Bankpozitif Personal Data Protection Policy

BANKPOZİTİF KREDİ VE KALKINMA BANKASI A.Ş.
MERSİS NO: 0854012611200011
VERSION: 03

Contents

1. Introduction

Personal data means all kind of information relating to an identified or identifiable natural person. Personal data is protected mainly by the Constitution and by other laws and legal regulations.

According to article 20 of the Constitution, which regulates the confidentiality of private life, everybody has the right to demand protection relating to him/her. This right covers the right of being informed about the personal data, reaching the data, demanding correction or deletion of the data, and learning if the data is used in accordance with the purpose of processing. Protection of personal data and related rights are among the most important components of confidentiality of private life, which is one of the basic human rights and freedoms.

Personal data is also protected by the Turkish Criminal Code and the Law numbered 6698 on Protection of Personal Data which was enacted as per the aforesaid article of the Constitution.

Articles 135-140 of Turkish Penal Code regulates the offenses related with personal data. Among the offenses, processing the data as against the law, unlawful transfer of it to the third parties and not deleting the data were stated in the Law.

With the law numbered 6698 on Protection of Personal Data, the purposes of processing of personal data and special categories of personal data and the way these data are processed were regulated and basic rules were set.

The Bank attributes utmost importance to the protection of personal data as part of the legal requirements stated above and also as part of its corporate approach and aims to take all the measures in implementation for this purpose.

2. Definitions

Anonymization	Bringing the personal data in a state that can not be connected under any circumstances to an identified or identifiable person by even matching with some other data.
Bank	Bankpozitif Kredi ve Kalkınma Bankası A.Ş.

Ethical Principles of Banking	The principles that were published by the Banks Association of Turkey and accepted by the Board of Directors of our Bank on 22.02.2007
Destruction	Operations for the purpose of deletion, removal and anonymization of personal data
KVKK	The Law numbered 6698 on Protection of Personal Data
Personal Data	All kind of data relating to an identified or identifiable natural person
Processing of Personal Data	Any operations which are performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
Board	The Board of Protecting the Personal Data
Special Categories of Personal Data (SCPD)	Data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, and biometrics and genetics are special categories of personal data.
TCK	The Criminal Code numbered 5237
Data Controller	Natural or legal person who determines the purposes and means of the processing of personal data, and who is responsible for establishment and management of the filing system. In our Bank practice it represents the Bank as a legal entity.
Data Processor	Natural or legal person who processes personal data based on the authority granted by and on behalf of the data controller.
Data Filing System	Any recording system through which personal data are processed by structuring according to specific criteria. These systems can be established in electronic or physical environments. According to this,

	in the In the filing system, personal data might have been classified according to name, surname or identity number or in another systematic criteria.

3. Basic Approach in Processing Personal Data

The Bank adopted the following basic policies in processing the personal data:

- The data shall be processed in conformity with the law and good faith;
- Measures shall be taken for the personal data being accurate and if necessary, up to date. Within this scope, the Bank is entitled to take reasonable measures in order to verify the owner of the data and up-to-datedness of the data.
- The data can be processed for specified, explicit, and legitimate purposes. Therefore, data that are not needed for performing the activities of the Bank shall not be gathered from the persons; concerning the processed data, in the relevant processes, the purpose of data processing shall be determined in writing.
- Personal data can be processed only to the extent of the purpose which they are maintained. Where such data needs to be processed for other reasons, the required measures including obtaining of the person's consent and informing him in accordance with the current legislation will be taken by the related departments.
- Personal data will be kept for as long as the minimum period stated in the legislation. At the end of this time period, such data will, either on the Bank's initiative or upon the request of the owner of the data, will be deleted, destroyed or anonymized. Our Board of Directors has determined the Bank's policy concerning deleting, destroying or anonymizing the personal data as part of this policy.

The Bank will make the necessary amendments to the written processes to ensure that the above-mentioned fundamental policies are taken into consideration when carrying out the Bank activities and; will identify the implementation principles on this matter in the detailed implementation instructions.

The Bank's rules and regulations on this matter indicate to the above mentioned fundamental approach and include the following topics:

- Enlightening and informing the owners of the personal data;
- The way the owners of the personal data can exercise their rights provided by the laws, and laying down the operational parameter of this in the Bank;
- The duration during which personal data should be kept;
- Specifying the purpose and scope of processing personal data;
- Taking the measures that are necessary for proper protection of personal data;
- Displaying higher level sensitivity for the protection of personal data that has special characteristics;
- The scope of reporting and provision of information to official authorities, where this is required by the legislation that is in force;
- To specify the internal authorities, duties and responsibilities.

3.1.1 Implementation of the Pertaining Legislation

Law on Protection of Personal Data (KVKK) was published and took effect in the year 2016. However, personal data is at the same time is customer secret under Banking Law. For this reason, The Bank had already taken measures for the protection of customer secrets including the personal data, as per the requirements of Banking Law and the associated rules and regulation, even before Law 6698. Nevertheless, necessary efforts for compliance with Law 6998 and the other new rules were made, and is still being made in accordance with the transitionary provisions of the Law.

The Bank is aware that should there be any discrepancy between this policy, implementation instructions or other written rules and regulations now inforce or that are being prepared, and the pertinent legislation, the pertinent legislation must be observed. When such discrepancies are noticed, the concerned Departments are obligated to change their practices according to the legislation, and to update their written rules and regulations accordingly as soon as possible.

3.1.2 Measures Taken to Ensure Secure Storage of Personal Data

Before Law 6698, the Bank had taken technical and administrative measures for the protection of customer secrets according to the Banking Law and the sub-regulations. These measures serve, at the same time, protection of the personal data, and basically include the following aspect.

1. Measures Regarding Processing of Data

The Bank will process the personal data without consent only in cases mentioned in the law, and in other cases, with the express consent of these persons.

Banking activity is such an activity field that requires processing of much more personal data in comparison to the other fields of businesses, and is strictly regulated by the Banking Law.

All of the business activities of the Bank are regulated in writing by detailed implementation instructions. These rules and regulations also include verification of identities, identification of the customer, credit processes, risk management activities, and data processing etc. within the framework of the services provided. The Bank has numerous written rules and regulation on this matter, which are listed under the heading of "pertinent documents" in this regulation.

Even where consent is not required, data processing will be carried out within the limits of and proportional to the purpose of the data processing. Written internal Bank rules and regulations are laid down for this purpose. These rules and regulations are about the details as to which kinds of data can be processed with respect to which groups of persons.

The Bank's employees have been and are informed about the obligations on processing of personal data.

Strict rules for ensuring confidentiality of information are included in the service contracts made by the Bank with third parties. These rules should include, in the case that the SCPD is shared with the third parties, the third party shall be liable to take the necessary measures to be demanded by the Bank when there is a need.

Where consent is required for processing of the data, the way such consent should be obtained was regulated in writing.

2. Administrative and Technical Measures against Unlawful Access to and for the Protection of Data

The Bank takes technical and administrative measures regarding personal data, for the prevention of operational mistakes, infiltration to the bank systems or other kinds of unlawful access. These measures have indeed been implemented for a long time within the framework of the BRSA regulations concerning administration of information systems, operational risk management, and the COBIT practices or of the other pertinent legislation. The measures taken for this purpose are summarized at below:

- The Information Security Regulation lays down the high-level rules about the security of the information that is created, processed, communicated, stored and saved as back-up and; about changing, accessing to, recording or deleting them to a certain extent and in accordance with certain rules.
- The Security Department Regulation lays down the rules pertaining to the physical security of the building where the Bank operates.
- The Operational Risk Management Regulation lays down the operational risk management rules and principles that will be implemented by the Bank.
- The implementation instructions that is published by the Bank regulates the following matters:

    - Principles on use of network;
    - Network and security software practice;
    - Principles on information security incident management;
    - Principles on IT infrastructure activities as well as on monitoring capacity and performance;
    - IT changes and architecture management;
    - Access to information by support service firms;
    - Software development applications from external sources;
    - Software development applications by internal sources of the Bank;
    - Principles on e-mail use;
    - Use of safe passwords; firewall applications;
    - Masking of critical data;
    - Ensuring suitable system room environment and security;
    - Software development standards and rules;
    - Measures for protection against malicious codes;
    - Principles on provision of remote access;
    - Classification of the assets as well as information assets owned by the Bank;
    - Principles on updating and backing up of data;
    - Implementation principles regarding protection of customer secrets within the framework of the Banking Law.

On the other hand, the Bank has independent companies conduct infiltration tests regularly every year, as per the rules and regulations of the BDDK pertaining to this matter and; the actions that would be taken according to the results of these tests are reported to the BDDK, with the knowledge of the Board of Directors.

Furthermore, the information systems and the banking processes of the Bank is regularly audited by independent audit companies and; these audit reports are discussed by the Audit Committee and the Board of Directors, and also reported to the BDDK.

3. Audit

Fulfilment of the obligations of the Bank under the KVKK is regularly audited within the framework of the rules laid down in this policy and the other applicable written rules and regulations, and within an audit plan that is drafted by the Internal Audit Department of the Bank. The Internal Audit department shall pay a special attention to the audit of implementation of the rules related with protection of the SCPD.

In addition to these, sufficient control processes regarding the practices on processing of personal data are developed within the framework of the internal system practices of the Bank.

4. Third Party Relations

Where the data, for which the Bank is the controller, is processed by other real and legal persons on behalf of the Bank, joint responsibility applies. For this reason, where the Bank uses third parties for processing of the data,

- Provisions to the effect that the responsibilities of the third parties for the protection of personal data would be the same as those of the Bank, will be included in the contracts;
- Should it be deemed necessary and appropriate by the Bank, measures to increase awareness regarding protection of personal data by third persons will be taken;
- Services that would, when appropriate, be obtained from third persons under this scope will be subjected to on-site or off-site audits by the Internal Audit Department.

4. Processing of Personal Data

The Bank can process personal data in accordance with the second paragraph of Article five of Law 6698, or otherwise by obtaining the express consent of the owner of that data on that matter.

4.1 Processing of Personal Data without the Consent of the Data Owner

According to the Law, personal data can be processed without the consent of such persons only under the following circumstances:

a) Where it is explicitly provided in the law;

b) Where it is required for the protection of the life or the integrity of the body of a person, who cannot because of impediments that cannot be overcome, express his consent or whose consent would not be deemed legally valid or; of somebody else;

c) Where it is required for the processing of the personal data that belongs to the parties to the contract, provided that this is directly associated with making or performance of such contact;

c[1]) Where it is required for the fulfilment of the legal responsibility of data executive;

d) Where the data has been disclosed to the public by the concerned person himself;

e) Where processing of the data is required for the constitution, exercise or protection of a right;

f) Where it is required for the legitimate interests of the data executive, provided that the fundamental rights and freedoms of the concerned person are not violated.

In any case, data processing activities of the Bank shall be conducted in compliance with the basic rules on processing of personal data.

4.2 Processing of Personal Data with Express Consent of the Owner of the Data

If any of the above-mentioned circumstances does not exist, processing of a personal data is possible only when the express consent of the owner of that data is obtained.

Where the consent of the person is obtained for processing of the data, such consent should be clear and specific enough not to cause any doubt and; the person must have been given the opportunity to communicate their refusal to give their consent for data processing.

When asking for their consent, it must be sufficiently explained to the persons what data would be processed and; they must also be provided with information as per the provisions of the KVKK pertaining to their enlightenment.

The consent of the persons will be taken in writing, by using a recorded data saver or by any other method permitted by the pertinent legislation.

In principle, data that is processed upon receipt of consent will be used within the limits of and in proportion to the purpose pointed out in the statement of consent. For as long as any one of the conditions listed in the second paragraph of the fifth article of the KVKK does not exist, the data can be processed for another purpose only if the data owner's consent for such purpose is obtained.

4.3 Special Categories of Personal Data

In the law, a special importance is attached to some personal data. Rules that are stricter than those that apply to other personal data are introduced with respect to processing personal data of special categories.

Where provided in the law, the Bank can process the personal data with special categories, other than those about health and sex life, without having to obtain that person's consent. According to the law, data about health and sexual life however, can be processed by the persons or authorized institutions and establishments that are under the obligation of keeping secrets, without having to obtain the concerned person's consent, only with the purpose of protection of public health, preventive medicine, medical diagnosis and health care services as well as for the planning and management of health services and financing of health. In our Bank, health data is, in practice, processed under the scope of human resources procedures, and only to the extent it is required for fulfilling the obligations that originate from Occupational Health and Safety Law 6331. The Bank must also take express consents of the employees. Data about sex life of the persons are not processed by our Bank.

4.4 Informing about Processing of Personal Data

The main communication channel of the Bank is its' corporate web site, after the Law took effect, the Bank put a text providing information as per Article 10 of the KVKK to its web site.

The Bank must enlighten the persons, whose data it processed, on the following matters

Information that is the subject matter of the enlightenment:

- Identity of the Bank as data controller or his representative if there are any;
- Purposes for processing personal data;
- The persons to whom and the purpose for which the data can be transferred;
- The method and the legal reason for collecting the data;
- The persons' legal rights.

The Bank will take the measures that are necessary for sufficient enlightenment of the persons on the KVKK.

Under the following circumstances, the Bank may not be obligated to enlighten:

- Where processing of the personal data is required for prevention of perpetration of an offense or for a criminal investigation;
- Where the personal data, which has been disclosed to the public by the concerned person himself, is processed.

5. Persons' Rights Under the Scope of the KVKK

The persons whose personal data are processed do have the following rights that originate from the Law:

a) To learn whether or not his personal data is processed by the Bank;

b) If his personal data is processed, to ask for information about it;

c) To learn the purpose for which his personal data is processed, and whether or not they are used in accordance with that purpose;

c1) To know the third persons in or outside the country, to which the personal data is transferred;

d) Where the entered personal data is incomplete or incorrect, to ask for their correction;

e) To ask, within the framework of the conditions provided in the KVKK, for the deletion or destruction of the personal data;

f) To ask for the notification of the actions carried out according to subparagraphs "d" and "e", to the third persons, to whom the personal data has been transferred;

g) To raise objection to the emergence of an unfavorable result upon analysis of the processed data exclusively by automatic systems;

g1) To ask for compensation of losses incurred as the result of unlawful processing of the personal data.

The Bank will take all measures that are necessary for the persons to fully and appropriately exercise the above-listed rights.

6. Transfer of Personal Data to Third Parties

Personal data can be transferred to third persons only in cases mentioned in Articles 8 and 9 of the KVKK, without prejudice to the provisions in the other laws, first and foremost the Banking Law.

Personal data can be transferred in accordance with the KVKK, only in below mentioned cases:

- Where it can be processed as per the KVKK without the person's consent;
- Provided that sufficient measures are taken, where personal data with special characteristics, except those about health and sex life, are processed in accordance with the third paragraph of the sixth article of the KVKK; where any one of the conditions that require processing of the data about health and sex life exists;
- Where the express consent of the person about transfer of the data has been obtained.

Personal data can be transferred to abroad, only to the countries that the Board would announce as countries where sufficient protection exists, and only in cases mentioned at above. When data transfer to a country, where sufficient protection to be announced does not exist, is considered, the data cannot be transferred without obtaining a guarantee letter from the organization and without the permission of the Board.

Personal data can, within the framework of the explanations at above, be transferred to the following persons and groups:

Person/Group That Data Can Be Transferred To	Definition	Purpose of Data Transfer
Main shareholder of the Bank	Means the main shareholder of the Bank.	Limited to the purposes listed in Article 73 of the Banking Law (preparing consolidated financial statement, risk management and auditing activities).
Our subsidiaries	Mean the companies that our Bank is a shareholder.	Continuation of the activities of the Bank, which requires also the participation of the Bank's associates; carrying out of the services provided by the associates to the Bank, and to the associates by the Bank.

Legally Authorized Public Institutions and Organizations	Means the official institutions and organizations that are authorized to demand, in accordance with the authority provided by law, information that constitute customer secrets.	With the authority and purpose stated in the laws that pertain to such public institutions and organizations.
Legally authorized private law entities	Means the Private Law Entities that are authorized to demand, according to the provisions of the pertinent legislation, information and documents from our Bank	Within the limits of the purpose for making such demand as per the pertinent legally given authority.
Our business partners/organizations from which service is procured	Means the persons or organization with which our Bank does business or procure services under a certain contract.	With the purpose of performance of joint activities, or performance of services by the service providing persons and organizations.
Other persons and organizations mentioned in the Banking Law	Other persons and organizations mentioned in Article 73, with heading "Keeping of Secrets", of the Banking Law.	Within the framework of the confidentiality agreement, for the purposes mentioned in Article 73

7. Categorization of Personal Data

Personal data are, with respect to the purposes of this policy, grouped under the topics indicated in the table at below. Each one of these data groups contains numerous detailed data items. The Bank will make separate assessments for each of these data groups and items and; will designate the data it can process according to the KVKK and the other pertinent legislation without also receiving the data owners' approval, and the data for which it must obtain the data owner's consent as well as the method and purpose of obtaining such data.

Data processing requirements are integrated with the new product and activity processes of the Bank for the data groups indicated on table at below. When making the assessment of the demands for new products and activities, the purpose for which every different personal data would be processed; whether or not processing of the data other than those that are already processed is needed and; whether if the person's consent is needed for the data processing activities will be considered as part of the risk analysis.

Data Group	Explanation of the data
Identity Details	Means all information that help identification of the real person. They also include the identity details that are used to identify that person.

Work/Job Details	They include information about the current and past work experience of the real persons, their employment status, manner and profession as well as the pay and income they get for these jobs.
Address Details	Work and home address details of the real persons, and information on the duration of their stay at those addresses.
Communication Details	Means the contact details of real persons, including home, work and mobile phone numbers as well as e-mail and registered e-mail (KEP) addresses and fax numbers.
Financial Details	Includes all kinds of information about a person's financial standing, transaction profile and capacity like personal and household income and expenses, assets, company partnership or ownerships, other financial activities, credit limit and risk details, tax liabilities etc..
Family Details	Includes all kinds of information about the family and first and foremost the names of the family members of the real persons.
Training/Education Details	Includes information about the education backgrounds of the real persons, the schools they go and were graduated from, their grades, the special training and seminars they attended, the certificates they have, their fields of expertise and capabilities, etc..
Physical Features	Includes information about the appearance and voice of the person.
Social Details	All kinds of information about the social life of the real persons.
Medical Details	Information about the medical conditions of the real persons. It includes information on his general state of health, past medical record, disabilities if any.
Sexual Preferences	Information about the sexual preferences of the real persons.
Genetic and Biometric Data	All kinds of genetic and biometric data that helps identification of real persons.
Other Information	It is any data that does not fall under the scope of any of the above-mentioned data groups. It includes also the information about the race, political thought, philosophical believes, sects, other believes, outfit, affiliations to societies and foundations, and criminal records of the real persons and; the restrictive security measures they are subjected to.

8. Groups of Persons Whose Data is Processed

The Bank can, during carrying out the activities that fall under the scope of the fourth article of the Banking Law, process the data groups listed at above, in accordance with the characteristics of the activity and the persons are parties to such activities, as required by the pertinent legislation and the KVKK. The group of persons whose personal data is or can be processed, depending of the nature of the activities of the Bank, are classified as follows

Group of Persons	Scope
Customer	Means any real persons for which a customer number is assigned in the banking system, even if a product/service is or is not defined for him.
Applicants (for credit and other banking products and services)	Means any person who had applied to the Bank for banking products and services (even if he has not used it). Details will depend of product types.
Spouses, children and other family members	Means the spouse, children or other family members of any person of whose personal data is processed by the Bank
Guarantors	Means any real persons who stand or suggested as guarantor for any loans.
Shareholder/controller of a legal entity	Means a real person shareholder of an existing or potential legal entity customers or who controls those entities and beneficial owners.
Authorized person/representative of a legal entity	Means an authorized real person and/or a person who represents an organization that is not a legal entity.
Parents, proxies, guardians or similar persons	Parents, proxies or guardians of the persons of whom the Bank is processing personal data.
Personnel	Means the current and former employees of the Bank.
Personnel candidate	Means any person who has applied for a job in the Bank and who has sent his CV for this purpose but not was not accepted as an employee .
Member of the Board of Directors	Means any existing or former members of the Board of Directors of the Bank.
Service providers	Any employee of a service provider corporation from which the Bank procures services, or any real person from whom service is procured directly.
Visitors	Any visitor who comes to any building where the Bank provides its services, or who visits the web page administered by the Bank.
Other	All other individuals not stated above whose personal data are processes according to KVKK and this policy

8.1 Data Processing Activities Carried Out at the Entrance of or Inside the Building, and the Internet Web Page Visitors

a) Monitoring Activities at Entrances and Exit Points of the Buildings;

Our Bank conducts visual monitoring and recording activities at the entrance and within the building, with the purpose of ensuring the safety and security of the Bank's employees, the visitors as well as the building itself and the fixtures in it. Recording of the images and voices of the persons is considered as a data processing activity.

Our Bank conducts all of these data processing activities in compliance with the privacy obligations, first and foremost those imposed by the Constitution.

The visual monitoring and recording activities that are carried out by the Bank are conducted within the framework of the Law Pertaining to Private Security Services and of the other pertinent legislation. Access to this data is granted only to certain employees within the framework of their duties, authorities and responsibilities.

Visual recording is made at the entrance and reception desk of the building, to monitor the person who enter and leave. Visual monitoring and recording activities inside the building are conducted entirely and exclusively for security purposes, and when selecting the places that would be monitored and that the cameras would be located, any violation of privacy (monitoring of the toilets, etc.) is disallowed.

b) Internet Access, Web Site Visitors

Where cable or wireless Internet access is offered in the Head Office building, to those who are not the employees of the Bank, such internet access records are logged in accordance with Law 5651 on the Regulation of Internet Publications and on Fighting the Crimes that are Committed via Such Publications and; these logs are processed only when they are required by the competent authorities as per the said law, or under the scope of legal obligations regarding risk management/control or supervision activity.

The surfing activities of the visitors of our web pages inside our Internet site would be recorded by using available technical tools like cookies, with the purpose of facilitating their visits according to their expectations; offering them customized content and; allowing online advertisement activities.

9. Media Where Personal Data Is Stored

Personal data can be processed by completely automated processes as well as non-automated ways as part of a data recording system.

Within this scope, personal data can be processed and stored in the following media:

- In electronic environment through digital and electronic banking and loan applications.
- In applications and servers where the Bank's systems reside, within the scope of applications, customer onboarding and banking transactions of customers.

- In the servers where the electronic copies of documents bearing the personal data or all kinds of electronic files with personal data are stored.
- Within the head office, in the physical files and documents where personal data is stored, such as customer documents, loan application documents, collateral documents etc., within the Head Office Archive Room and in Central Archive area.
- Within the computers used by the Bank employees, in electronic format.
- By other real and legal persons as data processors, from whom the Bank procures service.

The Bank has already taken the necessary measures for protecting the security of the media listed above. Moreover, when it is necessary to share the personal data with the third parties, within the scope of service relationship, the liabilities related with protection of the personal data are clearly described in the service agreements, according to the BRSA regulation on support services, KVKK and its sub-regulations.

10. The Policy of Processing Special Categories of Personal Data

Based on special emphasis in the KVKK on the special categories of personal data, the Bank had a separate policy on processing, retention and security of such data. Rules set in this policy with regard to processing special categories of personal data are applied in addition to rules set in the other sections of this policy document.

10.1 Basic Approach of the Bank in Processing Special Categories of Personal Data (SCPD)

SPCD was defined in the relevant law in a limited manner by listing such data. The Bank has determined the list of its SCPD processed as part of its activities, during the data inventory works, according to the law.

The Bank will process the SCPD if it is required by laws and in other cases only if it is mandatory. Such cases are accepted as exceptional. Within the scope of new product/activity procedures of the Bank, the units demanding the new product or activity shall indicate in the risk analysis forms if there is a need to process SCPD. In such cases, the demand for processing the SCPD will be assessed by the relevant departments captiously.

The main approach of the Bank concerning processing of the SCPD is explained in the following table as per data types.

Type of the SCPD	Scope of the Data	Explanations
Race	Data about a persons' race	Will not be processed by the Bank
Ethnical origin	Data about the ethnical origin of a person	Will not be processed by the Bank
Political opinion	Data about political opinion that a person has	Will not be processed by the Bank
Philosophical opinion	Data about philosophical opinion of a person	Will not be processed by the Bank
Religion	Data about the religious belief of or if a person has any religious belief or not	Will not be processed by the Bank. On the other hand the ID documents (nüfus cüzdanı) used in Turkey may contain the religion information on it. When, in the cases requiring identification, it is done by using the nüfus cüzdanı, then a document containing religion information enters into the files of the Bank. The Bank may take an electronic copy or file such a document it newly received only by masking the said information.
Sect	Data about religious sect of a person	Will not be processed by the Bank
Other beliefs	Every kind of beliefs of a person that can be classified under other names.	Will not be processed by the Bank
Appearance	Data about way of dressing of a person	Will not be processed by the Bank
Association, foundation or syndicate membership	Data indicating if the person has a membership in an association, foundation or syndicate and if he/she does, the name of such institution.	Will not be processed by the Bank
Health	Data about general or particular health situation of a person	Health information of the following groups will be processed by the Bank in order to fulfil various legal requirements: • Existing and potential customers (In relation to liabilities about easing access to banking products and services by handicapped persons) • Bank employees • Employee candidates In processing the health data of the persons, the Bank hall obtain an explicit consent of the data subject.
Sexual life	Data of sexual life of a person	Will not be processed by the Bank
Criminal records and security measures	Data indicating if the person has any criminal records or if there are security measures applied against him/her.	Criminal records of Bank employees (AGM and above level) and members of the board of directors are processed based on the liabilities coming the Banking Law. Data of other bank employees can be processes by getting explicit consent of the data subject.
Biometric data	Physical or behavioural data that can be used to identify the person	The Bank does not use biometric data for identification. Therefore, the Bank does not process such data. When there is a need to use biometric data for identification, Bank can process it by getting the explicit consent of the data subject.
Genetic data	Data of hereditary or nonhereditary DNA information of a person	Will not be processed by the Bank

As explained in the above table too, the Bank process SCPD for very limited situations and purposes.

When getting the consent of the data subject to process the SCPD, it should be received only if the subject is enlightened concerning which type of data will be processed and for what persons; if the data needs to be transferred, to whom they would be transferred and other subjects as required in the KVKK. In this matter, the Bank needs to act more cautiously and meticulously compared to processing of normal personal data.

10.2 Measures Concerning Processing of the SCPD

The Bank has a lot of processes and practices in order to ensure security of the data based on the liability of protecting customer secrecy required by the Banking Law and its sub-regulations. The measures here shall be applied as additional measures to the existing ones.

a) Measures Concerning SCPD Processing Processes

1. The SCPD processing activities of the Bank are already very limited. In the cases that the SCPD is processed, access to such data shall be restricted to only a limited user group.
2. In the case that the religion information obtained from the data subject as part of identification requirement, the data shall not be retained on the core banking system or any other systems used by the Bank; the data shall be masked on the physical documents.
3. Only a very limited user group can access the files containing the health data of the employees. As a rule, the workplace doctor will keep the health files. The Bank shall keep minimum level of health data on the PYS. (Personal Management System application)
4. Trainings: The Bank gives regular trainings to its employees concerning personal data protection regulations and relevant bank processes. During these trainings special emphasis will be on the need for special protection of the SCPD and measures for that purpose.
5. In the agreements that the Bank will sign with third party service providers and its employees, special provisions should be added as to the protection of the SCPD. The executive of the new employee takes necessary measures in order to prevent access of the employee to such data, before signing the said agreement.
6. Demands of third parties for obtaining the SCPD must be evaluated by the Bank very cautiously. The Bank shall refuse such demands that are not explicitly in accordance with the Banking Law,

KVKK and other relevant legislation. In transferring the SCPD to the third parties, the Bank shall strictly comply with the articles 6, 8 and 9 of the KVKK.

7. The Internal Audit Department shall pay a special attention to the audit of implementation of bank rules concerning protection of the SCPD during its audits related with the personal data protection legislation.
8. Only a small group of users shall have access to the screens where the SCPD is retained in the core banking system considering the nature of the activity as well. Such access rights will separately be reviewed during the regular reviews of role and authority matrices. Even if the SCPD is available in the database, they should not be seeable in the user screens as long as it is required by the nature of the activity.
9. In the case that a bank employee who has access rights to the SCPD left the Bank or moved to another role that does not have such access rights, the Bank shall immediately cancel his/her existing access rights. Physical materials containing the SCPD that had been delivered to the said person, shall be retrieved in the shortest time.

b) Measures Concerning Security of Environments Retaining the SCPD

If these environments are electronic;

- The data shall be kept by using cryptographic methods and the code shall be kept in a secure separate environment.
- If the data is kept in an electronic office file created by the users, then the file must be protected by a password. The opening password should be long and complex enough to ensure an adequate level of protection. The department or the employee who created the file must take the required measures to protect the security of the password.
- Transactions on the SCPD fields in the banking systems used by the Bank shall be logged in the secure way.
- The Bank provides for the necessary security tools for the environments where the SCPD is retained and regularly updates these tools. As per the BRSA regulations, regular penetration test are conducted and necessary actions are taken in order to close the findings detected during these tests.
- If there is a need for a remote connection to environments where the SCPD is retained, a double verification mechanism must be used.

If these environments are physical;

- The Bank takes necessary measures in those environments against the risk of fire, electrical leakage, flood or similar physical threats.

- Access to archiving environments of the Bank is restricted and the relevant departments take necessary measures to prevent unauthorized access.
- In order to ensure security of environments containing the SCPD sufficient measures are taken. This is mainly the responsibility of the executive of the relevant department. These measures include at the minimum level keeping the SCPD data in locked cabinets, implementation of clean desk principle and processing the least data possible.
- The department executives take necessary measures in order not to share the physical environments containing such data with the irrelevant parties.

c) Measures Concerning Transferring of the SCPD to Third Parties

The Bank will not transfer the SCPD to third parties as long as it is not mandatory based on the nature of the activity.

- In the agreements to be signed with the third parties, if the SCPD will be transferred, provisions will be added in order to ensure the security of the said data.
- If the SCPD will be transferred to the parties out of the Bank, it will take measures to ensure the security of messages and document deliveries. Within this scope, measures such as encrypting the data, transferring the date via VPN, and sFTP, putting warning remarks on documents in order to secure its confidentiality.

11. The Policy of Destruction of Personal Data

Where, according to the KVKK, the reason for processing the personal data ceases to exist, the data controller must, at his own initiative or upon the request of the concerned person, destructs them.

According to Article 42 of the Banking Law, the original copies of the letters received by the Bank and of the documents regarding the activities, or if this is not possible, their undoubtedly reliable copies and the dated and numbered copies of the letters, as reproduced by machines, must be kept by the Bank for a period of ten years, within the framework of applicable procedures. They can also be kept in the form of microfilm and microfiche, or on magnetic or similar media. The procedures and principles on the implementation of this article are laid down by the BDDK, by regulations.

On the other hand, in Article 62 of the Banking Law, savings, participation funds and deposits with, and the claims from the Bank are subject to ten-year statute of limitations, which starts to run from the latest request or transaction or written instruction of their owner.

In the MASAK legislation as well there are obligations regarding such keeping or custody. According to Article 8 of Law 5549 Pertaining to Money Laundering and Prevention of Financing of Terror, any document regarding the obligations and transactions under the scope of this Law, and on any kind of media, must be kept for a period of eight years, starting from the latest date of entry in the books and records and; where such document is about identification, starting from the date of latest transaction.

In Tax Procedure Law and Turkish Commercial Code, there also are provisions of statute of limitation regarding accounting books and documents.

The Bank will, under the scope of processing of personal data, keep such personal data for the duration of the statutory period, in accordance with the scope and purpose of the processed data, and first and foremost with the above-mentioned legislation. Upon elapse of such period, the legislation then in force will apply to the deletion, destruction and anonymization of such data.

11.1 Factors Requiring Destruction of Personal Data

Data for which the legal retention time ended or the data that retention is not required legally, will be deleted, destroyed or anonymized in the following cases: (Excluding the situations that an appropriate consent of the related person is received by the Bank to continue processing the data)

- Revision or cancellation of legal regulations which are considered as the reason of data processing.
- Invalidity of the agreement that is the base of data processing, ending the agreement period, termination of or reneging from it.
- The purpose of data processing is not valid anymore.
- Processing the data is against the law and good faith.
- Retrieving the data processing consent by the client, in cases where consent is required for processing.
- Acceptance of the related persons' application by the data controller, concerning processing his/her data, based on the rights stated in the Law, article 11 and sub-articles (e) and (f).
- Application of the related person to the Board and acceptance of the person's demand by it, in cases that the Bank refused the person's demand for deleting, destroying or anonymizing his/her data; or the response of the Bank to such a demand was considered to be insufficient by the person; or the Bank did not send a response to the applicant in due time.

- There are no situations that rationalize retention of the data for which maximum retention period ended.
- The conditions described in articles 5 and 6 of KVKK are no longer applicable.

11.2 Determination of Personal Data That Will Be Destructed

The personal data exists in the data inventory of the Bank that needs to be destructed will be determined by the department executives under the coordination of the Personal Data Committee every six months and they are communicated to the committee. In the Bank's practice the periodical destruction times are March and September.

Person categories and data groups sent by the department executives are evaluated by the committee and it is decided if factors that required destruction exists. Additionally, if there are other data groups that needs to be destructed, they are identified. Operations must be completed by the end of the month following the six-monthly periods. If other periods are set in the legal regulations or by the Board, those periods will apply.

The method to be used for the data that will not be processed by the Bank any more will be determined by the Committee, by getting the opinion of concerned departments when necessary. In accordance to the decision to be taken, the person who will perform the transaction destructs the data and those operations are recorded. Procedural details are determined by the Bank management with implementation instructions. The Personal Data Committee shall take required technical or administrative measures in order to make sure that the destruction operations are conducted in an appropriate manner.

Completion of operations for the data decided by the Committee, to destruct is controlled by the Internal Control and Compliance Department using an appropriate control method to be determined by itself. Such operations are also audited by the Internal Audit Department during its audits. During the controls and audits, it is controlled or audited if the operations of the Bank for destructing the data are carried out in accordance with the KVKK and its sub-regulations as well as the Bank's policy and procedures.

11.3 Destruction Methods

In the relevant legislation, three methods have been determined to destruct the personal data, which are deleting, anonymizing and destroying.

Deleting the personal data is the transaction of making the data non-accessible and non-reusable by the concerned users by no means

Destroying the data is the operation of making all the physical recording means which are available to store data non-usable and non-recoverable.

Anonymizing the data means making it not possible to identify or possible to identify the related person using the data even by combining with other data

The data controller or processors need to anonymize the data in a way that it would not possible to connect the data to an identified or identifiable person;

a) By using appropriate techniques in terms of recording media and relevant activity area.
b) By using recovery techniques or by matching with other data.

11.4 Destructing the Data upon the Demand of the Data Subjects

In the case that the Bank receives a demand from a data subject destructing his/her personal data, the first thing to be done is to determine if the legal liabilities of the Bank concerning the processing of the concerned data continues or not, by the relevant departments. If needed, the required decision is taken by the Personal Data Committee.

If the Bank determines that the Bank must continue to process the data, the demand of the person is concluded within the time period defined in the legal regulations and he/she is informed about the result of his/her application in a written or electronic way.

If there are no valid reasons to continue processing the data, the data subject will be informed within the time determined in the legal regulations and the destruction operations will be carried out according to legal and internal regulations available at the time of destruction.

11.5 Measures Concerning Destruction Processes

The following measures shall apply in order to ensure that destruction operations are carried out in accordance with the legal regulations and bank procedures for the data decided to be destructed:

- The Bank employees will be trained as to how the destruction should be made.

- The Internal Control and Compliance Department, using an appropriate control method, shall control destruction operations.
- The Internal Audit Department audits if the destruction operations are carried out in accordance with the legal and internal regulations.
- IT Developments for destruction of data in the core banking system will be tested in the test environment by the relevant departments in order to make sure the rules work correctly. When the rules run in the production environment, results are controlled again in order to verify that the destruction is completed successfully.
- Data to be destructed but kept in the archives of the Bank will not be demanded by the concerned users from the department or persons who are responsible from technical storage, protection and backup of the said data. The said personnel need to question if the demanded data is a data subject to destruction or not and has to reject the demand if the data is a destructed data.
- The Personal Data Committee keep records of periodic destruction works and performs monitoring of the whole process.

12. Management of Demands Under the Scope of the KVKK

The provisions on the rights of the owners of the personal data and the way these rights would be exercised, are included in Article 13 of the KVKK.

They can, within the framework of their rights under this Law, communicate their demands regarding their personal data, in writing, by using the Bank's website, or by using any other method that would be decided by the Board.

Such demands of the persons from the Bank regarding this matter will be considered with priority, and an answer must be given to them as soon as possible, but latest in 30 days. The process regarding it will be followed up by the Internal Control and Compliance Management, and the Personal Data Committee and when necessary, the Management Committee will be informed about any problems that may be encountered.

The Bank will conduct a reasonable inquiry to verify that the demanding person is indeed the owner of such data. In such matters, first and foremost, the provisions of the Banking Law pertaining to the protection of customer secrets will be observed.

The Bank has the right to reject the following demands, by also explaining the reason for it:

- Any application that is made by any person who does not own the data;
- Any application that had been answered in the past, by the Bank;
- Processing of personal data by anonymizing them by converting into official statistics, for purposes like research, planning and statistics;
- Other cases stated in the pertinent legislation.

You may find more information about protection of personal data in the official web site of the Personal Data Protection Institution. Please click here for the web site.

Please click here to read our Bank's public disclosure text for processing of personal data.

For your applications under the Protection of Personal Data Law, you can use the application form available in our corporate web site:

https://www.bankpozitif.com.tr/En/AboutUs