

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

TABLE OF CONTENTS

- I. Introduction**
- II. Policy Holder**
- III. Purpose**
- IV. Scope**
- V. Update**
- VI. Definitions**
- VII. Roles and Responsibilities**
 - 1. Data Inventory Responsible
 - 2. Data Controllers' Contact Person
 - 3. Senior Management of the Data Controller
 - 4. PDP Advisory Group
- VIII. Approval**
- IX. Data Subject**
- X. Data Categories**
- XI. Activities and Objectives for Processing and Exchanging Personal Data**
- XII. Measures Taken when Transferring Data to Third Party Service Providers**
- XIII. Data Protection Policy and Procedures**
- XIV. Risk Analysis**
- XV. Non-Policy Situations**
- XVI. Principles of Processing Personal Data**
 - 1. Lawfulness and fairness
 - 2. Being accurate and kept up to date where necessary.
 - 3. Being processed for specified, explicit and legitimate purposes.
 - 4. Being relevant, limited and proportionate to the purposes for which they are processed.
 - 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.
 - 6. Building Entrances and Activities of Personal Data Processing and Network and Website Users
 - 7. Processing of Customers' and Business Partners' Data
 - 8. Processing of Employees' and Candidate Employees' Data
- XVII. Terms of Processing Personal Data**
 - 1. Identification and Processing of Personal Data
 - 2. Exceptions
 - 3. Processing Special Categories of Personal Data
 - 4. Transfer of Personal Data
- XVIII. Data Controller's Obligations**
 - 1. Obligation to Inform Data Subject
 - 2. Obligation to Respond to the Request of Data Subject
 - 3. Obligation to Ensure Security of Personal Data
 - 4. Taking Technical and Administrative Measures for Providing Legal Data Processing
 - 5. Taking Technical and Administrative Measures to Prevent Illegal Access to Personal Data
 - 6. Obligation to Register to Data Controllers' Registry
 - 7. Erasure, Destruction, and Anonymization of Personal Data

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

I. Introduction

With this policy, within the framework of the Personal Data Protection Law (Law) and relevant national legislation no. 6698; the rules to be followed with the principles adopted by ARKAS HOLDING A.S (Data Controller) regarding the collection, processing, transfer, update, and destruction of personal data have been determined.

II. Policy Holder

The owner of Personal Data Protection and Processing Policy is ARKAS HOLDING A.S as the Data Controller.

III. Purpose

With this policy, it is aimed to provide explanations about the rules adopted by the Data Controller for the processing of personal data and the protection of personal data; in this context, it is aimed to ensure transparency and inform the persons whose personal data are processed by our company, business partners, employees and candidate employees, current and potential customers, shareholders, visitors and third parties.

IV. Scope

This policy covers shareholders and partners, employees, candidate employees, interns, sub-contractors, suppliers, current and potential customers, visitors and third parties.

V. Update

Personal Data Protection and Processing Policy is reviewed and recorded once a year regardless of the change requirements in its corporate or legal content. The most up-to-date version is published on the data controller's website.

VI. Definitions

Definitions not included herein shall be used as defined in the Law and regulations.

- *Explicit Consent*: Freely given, specific and informed consent.
- *Anonymization*; Rendering personal data impossible to link with an identified or identifiable natural person, even though matching them with other data.
- *Obligation to Inform*: At the time when personal data are obtained, the data controller or the person authorised by it is obliged to inform the data subjects the identity of the data controller and of its representative, if any; the purpose of processing of personal data; to whom and for which purposes the processed personal data may be transferred; the method and legal basis of collection of personal data and other rights referred by Law.
- *Data Subject*: Natural person whose personal data are being processed.
- *Personal Data*: Refers to any information relating to an identified or identifiable natural person; such as name, surname, date of birth and place of birth of the persons, information about the physical, family, economic and other characteristics of the person, name, telephone number, motor vehicle license plate, social security number, passport number.

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

- *Processing of Personal Data*: Refers to 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.
- *Special Categories of Personal Data*: Refers to 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.
- *Data Processor*: Means the natural or legal person who processes personal data on behalf of the data controller upon its authorization. These persons are separate natural or legal persons authorized by the Data Controller through a personal data processing agreement, who process personal data within the framework of the instructions given to them. Any natural or legal person can be both a Data Controller and a Data Processor at the same time.
- *Data Controller*: Means 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 Controllers' Registry (VERBİS)*: Data Controllers' Registry (VERBİS) is an information system that is accessible on the Internet and established and managed by the Presidency under supervision of the Board which is the managing body of the Authority (Personal Data Protection Authority), that data controllers will use for the registration with the Registry and the other operations related to the Registry.

VII. Roles and Responsibilities

Four different roles have been identified that complement each other under the Personal Data Protection and Processing Policy.

1. Data Inventory Responsible

Two "Data Inventory Responsible" are assigned -one principal and one substitute member- by the Data Controller. The Data Inventory Responsible has the responsibilities listed below.

- 1.1. The Data Inventory Responsible shall establish a detailed personal data processing inventory with all employees of the Data Controller to which he/she is affiliated and coordinate the related activities.
- 1.2. To follow the changes and regulations in the data processing activities and to keep the inventory up to date.
- 1.3. Inform the Data Controllers' Contact Person regarding prospective changes in the inventory.
- 1.4. Perform the work and transactions specified in the company's policies, procedures and instructions.

2. Data Controllers' Contact Person (DCCP)

There is a "Data Controllers' Contact Person" assigned to each Data Controller. The Data Controllers' Contact Person has the responsibilities listed below.

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

- 2.1. The Data Controllers' Contact Person is aware of all processes and activities related to the protection of personal data within the Data Controller to which he/she is assigned.
 - 2.2. Representing the Data Controller in official and internal audit processes, taking the actions requested and needed, ensuring that they are finalized.
 - 2.3. Responding requests from data subjects.
 - 2.4. Informing the company management, the Personal Data Protection Advisory Group and the Legal Department in case of a data breach.
 - 2.5. Monitoring changes in the data processing activities reported by the Data Controller and related units in the areas of responsibility together with the Data Inventory Responsible and keeping the inventory up to date.
 - 2.6. Informing the Authority of any changes in the information recorded in the VERBİS within seven days from the date of occurrence of the change via VERBİS.
 - 2.7. Ensuring communication with the Authority.
 - 2.8. Duly make legally necessary notices in case of data breach
 - 2.9. Perform the work and transactions specified in the company's policies, procedures and instructions.
3. *Senior Management of Data Controller*
- 3.1. Duty of the Senior Data Controller Management (Chairman of the Board of Directors, General Manager, etc.) is to control the Data Controllers' Contact Person's duty as described in the Law.
 - 3.2. The changes and assignments of the Data Controllers' Contact Person and Data Inventory Responsible shall be made by the Data Controller's Senior Management upon the termination of the employment contract and notified to the Personal Data Protection Advisory Group.
4. *PDP Advisory Group*
- 4.1. Personal Data Protection Advisory Group is responsible for preparing, updating and auditing the Personal Data Protection Law policies and procedures that will be applicable for the Data Controller.
 - 4.2. Following updates and amendments to the legislation of the Law.
 - 4.3. Taking necessary actions for situations that require updating in administrative and technical measures.
 - 4.4. Providing consultancy for personal data protection throughout Arkas Group companies.
 - 4.5. Provides consultancy on the actions covered by the legislation, such as Authority's audit and inspection, data subject's request, complaints, etc.

VIII. Approval

The relevant senior management representatives approve the policy prepared by the Personal Data Protection Advisory Group on behalf of the Data Controller.

IX. Data Subject

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

Personal data of the employee, candidate employee, person appearing in news, shareholder/partner, potential customer, intern, supplier's employee, supplier' officer, customer, parent/custodian/representative, visitors, etc. natural persons are processed.

X. Data Categories

Identity, communication, location, personal information, legal transaction, customer transaction, physical environment security, transaction security, risk management, finance, professional experience, marketing, visual and audio records, philosophical belief, religion, sect and other beliefs, association membership, health information, criminal conviction and security measures, and biometric data are processed following the purpose of personal data processing.

XI. Activities and Objectives for Processing and Sharing Personal Data

Personal data shall be processed for the purposes listed above and limited to the activities of the Conducting Emergency Management Processes, Conducting Information Security Processes, Execution of Employee Satisfaction and Loyalty Processes, Fulfilment of the Obligations of Employees arising from Employment Contract and Legislation, Execution of Benefits Processes for Employees, Conducting Audit / Ethical Activities, Conducting Training Activities, Execution of Access Rights, Conducting Activities in Accordance with the Legislation, Execution of Finance and Accounting, Ensuring Physical Security, Execution of Assignment Processes, Monitoring and Execution of Legal Affairs, Execution of Internal Audit / Investigation / Intelligence Activities, Conducting Communication Activities, Planning Human Resources Processes, Execution / Audit of Business Activities, Conducting Occupational Health / Work Safety Activities Taking and Evaluating Suggestions for Improvement of Business Processes, Conducting Business Continuity Activities, Conducting Logistics Activities, Execution of the Procurement Process of Goods / Services, Execution of After Sales Support Services, Execution of Sales of Goods / Services, Execution of Production and Operation Processes of Goods / Services, Execution of Customer Relationship Management Processes Organization and Event Management, Conducting Performance Evaluation Processes, Conducting Advertising / Campaign / Promotion Processes, Execution of Risk Management Processes, Custody and Archive Activities Social Responsibility and Civil Society Activities, Conduct of Contract Processes, Conducting Strategic Planning Activities, Tracking of Requests / Complaints, Ensuring Security of Movable Goods and Resources, Execution of Remuneration Policy, Ensuring the Security of Data Controller's Operations, Conducting Marketing Processes of Products / Services, Foreign Personnel Work And Residence Permit Procedures Informing Authorized Persons, Institutions and Organizations, Execution of Management Activities.

Personal data is transferred to our business partners and suppliers, Arkas Holding S.A and its affiliates/subsidiaries, legally competent public institutions, organizations and persons following the basic principles stipulated by the Law and within the scope of the personal data processing conditions and purposes specified in Articles 8 and 9 of the Law and for the purposes set out above.

XII. Measures Taken when Transferring Data to Third Party Service Providers

Articles for the protection of personal data are added to contracts and annexes made with third-party service providers, a separate confidentiality agreement is made, additional commitment or protocols are issued and the said service providers are audited and it is checked whether the personal data are properly protected. In addition, a "Framework Data Transfer Agreement" is

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

organized between group companies and affiliates and subsidiaries and personal data sharing is organized within the Group.

XIII. Data Protection Policy and Procedures

This policy includes the general requirements for the protection and processing of personal data within the Data Controller.

1. "Personal Data Storage and Disposal Policy" includes rules and procedures for the storage and disposal of personal data within the Data Controller.
2. "Special Categories of Personal Data Processing and Protection Policy" includes the rules and procedures governing the terms and methods of processing specific to sensitive personal data within the Data Controller.
3. The purpose of "Employee Personal Data Protection and Processing Policy" includes the rules and procedures governing the protection and processing of personal data about the persons working within the Data Controller.
4. "Information Systems General Standards and Security Policy" ensures the security and confidentiality of information and data in all kinds of commercial and operational electronic, written or other environments; determines the general principles regarding the processing of personal data for employees.
5. It is ensured that the processes of informing the persons related to the Obligation to Inform and Explicit Consent texts and processing personal data in accordance with the Law.
6. The employees are informed about the Law via internal training and aimed to raise awareness.
7. Procedure of Handling Data Subject Requests within the Data Controller, the rules and conditions of the process of investigating, responding to the requests from the data subjects and taking the necessary actions regarding these requests are determined.
8. Within the Data Controller, personal data processing activities are regularly audited.

XIV. Risk Analysis

Risk findings arising as a result of the audits carried out regularly by the Internal Audit Department are evaluated with the Personal Data Protection Advisory Group. Arkas Holding A.Ş. and its affiliated companies are informed about the actions to be taken or the processes to be changed and the relevant Data Controller is ensured to take the necessary measures.

XV. Non-Policy Situations

Persons who detect different practices other than those describe in this policy shall receive support from the Data Controllers' Contact Person and Data Officials and inform the Personal Data Protection Advisory Group in writing.

XVI. Principles of Personal Data Processing

In order to ensure compliance with the Law, personal data are processed in accordance with the general principles and provisions stipulated in the legislation. In this context, the Data Controller acts in accordance with the principles listed below in the processing of personal data in accordance with the legislation related to the Law.

1. *Lawfulness and fairness*

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

The Data Controller acts in accordance with the Law and the rules of integrity within the scope of personal data processing activities.

2. Being accurate and kept up to date where necessary

The Data Controller shall establish the necessary systems to ensure that the personal data processed by taking into account the fundamental rights of personal data owners and their legitimate interests are accurate and up-to-date and to take necessary measures accordingly.

3. Being processed for specified, explicit and legitimate purposes

The Data Controller determines for what purpose personal data will be processed and submits these purposes to the data subjects' information before personal data is processed. Personal data shall not be processed except for the legitimate and lawful purposes specified.

4. Being relevant, limited and proportionate to the purposes for which they are processed

Data Controller; handles personal data in a manner that is conducive to achieving the specified purposes and avoids the processing of personal data that is not relevant or needed in achieving the purpose. In this context, it takes into account proportionality requirements and does not use personal data other than for the purpose of processing.

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.

The Data Controller primarily determines whether a period is foreseen for the storage of personal data in the relevant legislation. If a storage period is determined, it acts in accordance with this period. If a period of time has not been determined, it retains personal data for the time required for the purpose in which they are processed.

6. Building Entrances and Activities of Personal Data Processing and Network and Website Users

In order to ensure security by the Data Controller, personal data processing activities are executed in the premises and facilities of the Data Controller for monitoring the guest entrance and exit. Personal data processing is executed by the Data Controller through the use of security cameras and the recording of guest entrance and exit.

Image records of our visitors and all data subjects are taken at the entrances of the Data Controller's building, facility and within the facility via camera and monitoring system; visitor list including name, surname, ID number, driver's license number, passport number, personnel registration number, title, work domain, gender, company name, date and time of entry and exit, vehicle license plate information is kept.

The Data Controller aims to increase the quality of the service provided, to ensure its reliability, to ensure the security of the Data Controller, customers, and third parties and to protect the interests of the customers regarding the service they receive within the scope of surveillance activity with the security camera.

The regulations contained in the Law and the "Law on Private Security Services" no. 5188 and the relevant legislation are executed in accordance with the regulation of the conduct of camera monitoring activities by the Data Controller for security purposes.

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

In accordance with Article 12 of the Law, necessary technical and administrative measures are taken to ensure the security of personal data obtained as a result of camera monitoring activity.

In order to ensure security by the Data Controller and for the purposes specified in this policy, internet access can be provided to the visitors who request during their stay in the buildings and facilities. In this case, log records related to internet access are recorded in accordance with the "Law No. 5651 on the Regulation of Broadcasts on the Internet and the Fight Against Crimes Through These Broadcasts" and the relevant provisions of the legislation; these records are only processed for the purpose of fulfilling the relevant legal obligations in the audit processes to be executed within the Data Controller or requested by the competent public institutions and organizations.

Only a limited number of Information Security Unit personnel have access to the records which are maintained in a digital environment.

The log records obtained are recorded with the timestamp to ensure the principle of invariance and are kept with the access of a limited number of Information Security Unit employees.

7. Processing of Customer and Business Partners Data

Personal data may be processed to communicate with the customers in writing and verbally for the purposes stated above.

Due to the relationship arising from the contract, personal data of current and potential customers and business partners (in case the business partner is a legal person, the business partner's officer) can be processed for the establishment, implementation, and termination of a contract without approval. Personal data prior to the contract, during the contract-starting phase; to prepare an offer, prepare a purchase form, or meet the data subject's demands for the implementation of the contract.

For advertising purposes, personal data is processed for advertising or market and public opinion research only if the purpose of collecting this information is suitable for those purposes. Data subject is informed that the information will be used for advertising purposes.

Personal data can be processed without explicit consent in order to clearly state the data processing in the relevant legislation or to fulfil a legal obligation determined by the legislation, if it is clearly required by our legal obligations or Law. The type and scope of data transactions must be required for legally permitted data processing activity and must comply with applicable legal provisions.

Special categories of personal data is processed provided that adequate measures are taken to be determined by the Authority and within the framework of the provisions of the Law.

Data subject's special categories of data, other than his health and sexual life, are processed with his explicit consent. If the person does not have explicit consent, it is processed within the exceptions stipulated in the Law.

8. Processing of Employee and Candidates' Data

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

The rules and procedures that regulate the terms and methods of personal data protection and processing of individuals working within the Data Controller are included in the "Protection and Processing of Employee Personal Data Policy".

However, it is mandatory to collect and process the personal data of the employees until the establishment, implementation, and termination of the employment contract. The explicit consent of the employees may not be obtained for these. Personal data of potential employee candidates are also processed in job applications. In case of rejection of the candidate's job application, the personal data obtained at the time of application are kept for as long as the retention period, at the end of this period, they are erased, destructed or anonymized.

Personal data of the employee may be processed without further approval for the purpose of clearly specifying the processing in the relevant legislation or fulfilling a legal obligation determined by the legislation.

Personal data of the employees can be processed without further approval in cases where there is a legitimate interest of the data controller. If the data of the employees are processed based on the legitimate interest of the data controller, it is examined whether this processing is moderate or not and it is checked that the legitimate interest does not violate a right of the employee to be protected.

Special categories of personal data is only processed under certain conditions. Data related to race and ethnicity, political opinion, religion, philosophical belief, sect or other beliefs, disguise and clothing, membership to associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data are defined as special categories of personal data. Special categories of personal data may only be processed with the explicit consent of the employee and by taking the necessary administrative and technical measures.

The situations listed below are exceptions to this provision, and even if the employee does not have explicit consent, the personal data may be processed. Special categories of personal data other than the health and sexual life of the employee can only be processed by the authorized institutions and organizations and the persons under the obligation of keeping secret for the purpose of protecting public health, executing protective medicine, medical diagnosis, treatment and care services, planning and managing the financing and health services when stipulated by law.

XVII. Terms of Processing Personal Data

1. Identification and Processing of Personal Data

According to the law, personal data is defined as "any information related to an identified or identifiable natural person". The concept of personal data is not only information that enables the recognition and identification of persons such as name, surname, place of birth, date of birth, but also covers all physical, social, cultural, economic and psychological information of the persons.

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

In addition to the identity information of the person, all information that ensures that the person is specific or identifiable such as citizenship number, tax number, passport number, social security number, driver's license number, motor vehicle license plate, home address, business address, e-mail address, telephone number, fax number, CV, photo, video, genetic information, blood type, criminal history, and criminal record information are personal data and are covered by the protection of personal data.

In accordance with this definition, the Data Controller determines whether all data collected by the Data Controller, including its business partners, employees and customers, are included in the scope of personal data and processes the same in accordance with the rules defined in the Law.

Processing of personal data; if obtained by fully or partially automated means or by being part of any data recording system and by non-automated means, covers all kinds of operations performed on data such as saving, storing, preserving, modifying, rearranging, disclosing, transferring, making available, classifying or preventing its use.

2. Exceptions

The Data Controller processes personal data with the explicit consent of the data subjects in accordance with the Law. However, it is possible to process personal data without seeking explicit consent if any of the following conditions exist.

- 2.1. Clearly prescribed by law (tax legislation, labour legislation, trade legislation, etc.).
- 2.2. Where it is necessary to process personal data of contract parties,
Processing of personal data pertaining to the parties of the contract is required, provided that it is directly related to the establishment or performance of a contract (Labor contract, sales contract, transportation contract etc.).
- 2.3. It is mandatory to protect the life or body integrity of the persons or another person for whom legal validity has not been recognized for its consent and being in a position of not capable of explaining its consent due to the actual impossibility.
- 2.4. In cases where data controller is required to fulfill its legal obligation (financial audits, security legislation, compliance with sector-oriented regulations, etc.)
- 2.5. Making the personal data public by the data subject (providing the information of the persons concerned to the public).
- 2.6. Data processing is mandatory for the establishment, use or protection of a right (mandatory data to be used in works such as litigation, registration procedures, all kinds of land registry transactions, etc.)
- 2.7. It is mandatory to process data for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject.

3. Processing Special Categories of Personal Data

Some personal data within the scope of the law are called "Special Categories of Personal Data". The Data Controller cannot process such data without the explicit consent of data subject. Explicit Consent is " a consent on a particular subject, based on the information and expressed in free will".

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

The Law has considered biometric and genetic data of a person concerning his/her race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, appearance and clothing, membership to an association, foundation or trade union, health, sexual life, criminal conviction and security measures as special categories of personal data. These data are limited in number as defined in the Law and cannot be increased through interpretation.

The Data Controller shall also take adequate measures determined by Personal Data Protection Board (Board) in the processing of sensitive personal data.

Data Controller, in accordance with the Law, can only process special categories of personal data as follows.

- 3.1. With the explicit consent of the data subject.
- 3.2. With the provision of the Law (personal data other than health and sexual life can be processed without seeking the explicit consent of the data subject in cases stipulated by the laws).
- 3.3. Planning, management and financing of health services for public health reasons (Public health protection, preventive medicine, medical diagnosis, treatment and care services, and planning, management and financing of health services, by persons under the obligation to keep secrets or processed by authorized institutions and organizations).

4. Transfer of Personal Data

The Data Controller, by taking necessary security precautions for the purposes of personal data processing in accordance with the articles 5/2 and 6/3 of the Law, can transfer personal data to third parties as long as it meets the requirements (legal reasons) specified in the Law. At the same time, the Data Controller may transfer personal data to third parties without explicit consent in accordance with the data processing requirements outlined in the Law.

The Data Controller takes the necessary administrative and technical measures to transfer the data he processes without explicit consent, in accordance with the restrictions in the Law.

The data controller may transfer the personal data to foreign countries declared to have sufficient protection by the Board. However, for countries where adequate protection is not available; data controllers in Türkiye and in the relevant foreign country must mutually commit in writing that there is adequate protection. The Board must grant transfer permission in the same way. Personal data can be transferred to foreign countries if these conditions are met.

XVIII. Data Controller Obligations

1. Obligation to Inform Personal Data Owner

During the acquisition of personal data, the Data Controller shall clarify the following matters to personal data owners.

- 1.1. Identification of data controller or its representative, if any
- 1.2. For what purpose the personal data will be processed

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

- 1.3. To whom and what purpose the personal data shall be transferred
- 1.4. Method and legal reasons for personal data collection
- 1.5. Rights of the personal data owner under to Article 11 of the Law

In accordance with this obligation, the Data Controller informs the persons concerned with the text for the obligation to inform. Obligation to inform is conducted as soon as the first contact is made with the concerned person.

If the personal data is not obtained from the concerned person, the obligation to inform must be made within a reasonable time. In case the personal data will be used for communication with the relevant person, or if the personal data will be transferred, the relevant people must be informed during the first communication.

2. Obligation to Conclude Applications of Personal Data Owners

Personal data owners may request information in writing in accordance with the Law by applying to the Data Controller or by other methods to be determined by the Board.

The Data Controller responds to applications in accordance with Article 13 of the Law in order to evaluate the rights of personal data owners and to inform them personally. The data controller creates and implements procedures for other administrative and technical regulations.

The rights of personal data owners are as follows;

- 1.1. Being aware of whether their personal data are processed
- 1.2. Request information about personal data if processed
- 1.3. Being aware of the purpose of the processing of personal data and whether they are used in accordance with their purpose
- 1.4. Being aware of the third parties to whom personal data are transferred in Türkiye or abroad
- 1.5. Requesting correction of personal data in case of incomplete or incorrect processing
- 1.6. Requesting the erasure or destruction of your personal data within the framework of the conditions stipulated in the relevant legislation
- 1.7. Requesting notification of the transactions made on the personal data made in accordance with the relevant legislation to third parties to whom their personal data are transferred.
- 1.8. Objecting to a result against the contact as a result of exclusive analysis of the processed data through automated systems
- 1.9. If the personal data is damaged due to the processing of their personal data in violation of the Law, requesting the removal of the damage.

The Data Controller processes requests submitted to registered e-mail addresses signed with a written or secure electronic signature, or requests submitted using the "Application Form" on the website. If the Board determines other application methods, the application shall be accepted with these methods.

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

The Data Controller responds to the request as soon as possible and within 30 (thirty) days at the latest, depending on the nature. The Data Controller may accept the applications and take the necessary actions or reject the applications with their reasons.

The personal data owner may file a complaint to the Board within 30 (thirty) days and in any case within 60 (sixty) days of the date of receipt of the answer in case the application is rejected, the answer given is insufficient or the answer is not answered.

The Data Controller shall respond to the personal data owners in time and in reasoned manner as required by the Law.

3. Obligation to Ensure Security of Personal Data

The Data Controller takes the necessary technical and administrative measures to ensure the appropriate level of security to prevent the illegal processing of the personal data they process and to prevent the illegal access to the data and to protect the data.

The Board will be able to make detailed arrangements about the obligations related to data security in the future. Therefore, the Data Controller shall exercise due diligence and ensure the security of personal data to comply with the obligations within this scope.

The Data Controller establishes the systems for conducting and having the necessary inspections related to the operation of the measures in terms of technical and administrative measures. These audit results are examined by the units in charge within the Data Controller and necessary measures are taken.

If the processed personal data is obtained by others in illegal ways, the Data Controller notifies violation to the Board within latest 72 hours (Seventy-Two) from the violation detection date. Following the determination of the persons affected by the data breach in question, the data subjects are also notified within the shortest possible time. If the contact address of the data subject can be reached directly, if it is not available, publishing the data controller through its website, etc. notification is made with appropriate methods.

4. Taking Technical and Administrative Measures for Providing Legal Data Processing

All processes related to the personal data processing activities performed by the business units within the Data Controller are collected and analysed in the personal data processing inventory. All activities conducted by the business units, from collection to deletion of data, are audited of compliance with the law.

Personal data processing activities are supervised by established technical systems. When a breach of law is detected, it is reported to the data subject and the deficiency or unlawfulness is eliminated.

The Data Controller informs and trains its employees on the Law and the processing of personal data in accordance with the Law.

Contracts and documents governing the legal relationship between the Data Controller and the Data Controller's business partners, employees and customers shall be accompanied by provisions imposing the obligation not to process, disclose or use personal data contrary to the regulations in the Law.

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

The procedures for ensuring the compliance of the activities of each business unit with the personal data processing requirements specified in the Law are determined for each business unit and the activity it executes. Implementation rules specific to business units are determined, necessary administrative measures are taken to ensure the supervision of these rules and continuity of implementation and training are provided by establishing a procedure.

5. Taking Technical and Administrative Measures to Prevent Illegal Access to Personal Data

The Data Controller shall take the necessary administrative and technical measures to prevent illegal obtaining, disclosure, display, and transfer of personal data to third parties according to the nature of the data to be protected.

Technical measures are taken in accordance with technological developments and the measures taken are updated and renewed when necessary.

Access and authorization technical processes are designed and commissioned by the Data Controller in accordance with legal compliance requirements.

Technological solutions are produced for issues with security risk.

Data Controller employees are trained in the technical measures taken and technically competent employee is employed.

The Data Controller has their employees sign the "General Standards and Security Policy of Information Systems" that their employees will not disclose the personal data they obtained if they are contrary to the provisions of the Law and will not use them for the purpose of processing.

The articles to protect the personal data are added to the contracts concluded by the Data Controller with the persons to whom the personal data are transferred.

The measures to be taken by the Data Controller are not limited to this article, however, the measures specified by the "Information Systems General Standards and Security Policy" and the "Personal Data Retention and Destruction Policy" created by the Data Controller are also implemented.

6. Obligation to Register to Data Controllers' Registry

The Data Controller shall submit its information and documents within the period determined and announced by the Board before commencing the data processing and shall be registered in the data controller's registry. The information to be declared to VERBIS are as follows;

- 6.1. Identity and address of the Data Controller representative
- 6.2. Reason for the processing of personal data
- 6.3. Explanations about the data subject group and groups of persons and the data categories of these persons
- 6.4. Recipient or recipient groups to which personal data can be transferred
- 6.5. Personal data expected to be transferred to foreign countries
- 6.6. Measures taken regarding personal data security

ARKAS HOLDING A.S
PERSONAL DATA PROTECTION AND PROCESSING POLICY
6.11.2019 / Version No: 1

6.7.The maximum time required for the purpose for which personal data are processed

7. Erasure, Destruction, and Anonymization of Personal Data

In the event that the reasons requiring processing are eliminated despite being processed in accordance with the relevant legal provisions as regulated in Article 138 of the Turkish Criminal Code and Article 7 of the Law, the Data Controller erases, disposes of or anonymizes the personal data upon its own decision or upon the request of the personal data owner.

The Data Controller shall take the technical and administrative measures detailed in the “Policy on Personal Data Storage and Destruction”; develops the necessary functioning mechanisms; trains, assigns and raises awareness of relevant business units to comply with their obligations contained herein.