

PERSONAL DATA PROTECTION POLICY

1. INTRODUCTION

Fundamental rights and freedoms, particularly right to privacy is guaranteed by the Constitution of the Republic of Turkey. The amendment to the constitution in 2010, to be informed about the processing of personal data, have access to it, request its correction or deletion and learn whether it is processed within stated purposes have been defined as a fundamental right. The procedures and principles regarding the storage, processing, transfer and destruction of personal data and the rights and obligations of the parties are regulated by Personal Data Protection Law which is applicable as of 7th Nisan, 2016.

As the processor of customer data to provide extensive banking services, employee data as the employer and personal data of visitors, suppliers etc., Isbank is obliged to take all necessary technical and organizational measures to provide an appropriate level of security against unlawful processing of personal data and unlawful access to it.

The Bank fulfills this responsibility in line with applicable law.

2. PURPOSE

The purpose of the Personal Data Protection Policy is to carry out Bank's data processing activities compliant with the applicable law and in accordance to main principles defined within Policy; also to increase knowledge of all employees and give guidance to them in terms of privacy. In this context, all activities should be executed according to principles set in this Policy and other internal regulations regarding information security.

3. SCOPE

The Policy relates to the protection of personal data belonging to employees, employee candidates, customers, potential customers, shareholders, visitors and other groups of natural persons that is processed by automated means or by non-automated means as part of a data filing system.

The Law essentially applies to "natural persons" while the data belonging to a legal person "which enables the identification of a real person" are also within the scope of the Law and therefore the Policy.

4. DEFINITIONS

Explicit Consent: Freely given, specific and informed consent

Bank: Türkiye İş Bankası A.Ş.

Data Subject: Natural person whose personal data is processed

Law: Personal Data Protection Law

Personal Data: Any information relating to an identified or identifiable real 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.

Policy: Personal Data Protection Policy

Data Processor: The natural or legal person who processes personal data on behalf of the data controller upon its authorization.

Data Filing System: The system where personal data are processed by being structured according to specific 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 (in terms of this Policy, Türkiye İş Bankası A.Ş.)

5. MAIN PRINCIPLES

General Principles

The Bank processes personal data;

- lawfully and fairly,
- with best effort for accuracy and up-to-dateness,
- for specified, explicit and legitimate purposes,
- relevant, limited and proportionate to the purposes for which it is processed,
- by storing it for the period for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed.

Obligation to Inform

Data controllers are obliged to inform the data subjects. Therefore, the Bank informs data subjects about the following:

- identity of the Bank (information regulated by Article 1524 of the Turkish Commercial Code and published on the Bank's website),
- the purpose of processing of personal data,
- to whom and for which purposes the processed personal data may be transferred,
- method and legal basis of collecting personal data,
- rights of data subjects as specified in the Policy

Conditions for Processing Personal Data

In line with the transferred principles, personal data cannot be processed without the explicit consent of the data subject, except for the conditions stated below:

- 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.

In cases where above conditions are met, personal data may be processed without explicit consent of the data subject. If the reasons for the processing no longer exist, personal data is destructed according to policy exclusively defined for this objective.

Conditions for Processing Special Categories of Personal Data

Personal data relating to 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 biometric and genetic data are deemed to be special categories of personal data.

Special categories of personal data can only be processed under the following conditions:

- Data subject has given his/her explicit consent.
- It is explicitly provided by law.
- 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 physical disability or whose consent is not deemed legally valid.
- It relates to personal data that have been made public by the data subject, and processing is in consistent with data subject's intention to make such data public.
- It is necessary for the establishment, exercise or protection of any right.
- It is necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and for the planning, management and financing of health-care services by persons subject to legal obligation of confidentiality or by competent public institutions and organizations.
- It is necessary for the fulfilment of legal obligations in the fields of employment, occupational health and safety, social security, social services, and social assistance.
- It relates to the current or former members and affiliates of foundations, associations, and other non-profit organizations established for political, philosophical, religious, or trade union purposes, or to individuals who are in regular contact with these organizations, provided that such processing complies with the applicable legislation governing these organizations and their objectives, is limited to the organizations' fields of activity, and does not involve disclosure of data to third parties.

This processing should align with the adequate measures determined by the local data protection authority.

Transfer of Personal Data

The Bank acts by fulfilling the requirements of the Law and other legislation regarding the transfer of personal data within the country or abroad. Provisions in other laws are reserved for the transfer of personal data in the country and abroad.

Rights of the Data Subjects

Data subjects has the right to request the following:

- 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,
- to request reporting of the erasure/destruction operations carried out 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 analyzing the data processed solely through automated systems,
- to claim compensation for the damage arising from the unlawful processing of his/her personal data.

The Bank may act on the requests or refuse it with justified grounds and delivers its response in writing or by electronic means. The Bank is obliged to conclude requests within the shortest time possible and within thirty days at maximum.

Obligations of Data Controller on Data Security

The Bank processes personal data based on the Policy. The Bank as data controller is obliged to take all necessary technical and organizational measures to provide an appropriate level of security for the purposes of preventing unlawful processing of and unlawful access to personal data; thus ensure solid protection. The data controller is also obliged to carry out the necessary audits, or have them made, in order to ensure the implementation of the Policy.

In case the personal data is processed by another entity on behalf of the data controller, namely data processor, data controller is jointly responsible for taking the measures. Therefore, in case of personal data transfers to processors, necessary contractual, technical and organizational measures should be taken and requested to be fully implemented.

The Law also defines the responsibility of natural persons who take part in data processing. The person who executes processing activities can neither disclose the data nor use it for purposed other than stated. This obligation continues even after the end of their term of office.

In case the data processed are obtained by others by unlawful means, the data controller obliged to communicate the breach to the data subject and notify it to the Board.

As the data controller, the Bank has to register with the "Data Controllers' Registry", which will be kept open to the public by the Personal Data Protection Authority. The Bank fulfills this obligation in line with the provisions of the By-Law On Data Controllers Registry and other procedures to be determined by the Board.

6. SUPERVISION/AUDIT

Compliance with the provisions of this policy is subject to internal audit.

7. ENFORCEMENT AND REVIEW

The Policy goes into effect upon approval of the Board and as of the date of publication. The policy is reviewed at least once a year in line with the provisions of the legislation and the Bank's requirements.