal data and authorization processes are designed and implemented in our Company.
- The processes regarding the PDPL and other relevant regulations are followed by the relevant units under the coordination of the Contact Person.
- Provisions are added to the contracts signed by our Company with third parties to whom personal data is transferred in accordance with the law, that necessary security measures will be taken to protect the transferred personal data and that these measures will be complied with in their own establishments.

In this framework, our Company is constantly working on the following organizational measures determined by the Board:

- Preparation of Personal Data Processing Inventory
- Corporate Policies (Access, Information Security, Use, Storage and Disposal etc.)
- Contracts (Between Data Controller - Data Controller, Data Controller - Data Processor)
- NDA
- In-house Periodic and/or Random Audits
- Risk Analysis
- Employment Contract, Disciplinary Regulation (Adding Legal Provisions)
- Corporate Communication (Crisis Management, Informing the Board and Data Subject, Reputation Management, etc.)
- Education and Awareness Activities (Information Security and Law)
- Notification to Data Controller’s Registry Information System (VERBIS)

4.2. Awareness Training and Supervision of Data Protection Processes

Our Company carries out the necessary trainings and studies in order to prevent the illegal processing of personal data and illegal access to the data.

In order to increase the awareness of the current employees of our Company on the protection of personal data, we work with professionals.

4.3. Protection of Special Categories of Personal Data

Our Company carefully protects special categories of personal data. The technical and organizational measures taken in this context have been determined based on the relevant legal regulation and the "Adequate Precautions to be Taken by Data Controllers in the Processing of Special Categories of Personal Data" published by the Personal Data Protection Authority.

4.4. Procedure to Follow in Case of Personal Data Breach

Our Company will notify the data subject and the Board within 72 hours, in case the personal data it processes is obtained by others illegally.

If deemed necessary by the Board, this may be announced on the Board's website or by any other method.

4.5. Personal Data Inventory

Each unit of our Company creates an up-to-date personal data processing inventory. The unit manager is responsible for the accuracy and updating of this inventory.

The correct keeping of inventories and the implementation of this Policy are constantly checked. Up-to-date developments regarding the protection of personal data are always followed.

5. APPLICATION OF DATA SUBJECTS TO DATA CONTROLLER, OUR COMMUNICATION CHANNELS AND EVALUATION PROCESSES OF THE APPLICATION

5.1. Subject of Application

Our Company cares about the rights of the data subjects.

An Application Form to Data Controller, where the data subjects can easily submit their requests, has been prepared by our Company and published on our website.

In addition, all applications made in accordance with the Comminuque On The Principles And Procedures For The Request To Data Controller will be evaluated.

Within the scope of Article 11 of the PDPL, everyone has the right to apply to our Company for the following matters:

- to learn whether his/her personal data are processed or not,
- to demand for information as to if his/her personal data have been processed,
- to learn the purpose of the processing of his/her personal data and whether these personal data are used in compliance with the purpose,
- to know the third parties to whom his personal data are transferred in country or abroad,

- to request the rectification of the incomplete or inaccurate data, if any,
- to request the erasure or destruction of his/her personal data under the conditions referred to in Article 7,
- to request reporting of the operations carried out pursuant to sub-paragraphs (d) and (e) to third parties to whom his/her personal data have been transferred,
- to object to the occurrence of a result against the person himself/herself by analysing the data processed solely through automated systems,
- to claim compensation for the damage arising from the unlawful processing of his/her personal data.

5.2. Application Guidance

Application Method	**Address to Apply**	**Application Subject Heading**
Application by hand *(If the applicant applies personally, the document proving his identity must be available. In case of application through a lawyer, a notarized warrant of attorney must be available)*	Muallim Naci Caddesi, No:22, Ortaköy/İstanbul	*"Information Request Under the Personal Data Protection Law "* will be written on the document.
Notice via Notary	Muallim Naci Caddesi, No:22, Ortaköy/İstanbul	*"Information Request Under the Personal Data Protection Law "* will be written on the document.
Email Via E-signature/Mobile Signature	tvf@hs01.kep.tr	*"Information Request Under the Personal Data Protection Law "* will be written on the subject.
Application via Registered Electronic Mail (REM) address	tvf@hs01.kep.tr	*"Information Request Under the Personal Data Protection Law "* will be written on the subject.

E-mail address registered in our systems *(Your e-mail address must match your identity in our systems before.)*	kvkk_bildirim@tvf.com.tr	*"Information Request Under the Personal Data Protection Law "* will be written on the subject.

5.3. Procedure After Application

Applications submitted to us are answered within 30 (thirty) days at the latest from the date they reach our Company, depending on the content of the request.

Our responses are sent on the basis of the form of notification specified by the applicant.

Data subjects; in cases where the application is rejected in accordance with Article 14 of the PDPL, the answer given is insufficient or the application is not answered in due time; Complaints can be made to the Board within thirty days from the date of our Company's response, and in any case within sixty days from the date of application.

5.4. Application Fee

Applications are made free of charge as a rule. However, if the request of subjects requires an additional cost, the fee in the tariff determined by the Board will be charged by our Company.

6. INFORMING DATA SUBJECTS

Our Company, in accordance with the regulation in Article 10 of the PDPL, informs the persons concerned about the process of obtaining personal data through this Policy and the texts on our website in an easily accessible way. In this context, our Company informs the data subjects about the identity of the data controller, the purpose for which personal data will be processed, to whom and for what purpose the processed personal data can be transferred, the method and legal reason for collecting personal data, and other rights of the data subject.

An application form has been created and published on the website of our Company in order for the data subject to use their rights specified in the PDPL more easily.

7. PERSONAL DATA PROCESSING PURPOSE AND STORAGE PERIOD

7.1. Purposes of Processing Personal Data

Our Company processes personal data limited to the purposes and conditions in the personal data processing conditions specified in Articles 5 and 6 of the PDPL. These purposes and conditions are;

- It is expressly provided for by the laws.

- 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.
- Processing of personal data of the parties of a contract is necessary, provided that it is directly related to the establishment or performance of the contract.
- It is necessary for compliance with a legal obligation to which the data controller is subject.
- Personal data have been made public by the data subject himself/herself.
- Data processing is necessary for the establishment, exercise or protection of any right.
- Processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.
- Personal data, except for data concerning health and sexual life, listed in the first paragraph may be processed without seeking explicit consent of the data subject, in the cases provided for by laws.
- Personal data concerning health and sexual life may only be processed, without seeking explicit consent of the data subject, by the persons subject to secrecy obligation or competent public institutions and organizations, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

7.2. Storage Time of Personal Data

We keep personal data for the period specified in the relevant legislation. In addition, in determining the retention periods, our obligations arising from the relevant contracts, our administrative and legal responsibilities/obligations are also taken into consideration.

Personal data is deleted when the storage period we have determined expires, and is backed up only to provide evidence in possible legal disputes or to assert the relevant right related to personal data. In this case, personal data is not accessed for any other purpose.

Processed personal data and personal data inventories are reviewed in 6-month periods and personal data that needs to be deleted/destroyed are deleted/destroyed within these 6-month periodic destruction periods.

8. PERSONAL DATA PROCESSING ACTIVITIES IN THE BUILDING-SHIPYARD WITH THE ENTRY OF THE BUILDING-SHIPYARD

8.1. CCTV

In order to ensure the safety of the data subjects and our Company, monitoring activities are carried out through security cameras.

In this context, we act in accordance with PDPL and other relevant legislation.

8.1.1. Informing About CCTV

In accordance with Article 10 of the PDPL, the data subjects are informed about the activity, thus preventing harming the fundamental rights and freedoms of the persons concerned and ensuring transparency. Information is provided in areas where camera monitoring is carried out.

8.1.2. Purpose and Purpose Limitation of CCTV

We process personal data in accordance with “being relevant, limited and proportionate to the purposes for which they are processed” principle. The purpose of monitoring activity is limited to ensuring security. Therefore, the monitoring areas of security cameras, their number and when they will be monitored are determined in accordance with the said purpose.

8.1.3. Ensuring the Security of Data Obtained by CCTV

All necessary technical and organizational measures are taken to ensure the security of personal data obtained through CCTV. Detailed information can be found under the heading "Principles on the Protection of Personal Data".

8.1.4. Accessing and Sharing Information Obtained by CCTV

Only authorized persons can access the information obtained through CCTV and the environments where this information is stored. Live camera footage can be viewed by security personnel who are employees of the Company or outsourced services. A limited number of people who have access to the records declare that they will protect the confidentiality of the data they access with a confidentiality agreement. In addition, this information can be shared with public authorities upon written request.

8.2. Guest Entry/Exit Tracking

Personal data is processed for the purpose of ensuring security and tracking guest entries and exits. Regarding data processing activities, visitors are informed in the relevant areas.

8.3. Recording the Information of Electronic Devices at the Entrances of the Work Areas

In case our guests use their personal computers or similar electronic devices, we record the MAC addresses of computers or similar electronic devices. The reason for this is to ensure the security of our company and the people whose personal data are within our company.

9. REVIEW

This policy comes into force after being approved by the Company's board of directors. Approval is obtained from persons authorized by the board of directors for changes to be made in the policy. The policy is reviewed every 6 months and, if necessary, revisions are made with the approval of the authorized persons.

10. CONTAT PERSON

The contact person carries out the necessary work by ensuring coordination with the relevant units on organizational and technical measures. The principles determined by the Company regarding organizational and technical measures are taken into account. The contact person makes the necessary effort to comply with the personal data protection legislation. The contact person supervises the Company units for which he is responsible within the scope of personal data protection law. As a result of these audits, it warns the relevant units when necessary and informs the senior management of the situation.

The liaison person provides the coordination to respond to the related person applications made to the Company within the legal deadlines and in accordance with the procedure. The contact person manages the Company's relations with the Personal Data Protection Authority.

11. ENFORCEMENT

This Policy enters into force from the date of acceptance and announcement by authorized persons.