

**ANTALYUM PREMIUM MALL MAN. CON. TRADE. LTD. CO.  
PERSONAL DATA PROCESSING, STORAGE AND DISPOSAL POLICY**

**SECTION ONE - INTRODUCTION**

- 1.1. INTRODUCTION 2
- 1.2. PURPOSE 2
- 1.3. SCOPE
- 1.4. IMPLEMENTATION OF POLICY AND RELATED LEGISLATION
- 1.5. EFFECTIVENESS OF POLICY
- 1.6. DEFINITIONS

**SECTION TWO - GENERAL ISSUES REGARDING THE PROCESSING OF  
PERSONAL DATA**

**2.1. PROCESSING PERSONAL DATA IN ACCORDANCE GENERAL PRINCIPLES**

- a. Processing In Compliance With Law and Principles
- b. Keeping Personal Data Accurate and Up to Date When Needed
- c. Processing Personal Data for Specific, Clear and Legitimate Purposes
- d. Keeping Personal Data Connected, Limited and Measured With Purpose
- e. Storage of Personal Data for the Time Required by the Relevant Legislation or for the Purpose It Was Processed

**2.2. PROCESSING PERSONAL DATA ACCORDING TO PROCESSING  
CONDITIONS**

- a. Obtaining Clear Consent
- b. Exceptions to the lack of explicit consent in the processing of personal data

**2.3. PROCESSING SPECIAL PERSONAL DATA ACCORDING TO PROCESSING  
CONDITIONS**

**2.4. PROCESSING PERSONAL DATA ACCORDING TO TRANSPORTATION  
CONDITIONS**

- a. Domestic Data Transfer
- b. Transferring Personal Data Abroad
- c. Recipient Groups to which Personal Data is Transferred

**SECTION THREE - PERSONAL DATA CATEGORIES PROCESSED BY  
ANTALYUM SHOPPING CENTER, PURPOSE OF PROCESSING AND  
TRANSMISSION, TRANSFER RECEIVER GROUPS**

- 3.1. PERSONAL DATA CATEGORIES
- 3.2. PERSONAL DATA OWNER CATEGORIES
- 3.3. CLASSIFICATION OF PERSONAL DATA PROCESSED BY ANTALYUM SHOP  
BY DATA OWNERS

- 3.4. PURPOSE OF PERSONAL DATA PROCESSING
- 3.5. COLLECTION METHODS AND REASONS OF PERSONAL DATA
- 3.6. RECEIVER GROUPS OF PERSONAL DATA TRANSFER

## **SECTION FOUR - MATTERS ON PROTECTION OF PERSONAL DATA**

### **4.1. SECURITY OF PERSONAL DATA**

- a. Technical measures taken to prevent unlawful processing of personal data, to prevent unlawful access to data and to protect data
- b. Administrative measures taken to prevent unlawful processing of personal data, to prevent unlawful access to data and to protect data
- c. Supervision of Measures for Protection of Personal Data
- D. Measures to be taken in case of unlawful disclosure of personal data

### **4.2. PROTECTION OF SPECIAL PERSONAL DATA**

### **4.3. PROTECTION OF LEGAL RIGHTS OF PERSONAL DATA OWNERS**

## **SECTION FIVE - ISSUES RELATED TO THE STORAGE AND DISPOSAL OF PERSONAL DATA**

### **5.1. REGISTRATION ENVIRONMENTS WHERE PERSONAL DATA ARE STORED AND DISPOSED**

### **5.2. STORAGE AND TERMS OF PERSONAL DATA**

### **5.3. LEGAL, TECHNICAL AND ADMINISTRATIVE REASONS REQUIRING STORAGE OF PERSONAL DATA**

### **5.4. LEGAL, TECHNICAL AND ADMINISTRATIVE REASONS REQUIRING DISPOSAL OF PERSONAL DATA**

### **5.5. SAFE STORAGE OF PERSONAL DATA**

### **5.6. DISPOSAL OF PERSONAL DATA ACCORDING TO LAW**

### **5.7. GENERAL ISSUES REGARDING THE DISPOSAL OF PERSONAL DATA**

### **5.8. DISPOSAL METHODS OF PERSONAL DATA**

- a. Deleting Personal Data
- b. Destruction of Personal Data
- c. Making Personal Data Anonymous

### **5.9. PERIODIC DISPOSAL TIME OF PERSONAL DATA**

### **5.10. RESPONSIBLE UNIT FOR STORAGE AND DISPOSAL PROCESSES OF PERSONAL DATA**

## **SECTION SIX - RIGHTS OF PERSONAL DATA OWNERS, ISSUES ABOUT THE USE OF THESE RIGHTS**

### **6.1. RIGHTS OF PERSONAL DATA OWNER ACCORDING TO KVKK**

### **6.2. CONDITIONS THAT THE PERSONAL DATA OWNER CANNOT USE THE RIGHTS**

### **6.3. PERSONAL DATA OWNER'S USE OF RIGHTS**

### **6.4. ANTALIU SHOPPING CENTER RESPONSE TO APPLICATIONS**

### **6.5. PERSONAL DATA OWNER'S RIGHT TO COMPLAIN TO KVK BOARD**

## **SECTION SEVEN - PROCESSING, STORAGE AND DISPOSAL OF PERSONAL DATA**

## 7.1. UNIT RESPONSIBLE FOR THE PROCESSING, STORAGE AND DISPOSAL OF PERSONAL DATA

### **SECTION EIGHT - UPDATE, COMPLIANCE AND CHANGES**

#### 8.1. UPDATE AND COMPLIANCE

#### 8.2. CHANGES

ANNEX.1 - STORAGE AND DISPOSAL TIME TABLE OF PERSONAL DATA

ANNEX.2 - PERSONAL DATA PROTECTION COMMITTEE UNIT, TITLE AND DUTY LIST

### **CHAPTER ONE - INTRODUCTION**

#### 1.1. Introduction

ANTALYUM ALIŞVERİŞ MERKEZİ YÖN.İNŞ.TİC.LTD.ŞTİ.

(“Antalyum AVM”) We are sensitive to the security of your personal data.

In this context, it is our priority to process and store any personal data belonging to all persons associated with our Company including our customers and business contacts who benefit from our products and services in accordance with the Personal Data Protection Law No. 6698 (KVKK ”).

With this İşleme Personal Data Processing, Retention and Disposal Policy temel, the basic principles and principles adopted in the protection, storage and destruction of personal data by Antalya AVM are regulated and implemented as Company policy and made sustainable.

#### 1.2. Purpose

The purpose of this Policy is to determine the procedures and principles regarding the processing, protection, storage, deletion, destruction, anonymization of personal data processed by Antalya AVM in accordance with the legal legislation which is the basis of this Policy, and the actual data processed by Antalya AVM. to inform people about this matter.

#### 1.3. Scope

This Policy; our customers, platform (Antalyum AVM and [www.antaliiumavm.com/](http://www.antaliiumavm.com/) [www.antaliiumshopping.com](http://www.antaliiumshopping.com/)) websites, users, employees, employee candidates, company shareholders, company officials, visitors, business contacts (supplier, service provider, subcontractor, and all other personal data of authorized, shareholder and employees of the institutions we have business relationships with), store authorized, shareholders and employees of our tenants, and third parties that are automated or processed in non-automatic ways provided that they are part of any data recording system. data groups may apply to this Policy as well as to certain provisions (eg, only visitors).

#### 1.4. Implementation of Policy and Related Legislation

This Policy has been prepared based on the Law No. 6698 on the Protection of Personal Data, the Regulation on the Registry of Data Responsible No. 30286, and the Regulation on Deletion, Destruction or Anonymous Making of Personal Data No. 30224.

The relevant regulations in force regarding the processing, protection and destruction of personal data will primarily apply. In case of any inconsistency between the legislation and

the Policy, Antalya Shopping Center accepts that the current legislation will find its application.

#### 1.5. Effectiveness of Policy

This Policy, which was organized by Antalya Shopping Center, was published on the website of Antalya Shopping Center and entered into force on 12/06/2019. It may be updated from time to time due to policy, legal changes, changes in the processing of personal data of Antalya AVM or other reasons.

In case of renewal of the entire Policy or certain articles, the effective date of the Policy shall be updated. The policy is published on the Company's website (<http://www.antaliiumavm.com> [www.antaliiumshopping.com](http://www.antaliiumshopping.com)) and is made available to interested persons at the request of personal data holders.

#### 1.6. Definitions

The definitions used in the implementation of this Policy are as follows:

Recipient Group	Category of real or legal person to whom personal data is transmitted by the data officer
Anonymization	Making personal data unmatched to any identifiable or identifiable natural person, even by pairing it with other data
Employee (s)	In accordance with the Labor Law, <b>Antaliium AVM Yön.İnş.Tic.Ltd.Şti.</b> graduates who work internship (compulsory / optional)
Related User	Except for the person or unit responsible for the technical storage, protection and backing up of the data, the persons who process personal data in accordance with the authorization and instructions received from Antalya AVM organization or from Antalya AVM.
Destruction	Irrevocable deletion, destruction or anonymization of personal data
Recording Media	Any media containing personal data that is fully or partially automated or processed by non-automated means provided that it is part of any data recording system

Personal Data	Any information relating to an identified or identifiable natural person
Personal Data Owner / Contact	Real person whose personal data is processed
Processing of Personal Data	Obtaining and storing personal data in whole or in part by automatic or non-automatic means provided that it is part of any data recording system, storage, preservation, modification, reorganization, disclosure, transfer, takeover, making available, classification or use of data
Personal Data Inventory	The data processing activities of the data responsible according to the business processes; purposes for processing personal data, data category, the maximum amount of time required for the purposes for which the personal data are processed by linking them with the group of recipients transferred and the group of data subject, personal data and data security measures foreseen to be transferred to foreign countries
Personal Data Protection Committee	The committee, which has the authority to make decisions and submit them to senior management in order to ensure compliance, preservation, maintenance, management and development of the personal data protection legislation by Antalya Shopping Center and for this purpose, is formed by the participation of officials from different departments.
Committee	Personal Data Protection Board
Institution	Personal Data Protection Authority

KVKK / Law	Law No. 6698 on Protection of Personal Data
Personal Data	Data on the race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, costume and clothing, association, foundation or union membership, health, sexual life, criminal conviction and security measures of individuals
Periodic Destruction	Deletion, destruction or anonymization of the personal data processing, storage and destruction policy, which will be carried out ex officio at repeated intervals in case all the conditions of the processing of the personal data in the law are eliminated
Policy	The principles adopted in the processing, storage and destruction of personal data by Antalya AVM are regulated in this “Antalya AVM Yön.İnş.Tic.Ltd.Şti. Personal Data Processing, Retention and Disposal Policy ”
Deletion	The process of making personal data inaccessible and reusable for the users concerned
Data Processing	Real and legal person who processes personal data on behalf of the person responsible for the data
Data Responsible	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 recording system
Data Recording System	Recording system in which personal data is structured and processed according to certain criteria
Registry of Data Officers	The registry of the data responsible held by the Personal Data Protection Agency and open to the public
Annihilation	The process of making personal data inaccessible, retrievable and reusable by anyone

For definitions not included in this Policy, KVKK definitions apply.

## **PART TWO - GENERAL ISSUES REGARDING THE PROCESSING OF PERSONAL DATA**

Antalyum Shopping Center carries out personal data processing activities

I. General principles

ii. Personal data processing requirements

iii. It complies with the requirements of special personal data processing.

### **2.1. Kişisel Verilerin Genel İlkelere Uygun Olarak İşlenmesi**

a. Law and Integrity Processing

Antalyum Shopping Center; acts in accordance with the principles of legal regulations and general trust and honesty in the processing of personal data. In this context, our Company conducts personal data processing activities in compliance with the law, honesty rules and transparency.

b. Keeping Personal Data Accurate and Up to Date

Antalyum Shopping Center; It makes every effort to ensure that the personal data it processes are kept accurate and up-to-date, taking into account the fundamental rights of the personal data owners and their legitimate interests. Accordingly, it takes necessary administrative and technical measures and provides opportunities for personal data owners to correct and verify their personal data.

c. Processing Personal Data for Specific, Clear and Legitimate Purposes

Antalyum Shopping Center determines the purpose of personal data processing clearly and precisely and carries out its data processing activities for open, legitimate and lawful purposes.

D. The personal data should be connected, limited and measured

Antalyum AVM processes personal data in connection with data processing purposes and to the extent required by these purposes. It avoids the processing of personal data that is not or is not needed for data processing purposes.

to. Retention for the time required by the relevant legislation or for the purpose for which it was processed

Antalyum AVM stores personal data only for the period required for the purpose specified or processed in the relevant legislation. In this context, firstly, it determines whether a period is stipulated in the related legislation for storing personal data, acts accordingly if a period is determined, and stores the personal data for as long as necessary for the purpose for which they are processed. In the event that the reasons that require expiration or elimination of the time expire, personal data is deleted, destroyed or anonymized by us. Detailed information on this is given in Chapter 5 of this Policy.

### **2.2. Processing of Personal Data in accordance with Processing Conditions**

Antalyum AVM conducts its personal data processing activities in accordance with the data processing conditions set forth in the personal data protection legislation. In this context; personal data processing is only possible if the following data processing conditions are in place:

#### a. Obtaining Clear Consent

Pursuant to the law, personal data cannot be processed without the express consent of the person concerned. In order to carry out personal data processing activities by Antalium Shopping Center, “freely, with sufficient knowledge of the subject, without any hesitation, and limited to the purpose of data processing.” explicit consent is required.

#### b. Exceptions to the lack of explicit consent in the processing of personal data

Antalium AVM is able to process personal data without explicit consent in the presence of one of the following conditions in the Law:

##### 1) Explicitly foreseen in law

The personal data of the data owner may be processed in accordance with the law, provided that it is expressly provided by law.

##### 2) Failure to Obtain the Consent of the Data Owner Due to Actual Impossibility and Obligation of Personal Data Processing

Personal data may be processed without explicit consent if it is compulsory for the protection of the life or physical integrity of the person who is unable to disclose his or her consent due to impossibility or whose legal consent is not granted. For example, in the event that an express consent cannot be obtained due to the lack of consciousness of the person, personal data of the personal data holder may be processed during medical intervention in order to protect life or body integrity.

##### 3) The Personal Data Processing Activity Is Directly Related to the Establishment or Performance of the Contract

Personal data may be processed if it is necessary to process the personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract.

##### 4) Obligation of Personal Data Processing Activity in order to fulfill the Legal Obligation of Antalyum Shopping Center

Antalyum AVM will be able to process the personal data of the person concerned, if necessary, in order to fulfill its legal obligation.

##### 5) Data Owner's Public Data Publication

Personal data publicized by the person concerned, in other words, disclosed to the public in any way, may be processed without express consent.

##### 6) Obligation of Data Processing for the Establishment, Use or Protection of a Right

Personal data may be processed without explicit consent if data processing is necessary for the establishment, use or protection of a right.

##### 7) Obligation of Personal Data Processing for Legitimate Interests of Antalyum Shopping Center

Personal data may be processed without obligation of express consent if data processing is obligatory for the legitimate interests of Antalyum Shopping Center without prejudice to the fundamental rights and freedoms of the data owner..

### **2.3. Processing of Personal Data in accordance with the Processing Conditions**

Special personal data can only be processed with the express consent of the data owner. However, personal data other than sexual life and personal health data may be processed without the express consent of the data owner in the cases provided for by law. Personal data on health and sexual life can only be processed without explicit consent to protect public health, preventive medicine, medical diagnosis, treatment and care, planning and managing health care and financing. Therefore, personal health data can only be processed by the



Company physician who is under explicit consent or under the obligation to keep secrets until the contrary is foreseen under KVKK.

Antalyum Shopping Center ensures that adequate measures are taken by the KVK Board regarding the processing and protection of private personal data. Antalyum Shopping Center shows the utmost sensitivity to the protection and security of private personal data, and the technical and administrative measures taken to protect private personal data are carefully implemented and necessary audits are carried out at Antalyum Shopping Center. The measures taken to protect private personal data are described in detail in Article 4.2 of this Policy.

#### **2.4. Processing of Personal Data in accordance with Transfer Conditions**

Antalyum AVM is able to transfer the personal and private personal data of the data owner to third parties for the purpose of personal data processing and taking the necessary security measures, if any, with express consent, otherwise limited with legal reasons. In this context, Antalyum Shopping Center acts in accordance with the personal data transfer conditions stipulated in Articles 8 and 9 of the Law.

##### **a. Domestic Data Transfer**

In accordance with Article 8 of the Law, Antalyum Shopping Center carries out domestic data transfer activities in accordance with data processing conditions. (See Antalyum Shopping Mall Management Policy) Personal Data Processing, Retention and Disposal Policy - Part Two, Articles 2.1, 2.2 and 2.3.

##### **b. Transferring Personal Data Abroad**

In accordance with Article 9 of the Law, Antalyum AVM conducts the data transfer activities abroad in accordance with the data processing conditions (See Antalyum AVM Direct. Personal Data Processing, Retention and Disposal Policy - Section Two, Article 2.1, 2.2. and 2.3). Where personal data are transmitted without express consent in accordance with KVKK, one of the following conditions is also required for the foreign country to which it will be transferred:

ü The foreign country in which the personal data is transmitted is in the status of the countries where there is adequate protection by the Board,

ü In the absence of adequate protection to undertake an adequate protection of data in Turkey and in the relevant foreign country responsible for writing the CTL and permission from the Board

##### **c. Recipient Groups to which Personal Data is Transferred**

In accordance with the 8th and 9th articles of the Law, Antalyum Shopping Center provides the personal data of the data holders to business partners, suppliers, insurance companies, banks and financial institutions, law, tax and so on. Support to consulting and auditing firms, company officials, shareholders, legally authorized public institutions and private individuals in the fields of storage, archiving, information technologies (server, hosting, software, cloud computing) that process personal data on behalf of the Company. etc.) in order to continue their commercial activities and business processes. The classification of groups of recipients to whom personal data is transmitted is contained in Chapter 3 of this Policy.

In the event of personal data transfer, Antalyum AVM also ensures that third parties to whom it transfers personal data comply with this Policy. In this context, necessary protective arrangements are added to the contracts concluded with third parties and technical measures are taken.

### **CHAPTER THREE - PERSONAL DATA CATEGORIES PROCESSED BY ANTALIUUM SHOPPING, PURPOSE OF PROCESSING AND TRANSMISSION**

### 3.1. Personal

#### 3.1. Personal Data Categories

The personal data categories and descriptions processed within the scope of personal data processing activities carried out by Antaliu AVM are as follows: **Personal Data Categories**

##### Identity Data

Açıklama  
Information on the identity of the person: name-surname, T.C. identification number, marital status, gender, nationality, parent-name-surname, place of birth-date and other identification information and license information, identity card, passport, birth certificate and documents such as tax number, SSI number, vehicle license plate and other information.

##### Communication Data

Telephone number, address, e-mail address, fax number, such as information used for communication purposes and documents such as residence documents containing this information.

##### Personal Data of Family Members / Relatives

Personal data about the family members and relatives of the data owner in order to protect the legal and other interests of the Company / related person within the scope of our Company's activities. Example: Education of family members, income information, etc.

##### Financial Data

The data owner of the Company is the personal data regarding the information, documents and records showing all kinds of financial results that arise according to the legal relationship established with the person concerned. Example: Credit card information, income information, IBAN number, etc.

##### Physical Space Safety Data

Personal data relating to the records and documents received during entry and stay in the physical space. Example: Camera recordings, etc.

##### Personal Data

Within the scope of working relationship with our company, it is the personal data that is processed to obtain the information that is the basis of the personal rights of real persons.

Communication and Complaint Management Data	Personal data obtained in the process of receiving and evaluating any kind of request or complaint to our Company.
Private Qualified Personal Data	These are personal data which are determined by limited counting in the law and, if processed, at risk of discrimination against the data owners. Personally processed personal data processed by Antalyum AVM are data such as personal health data including blood type and CCTV records.
Transaction Data	These are data such as order and expenditure information, purchase information, opinion, request and instruction information related to the transactions performed by the data owner.
Marketing Data	The data we collect for marketing purposes is personal data including targeting information such as shopping preferences, occupation, educational status, number of children.
Device Information, Access and Location Data	These are the data that our company processes related to the device used by the data owner and the records of the access, sending and other activities made by the device and the information, data and records that determine the position of the person concerned. Example: GPS location data, etc.
Transaction Security Data	Personal data processed to ensure the technical, administrative, legal and commercial security of both the data owner and our Company.

### **3.2. Personal Data Owner Categories**

In the following, the platform (the websites of Antalyum AVM and Antalyum AVM brands) of our customers, employees, employee candidates, visitors, business contacts (suppliers, service providers, subcontractors, subcontractors, and similar business shareholders and employees), store tenants who are our tenants, shareholders and employees and third parties.

#### **Data Owner Categories**

#### **Explanation**

Customers	They are real persons who use or have used the products and services offered by our Company. (All people who visit Antalya Shopping Center and benefit from their services are in this category.)
Platform Users	They are the natural persons who have visited / used / used / used our electronic platforms ( <a href="http://www.antaliuvm.com">www.antaliuvm.com</a> ; <a href="http://www.antaliuvmshopping.com">www.antaliuvmshopping.com</a> , etc., our social media accounts, etc.) for any purpose.
Personnel	They are real persons in working relationship with our company.
Employee Candidates	They are natural persons who have applied to our company in any way and submitted their resume and / or information about the job application form to our company for review.
Company Shareholders	Antaliuvm AVM are the people who hold their capital shares.
Company Officials	They are the real persons and real person representatives of the legal persons who are in the senior management of Antalya Shopping Mall and / or are authorized to represent the Antalya Shopping Mall. The members of the board of directors are evaluated within this scope.
Business Connections (Shareholder, Authorized and Employees)	Real persons who are involved in all kinds of business relationships and all real persons working in real and legal persons (suppliers, service providers, subcontractors, etc.) in which our company has business relations. (Including company shareholders and officials)
Stores (Shareholder, Authorized and Employees)	They are all real people who work in the stores that have tenants in the shopping center. (Including store authorities, owners and shareholders)

Visitors	They are real persons who have been present for various purposes in corporate physical locations owned by our company.
Other third parties	They are other natural persons who do not fall into any data owner category.

### 3.3. Classification of Personal Data Processed by Antaliu Shopping Centers According to Data Owners

In the table below, the personal data owner categories mentioned above and the personal data categories within the processing activity

Personal Data Categories	Explanation
Identity Data	Customers, Platform Users, Employees, Employee Candidates, Company Authorities, Company Shareholders, Business Contacts (Shareholder, Authorized and Employees), Shops (Shareholder, Authorized and Employees), Visitors, Other third parties
Communication Data	Customers, Platform Users, Employees, Employee Candidates, Company Authorities, Company Shareholders, Business Contacts (Shareholder, Authorized and Employees), Shops (Shareholder, Authorized and Employees), Visitors, Other third parties
Personal Data of Family Members / Relatives	Employees, Employee Candidates, Company Officials, Company Shareholders, Business Relations (Shareholder, Authorized and Employee)
Financial Data	Customers, Employees, Employee Candidates, Company Officials, Company Shareholders, Business Contacts (Shareholder, Authorized and Employees), Stores (Shareholder, Authorized and Employees), Other third parties

Physical Space Safety Data	Customers, Employees, Employee Candidates, Company Officials, Company Shareholders, Business Contacts (Shareholder, Authorized and Employees), Shops (Shareholder, Authorized and Employees), Visitors, Other third parties
Personal Data	Employees, Employee Candidates, Company Officials, Company Shareholders, Business Contacts (Authorized and Employees)
Communication and Complaint Management Data	Customers, Platform Users, Business Contacts (Shareholder, Authorized and Employees), Shops (Shareholder, Authorized and Employees), Visitors, Other third parties
Personal Data	Customers, Employees, Employee Candidates, Company Officials, Company Shareholders, Business Contacts (Shareholder, Authorized and Employees), Shops (Shareholder, Authorized and Employees), Visitors, Other third parties
Transaction Data	Customers, Platform Users
Marketing Data	Customers, Platform Users
Device Information, Access Records and Location Data	Customers, Platform Users, Employees, Company Authorities
Transaction Security Data	Customers, Platform Users, Employees, Employee Candidates, Company Authorities, Company Shareholders, Business Contacts (Shareholder, Authorized and Employees), Shops (Shareholder, Authorized and Employees), Visitors, Other third parties

### **3.4. Purposes of processing personal data**

Antalyum AVM conducts its personal data processing activities in line with the following objectives. Personal data processing objectives, business processes and personal data categories are identified in relation to each business unit and process in a clear and detailed basis and recorded in the Personal Data Inventory of Antalya Shopping Center.

ü To make the necessary planning, evaluation and studies to benefit our customers from our products and services offered by Antalya Shopping Mall by the business units of Antalya Shopping Mall;

- ü To conduct advertising and marketing activities for products and services offered by Antalyum Shopping Center, to provide information on promotions, campaigns, offers, events and similar issues, to carry out corporate communication activities, and to offer products and services according to the tastes, usage habits and needs of the relevant persons;
  - ü Carrying out marketing and customer relationship management activities;
  - ü Organization of corporate communication and other activities, campaigns and invitations within this scope and informing them, conducting market research studies;
  - ü Number of users, type, frequency of visits, behaviors, geographical locations and similar statistics are prepared to improve the digital platforms offered to the customers of Antalyum AVM and to provide efficient and personalized experience to the platform users, to provide personalized content, campaigns and advertisements according to the interests and needs of the platform users. use of cookies for this purpose;
- 
- ü Follow-up, evaluation of customer requests, suggestions and complaints, customer satisfaction management and implementation of planning, statistics and satisfaction evaluation studies within this scope;
  - ü Business contacts, management of relations with shops, suppliers, subcontractors and similar business relationships, conducting business and commercial relations;
  - ü Ensuring the legal and commercial security of persons in business relationship with Antalyum AVM and Antalyum AVM (planning administrative operations for the services provided by Antalyum AVM, evaluating and auditing business partner / customer / supplier (authorized or employees), legal compliance process. );
  - ü Ensuring the physical security and control of the locations operated by Antalyum Shopping Center;
  - ü Planning and execution of occupational health and safety processes;
  - ü Use of legal rights, use of information about transaction history after the termination of legal relationship as evidence in case of dispute;
  - ü Determining and implementing commercial, legal and business strategies of Antalyum AVM;
  - ü Implementation of the financial policies of Antalyum Shopping Center;
  - ü Carrying out the human resources policies and recruitment processes of Antalyum Shopping Center, regulating employee control and supervision and employee rights, and fulfilling the legal obligations arising from the business relationship;
  - ü Planning, auditing and conducting information security processes, management of information technology infrastructure;
  - ü Conducting planning, reporting, visitor / customer statistics and similar investigations within the scope of Antalyum Shopping Mall activities;
  - ü Compliance with the relevant domestic legislation, provision of information requested by public institutions and organizations, fulfillment of reporting obligations.

### **3.5. Methods and Reasons for Collecting Personal Data**

Antalyum AVM, personal data of the data owners,

- ü Our websites and platforms belonging to Antalyum AVM and Antalyum AVM brands ([www.antaliuvm.com](http://www.antaliuvm.com) /[www.antaliuvmshopping.com](http://www.antaliuvmshopping.com)) are used in the context of Antalyum AVM sales and marketing activities through social media accounts operated on behalf of Antalyum AVM and its brands in various social media channels. e-mail, text messages (“SMS”), or multimedia messages (“MMS”),
- ü Through other communication methods including printed and electronic forms,
- ü By means of closed circuit camera systems located in Antalyum Shopping Mall locations,

- ü Contracts, commercial offers, printed and electronic forms, documents, correspondence signed within the scope of Antalya Shopping Mall business activities,
- ü Through the business cards and other documents obtained within the scope of the job interviews,
- ü Through third parties, such as group companies, business contacts or companies providing services / products of Antalya AVM; it collects by means of a variety of methods, whether fully or partially automated or not as part of any data recording system, whether verbal, written or electronic.

The personal data collected in accordance with these methods are kept in accordance with the data processing requirements of Part 2 of this Policy and for the purposes of personal data processing listed above, in compliance with the periods stipulated in KVKK and other legislation and taking all necessary administrative and technical measures. .

### **3.6. Recipient Groups to which Personal Data is Transferred**

In accordance with KVKK, Antalya AVM is able to transfer the personal data contained in this Policy to the recipient groups listed below for the purposes specified. Receptor groups to which personal data are transferred and the purposes of the transfer are determined clearly and in detail on the basis of each business unit and process by associating business processes and personal data categories and entered into the Personal Data Inventory of Antalya Shopping Mall.

<b>Recipient Groups</b>	<b>Personal Data Transfer Objectives</b>
Work partners	To ensure the fulfillment of the objectives of the partnership
Service Providers	In order to ensure the provision of services provided by our Company from external sources and necessary for carrying out the commercial activities of our Company.
Shareholders / Authorities	Pursuant to the provisions of the relevant legislation, our Company is limited to designing and auditing the commercial activities of our Company.
Legally Authorized Public Institutions and Organizations	Within the legal authority of the related public institutions and organizations
Legally Authorized Private Law Persons	Limited to the purpose requested by the relevant private law persons within the legal authority

The personal data transfers carried out by Antalya Shopping Center are in accordance with the issues set out in Part 2 of the Policy.



## **SECTION FOUR - ISSUES RELATED TO THE PROTECTION OF PERSONAL DATA**

In accordance with Article 12 of the KVKK, Antalyum AVM shall take the necessary technical and administrative measures to ensure the appropriate level of security according to the nature of the data to be protected and to prevent the unlawful processing of the personal data it is processing, to prevent unlawful access to the data and to ensure the preservation of the data. necessary audits in this context.

### **4.1. Securing Personal Data**

a. Technical measures taken to prevent unlawful processing of personal data, to prevent unlawful access to data and to protect data

The main technical measures taken to prevent unlawful processing of personal data, to prevent unlawful access to data and to protect data are listed below:

ü As regards the protection of personal data, technical measures are taken and the measures taken are updated periodically by Antalyum AVM, and regular inspections are carried out for the implementation of the measures taken.

ü Software and systems to ensure data security are established and used, servers that contain data are protected with up-to-date virus protection software to prevent unauthorized access to personal data both internally and externally and / or intrusion, session management software, password management software and firewalls.

ü Antalyum AVM works with a service provider that specializes in technical issues.

ü Access to personal data is limited for the purpose of data processing and the authority is regularly reviewed. Authorization is made on the basis of the principle that should be known.

ü Technical security systems are established for storage areas, security tests and investigations are carried out for the detection of security weaknesses on information systems, and existing or potential risks identified as a result of the tests and researches are eliminated.

ü Systems and backup software in accordance with technological developments are used to ensure that personal data is stored in a lawful and safe manner.

b. Administrative measures taken to prevent unlawful processing of personal data, to prevent unlawful access to data and to protect data

The main administrative measures to prevent unlawful processing of personal data, to prevent unlawful access to data and to protect data are listed below:

ü Antal Personal Data Protection Committee "was established and started to operate in Antalyum AVM for the purpose of ensuring compliance with the Law and its sustainability.

ü Antalyum AVM employees are regularly informed and trained on the protection and processing of personal data.

ü All activities carried out by Antalyum AVM have been analyzed in detail in all business units, and as a result of this analysis, personal data processing activities have been determined and recorded in personal data inventory. Inventory is updated regularly by Antalyum AVM.

ü The requirements to be fulfilled in order to ensure compliance with the personal data processing conditions in the personal data processing activities carried out by Antalyum Shopping Mall business units are determined in each business unit and detail activity.

ü In order to meet the compliance requirements, awareness is created and implementation rules are determined for the relevant business units; In order to ensure the continuity of these issues and practices, internal policies are implemented and audits are conducted.

ü Provisions have been added to the agreements and documents signed with employees and third parties for the purpose of processing, protecting and securing data confidentiality of personal data, and the provisions of the parties have been explicitly regulated and the provisions that impose sanctions for unlawful data processing activities have been applied.

#### c. Supervision of Measures for Protection of Personal Data

In accordance with KVKK, Antalya AVM carries out the necessary audits or has it done. The results of these audits are reported to the Personal Data Protection Committee, the senior management and the related department within the scope of the internal operation of the Company, actions are planned and the follow-up of the actions planned to improve the measures taken are followed up by the relevant process owners and the Personal Data Protection Committee.

#### D. Measures to be taken in case of unlawful disclosure of personal data

In the event that personal data is obtained or disclosed by others in an unlawful way, Antalya AVM will inform the relevant personal data holder and KVK Board as soon as possible.

### **4.2. Protection of Personal Data**

The law attaches particular importance to certain personal data, because of the risk of victimization and / or discrimination of persons when processed unlawfully. This data; race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, disguise and dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures and biometric and genetic data. With the law, special quality özel determined and processed in accordance with the law of the protection of personal data of the highest sensitivity is shown by Antalya Shopping Center.

Antalya AVM, within the scope of private personal data category; It processes and stores the CCTV records of the relevant data holders for health and safety data, criminal convictions and security data. It treats the security of these data with the utmost care and ensures the necessary audits within the Company.

In addition to the technical and administrative measures set out in Article 4.1 of this Policy, measures are taken for the processing of private personal data. These additional measures are listed below:

ü Access to special personal data is restricted for the purpose of data processing and is given to only a limited number of people on the basis of "What you need to know". For example, personal health data can only be processed by the Company physician, who is obliged to keep a secret. Authorization checks are performed periodically for authorized persons who provide access to personal data.

ü Additional security measures are taken according to the method of processing related to the processing and transfer of special personal data. (For example, sending encrypted e-mail, encryption by cryptographic methods, sharing in confidential document format, etc.). Private personal data transmitted electronically are transmitted only by encryption (such as PGP encryption).

ü Personal data stored in physical environment is stored in environments where adequate security measures are taken (locked cabinets with key only, etc.) and unauthorized access is prevented.

### **4.3. Protection of Legal Rights of Personal Data Holders**

Antalya Shopping Center observes all the legal rights of the personal data owners with the implementation of the Policy and Law and takes all necessary measures to protect these rights. Detailed information on the rights of personal data holders is provided in section 6 of this Policy.

## **SECTION FIVE - ISSUES RELATED TO THE STORAGE AND DISPOSAL OF PERSONAL DATA**

### **5.1. Recording Media where Personal Data is Stored and Destroyed**

Personal data processed and stored by Antalyum AVM can be recorded in different environments depending on the principles such as data quality, processing purposes and frequency of use. In this context, personal data of the data owners are kept in a safe manner by Antalyum AVM in the environments listed below, in accordance with the relevant legislation, in particular the provisions of the KVKK.

#### **Electronic environments:**

- ü Databases: Databases hosting personal data recorded and / or processed through enterprise applications
- ü File System: Spreadsheet, word processor, text or PDF files and similar files hosted in public areas or computers allocated to employees other than corporate applications
- ü Electronic Devices: Network Devices, Portable Media Devices (flash memory, hard disk, tape cartridges, etc.), Printers, Mobile Phones
- ü Peripheral Systems: CCTV Camera Systems, Card Reader Systems

#### **Physical environments:**

- ü Unit Cabinets
- ü Physical Archive (belonging to Antalyum Shopping Center)  
data can only be processed by the Company physician under the obligation of keeping secrets. Authorization checks are performed periodically for authorized persons who provide access to personal data.
- ü Additional security measures are taken according to the method of processing related to the processing and transfer of special personal data. (For example, sending encrypted e-mail, encryption by cryptographic methods, sharing in confidential document format, etc.). Private personal data transmitted electronically are transmitted only by encryption (such as PGP encryption).
- ü Personal data stored in physical environment is stored in environments where adequate security measures are taken (locked cabinets with key only, etc.) and unauthorized access is prevented.

### **4.3. Protection of Legal Rights of Personal Data Holders**

Antalyum Shopping Center observes all the legal rights of the personal data owners with the implementation of the Policy and Law and takes all necessary measures to protect these rights. Detailed information on the rights of personal data holders is provided in section 6 of this Policy.

## **SECTION FIVE - ISSUES RELATED TO THE STORAGE AND DISPOSAL OF PERSONAL DATA**

### **5.1. Recording Media where Personal Data is Stored and Destroyed**

Personal data processed and stored by Antalyum AVM can be recorded in different environments depending on the principles such as data quality, processing purposes and frequency of use. In this context, personal data of the data owners are kept in a safe manner by Antalyum AVM in the environments listed below, in accordance with the relevant legislation, in particular the provisions of the KVKK.

#### **Electronic environments:**

- ü Databases: Databases hosting personal data recorded and / or processed through enterprise applications
- ü File System: Spreadsheet, word processor, text or PDF files and similar files hosted in public areas or computers allocated to employees other than corporate applications
- ü Electronic Devices: Network Devices, Portable Media Devices (flash memory, hard disk, tape cartridges, etc.), Printers, Mobile Phones

ü Peripheral Systems: CCTV Camera Systems, Card Reader Systems

Physical environments:

ü Unit Cabinets

ü Physical Archive

## **5.2. Retention and Duration of Personal Data**

Antalyum AVM maintains personal data for the period required for the purpose specified or processed in the relevant legislation. Within this framework, Antalyum Shopping Center acts in compliance with this period if it is stated in the relevant legislation how long it is necessary to store personal data, if not, it stores the data for the period required to be processed depending on the services it provides. Personal data is deleted, destroyed or anonymized by Antalyum AVM in the event that the expiry of the period, the request of the data owner or the purpose that requires the processing of the data is eliminated. Detailed information on the storage periods of personal data processed by Antalyum AVM is provided in Appendix 1 of this Policy.

## **5.3. Legal, Technical and Administrative Reasons for Storing Personal Data**

In the event that the purpose of processing the personal data is terminated, the request of the data owner and / or the storage period determined by the relevant legislation and the company is reached, the personal data,

ü In case of possible legal disputes, it is not possible to provide evidence or to assert the right to a personal data or to establish a defense. In order to fulfill the legal responsibilities may be stored in accordance with the measurements and / or periods specified in the laws. The storage periods are determined on the basis of the time-out periods in order to assert the mentioned right in the facility. In this case, the stored personal data is not accessed for any other purpose and is only provided when it is required to be used in the relevant legal dispute.

ü Data to be destroyed by deletion, destruction or anonymization can be stored until the next periodic destruction date at the latest.

After the above-mentioned periods expire, personal data is deleted, destroyed or made anonymous.

## **5.4. Legal, technical and administrative reasons for the destruction of personal data**

### **Personal data stored by Antalyum AVM**

ü Eliminating all the purposes that require the processing of personal data and the reasons that require the storage of personal data,

ü In case the processing of personal data is only subject to the express consent, the data owner shall revoke its consent,

ü If the data owner requests the destruction of his personal data by using the rights specified in Section 6 of this Policy, which is within the scope of KVKK, and if the application is accepted by Antalyum AVM or the request is approved by the Board upon the rejection of this request,

ü Although the maximum amount of time required to keep personal data has passed there is no requirement to justify storing personal data for longer periods of time cases.

## **5.5. Secure Storage of Personal Data**

Antalyum AVM takes the necessary technical and administrative measures to prevent the loss, loss or alteration of the personal data it processes in safe environments and for illegal

purposes. Detailed information on personal data security is provided in Chapter 4 of this Policy under the heading “Protection of Personal Data”.

The main technical measures taken by Antalyum Shopping Center regarding the storage of personal data are listed below:

- ü Software and systems that provide data security are established and used for storing personal data in secure environments.
- ü Technical security systems for storage areas are established. Security scans and investigations are carried out in order to find security weaknesses on information systems, and studies are carried out to the extent permitted by the technology to eliminate the existing or potential risks determined as a result of the scans and researches.
- ü To the extent possible, technology measures are taken by Antalyum AVM for the protection of personal data, and the measures are regularly updated and audits are carried out at regular intervals for the implementation of the measures taken.
- ü Antalyum AVM works with a service provider that specializes in technical issues.
- ü Systems and backup software in accordance with technological developments are used to ensure that personal data is stored in a lawful and safe manner.
- ü Access to personal data storage is restricted, and only authorized persons are allowed access to such data for the purpose of storing personal data.

Considering the storage of personal data; The main administrative measures taken by Antalyum AVM are listed below:

- ü Antalyum AVM employees are regularly informed and trained on the protection, storage and processing of personal data.
- ü Provisions were added to the agreements and documents signed with third parties for the purpose of processing, storing and securing personal data in accordance with the law, and the obligations of the parties to take the necessary security measures were clearly regulated and sanctions were imposed for data processing activities contrary to the law and the contract.

## **5.6. Legal Disposal of Personal Data**

The main technical measures taken by Antalyum AVM for the destruction of personal data are listed below:

- ü Personal data destruction is carried out under the supervision of technical experts.
- ü The method of destroying the data to be destroyed at the end of the storage period or for any other valid reason may vary depending on the storage environment. For example, internationally accepted standards (DoD 5220.22-M, NIST 800-88, HMG IS5-E, VSITR, etc.) are used for the destruction of the backups whose storage period has been completed.
- ü Regarding the destruction process, records are kept on the date of destruction, who has done and approved the destruction and which personal data category information has been destroyed.

The main administrative measures taken by Antalyum AVM for the destruction of personal data are listed below:

- ü Personal data destruction is carried out under the supervision of a technical expert as well as a person authorized by the personal data protection committee.
- ü The personal data protection committee is tasked with evaluating and monitoring the personal data inventory on the basis of storage and destruction periods and coordinating the business units.
- ü Antalyum Shopping Center informs its employees about periodic and proper destruction of personal data and provides training.
- ü Audits are conducted and reported.

ü Contracts and documents signed with third parties include provisions for the processing, storage and destruction of personal data in accordance with the law, expiration of the storage period or destruction upon the request of the data owner. sanctions have been applied for its activities.

### **5.7. General Considerations on the Disposal of Personal Data**

If processed in accordance with the provisions of the Law and other relevant laws, the personal data shall be destroyed by the deletion, destruction or anonymization by Antalya AVM upon the request of the owner or data holder in case the purpose which requires the processing and storage of personal data disappears.

Antalya Shopping Center acts in accordance with the technical and administrative measures mentioned above, the provisions of the relevant legislation, Board decisions and this Policy in the deletion, destruction or anonymization of personal data. All transactions carried out by Antalya AVM regarding the deletion, destruction and anonymization of personal data are recorded and the said records are kept for at least three years except for other legal obligations.

Unless otherwise decided by the KVK Board, Antalya AVM chooses the appropriate method of deleting, destroying or anonymizing the destruction of personal data. Upon the request of the person concerned, he chooses and applies the appropriate method by explaining the justification.

### **5.8. Disposal Methods of Personal Data**

#### **a. Deleting Personal Data**

Deletion of personal data is the process of making personal data inaccessible and inaccessible to the users concerned. In order to delete personal data, Antalya AVM may use the following methods depending on the environment where the data is recorded.

#### **Recording Media**

#### **Data Destruction Method**

Third-party software in the cloud infrastructure, different software for data processing purposes

Enabling delete, saving data for the cloud infrastructure with an encrypted key and destroying the key at the end of the destruction process.

Different software for data processing purposes

Deletion by means of software capable of destruction at international standards

Databases

Delete with database command

Databases, data in the file system of the servers

Remove the user's access rights on the directory where the file is located, command to delete it or delete it by means of software capable of destroying in international standards

Paper and printed copies

Dimming (is the process of cutting personal data on the relevant documents where possible and making them invisible to the relevant users by using fixed ink, which cannot be recovered and read by technological solutions.)

#### b. Destruction of Personal Data

Destruction of personal data is the process by which personal data cannot be accessed, retrieved or reused by anyone in any way. To delete personal data, Antalya AVM may use one or more of the following methods, depending on the environment in which the data is recorded:

##### **Recording Media**

##### **Data Destruction Method**

Media that records data magnetically (Tape cartridges, etc.)

De-magnetization (The process of magnetic media being exposed to a very high magnetic field by passing through a special device and the data on it is unreadable.)

Media that record data magnetically and optically (Tape cartridges, DVD, CD, hard disk, etc.), Paper and Printed Copies

Physical Destruction (Melting, incineration or powdering of optical media and magnetic media; physical destruction of paper and printed copies by means of a paper destruction / trimming machine or incineration method.)

Magnetic and rewritable optical media (DVD-r, etc.)

Overwriting (Preventing the recovery of old data by writing random data of 0 and 1 at least seven times on magnetic media and rewritable optical media.)

Media that records data magnetically (tape cartridges, hard disk, etc.)

Destruction with "Block Erase" Command

Third-party software in the cloud infrastructure

Destroy all copies of encryption keys

#### c. Making Personal Data Anonymous

The anonymization of personal data means that personal data cannot be associated with any identifiable or identifiable natural person, even if it is matched with other data. In order to make personal data anonymous; personal data may be identified or identified, even by use of appropriate techniques for the recording medium and the field of activity, such as the return of

data by the data officer, recipient, or groups of recipients and the mapping of data to other data.

it must be made unrelated to a real person. Antalya AVM may use one or more of the following methods to anonymize personal data, depending on the environment or processing method in which the data is stored:

ü Subtracting Variables: A method of anonymizing by deleting one or more of the variables from the table completely

ü Subtracting Records: Anonymity is achieved by deleting the row or row relationships that provide the singularity in the personal data set.

ü Generalization: It is the process of converting the related personal data from a special value to a more general value.

ü Regional Concealment: If the combination of the values of a particular record creates a very visible condition, and if this is likely to cause the individual to become distinguishable in the community concerned, changing the value that creates the exception to an unknown value or changing it to “unknown” creates a singularity. and, if not used for a statistical result, another method commonly used within the community to reduce the likelihood of predictability.

ü Lower And Upper Coding: Defining a category for a given variable in the personal data set and combining the remaining values within the grouping created by this category.

ü Global Coding: Anonymization method by creating a common and new group for selected values and replacing all records in the data set with this new definition.

ü Sampling: In the sampling method, a subset from the cluster is described or shared instead of the entire data set.

ü Micro-Consolidation: With this method, all records in the data set are subdivided into a certain number of subsets, averaging the value of the subset of the specified variable and replacing the value of that subset of the variable with the average value, but this process also makes an analysis for the data to be used for statistical purposes. It might require.

ü Data Exchange: The data exchange method is a method of changing the record obtained by exchanging the values of a variable subset between the pairs selected from the records.

ü Adding Noise: Adding and subtracting to provide the distortions of a selected variable in the data set.

ü Other anonymizing statistical methods (K-Anonymous, L-Diversity, T-Proximity, etc.)

### **5.9. Periodic Destruction of Personal Data**

Antalya AVM deletes, destroys or anonymises personal data in the first periodic destruction process following the date when the obligation to delete, destroy or anonymize personal data arises.

The periodic period of destruction of Antalya Shopping Center is 6 months, however, Antalya Shopping Center accepts that the KVK Board may shorten the periods specified in this article in the event of irreparable damages or inconvenient damages.

### **5:10. Responsible Unit for Storage and Disposal of Personal Data**

The “Personal Data Protection Committee” was established with the aim of carrying out the processes of storing and destroying personal data and taking the necessary actions in accordance with this Policy. Detailed information on this issue can be found in Chapter 7 of this Policy.



The persons involved in the Personal Data Protection Committee are responsible for the full fulfillment of all obligations regarding the storage and destruction of personal data set out in this Policy.

## **CHAPTER SIX - RIGHTS OF PERSONAL DATA OWNERS, ISSUES ABOUT THE USE OF THESE RIGHTS**

### **6.1. Rights of Personal Data Holder in accordance with KVKK**

Personal data holder, in accordance with Article 11 of the KVKK by applying to the Antalya Shopping Center;

- ü To learn whether personal data is processed or not,
- ü Requesting information if their personal data has been processed,
- ü To learn the purpose of the processing of personal data and whether they are used appropriately,
- ü Knowing the third parties to whom personal data is transferred at home or abroad,
- ü If personal data is missing or mis-processed - request that it be corrected and the transaction carried out within this scope is notified to the third parties to whom the personal data has been transferred,
- ü Requesting the deletion or destruction of personal data and the notification of the transaction to third parties in the event that the reasons that are required to be processed are removed, even if they have been processed in accordance with the provisions of the Law and other relevant legislation,
- ü To object to the occurrence of a result against the person by analyzing the processed data exclusively through automated systems,
- ü In case of damage due to unlawful processing of personal data, it has the right to demand the damages.

### **6.2. In cases where the Personal Data Owner cannot exercise his / her rights**

As per Article 28 of the KVKK, the following cases are excluded from the scope of the Law. they cannot assert their rights in these matters listed in 6.1.

- ü Processing of personal data in the scope of activities related to him or his family members living in the same dwelling by real persons, provided that they are not given to third parties and the data security obligations are complied with,
- ü Processing of personal data for purposes such as research, planning and statistics by making it anonymous with official statistics,
- ü Processing of personal data for art, history, literature or scientific purposes or within the scope of freedom of expression, provided that it does not violate national crime, national security, public security, public order, economic security, privacy of private life or personal rights or constitute a crime,
- ü Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations, which have been assigned by law to provide national defense, national security, public security, public order or economic security,
- ü The processing of personal data by judicial authorities or enforcement authorities in relation to investigations, prosecutions, proceedings or executions.

Pursuant to Article 28, paragraph 2 of the KVKK, the data holder may not exercise his or her rights under Article 6.1 of this Policy, except for the right to claim damages:

- ü Personal data processing is necessary for crime prevention or crime investigation.

- ü Processing of personal data publicized by the person concerned.
- ü Personal data processing is required for the conduct of supervisory or regulatory duties, and for disciplinary investigation or prosecution by authorized and authorized public institutions and organizations and professional organizations in the nature of public institutions based on the authority granted by law.
- ü Personal data processing is necessary to protect the economic and financial interests of the State in relation to budget, tax and financial matters.

### **6.3. Exercise of the Rights of the Personal Data Owner**

The personal data holder shall fill in the application form at [www.antaliumavm.com](http://www.antaliumavm.com) and [www.antaliumshopping.com](http://www.antaliumshopping.com) by filling the rights specified in article 6.1 of this Policy, wet signed or registered electronic mail address, secure electronic signature, mobile signature before notified and registered in the systems via e-mail address. The application form to be made is explained in detail in the an Application Form within the Scope of Personal Data Protection Law adresi which is provided above.

If the personal data holder wishes to use this right through his / her representative, the documents proving his / her identity, approved by the competent authorities, supporting documents, if any, should be forwarded to Antalyum Shopping Center attached to the application form.

### **6.4. Antalyum Shopping Center's Response to Applications**

Antalyum Shopping Center will finalize the requests directed to it free of charge within the shortest time and within thirty days at the latest according to the nature of the demand. In case a cost arises due to the fulfillment of the demands, the fees in the tariff determined by the KVK Board may be requested.

Antalyum AVM may accept the request or reject it by explaining its justification; informs the personal data owner in writing or electronically. In case the request in the application is accepted, Antalyum Shopping Center fulfills the requirement of the request.

### **6.5. Personal Data Holder's right to complain to the KVK Board**

In case of rejection of the application, inadequate response or failure to respond to the application in due time; The holder of the personal data is entitled to file a complaint with the KVK Board within thirty days from the date of receiving the reply of Capito Antalyum AVM and probably within sixty days from the date of application.

## **PART SEVEN - PROCESSING, STORAGE AND DISPOSAL OF PERSONAL DATA GOVERNANCE STRUCTURE**

### **7.1. Unit responsible for the processing, storage and disposal of personal data**

The AV Personal Data Protection Committee "was established by Antalyum Shopping Center, which has the authority to make decisions and submit them to senior management for the purpose of ensuring, preserving, maintaining, managing and improving the personal data protection legislation and providing the necessary coordination within the structure of Antalyum Shopping Center for this purpose. The business units, titles and job descriptions of those responsible in the Personal Data Protection Committee are explained in detail in ANNEX.2.

The duties of this committee are as follows:

- ü To coordinate and manage all activities related to the processing, storage, protection and destruction of personal data at Antalyum Shopping Center.

- ü To prepare the basic policies regarding the processing, storage, protection and destruction of personal data and to submit them to the senior management for approval.
- ü To ensure the implementation of policies concerning the processing, storage, protection and destruction of personal data, to manage the compliance process with the legislation and company policy and to report to the senior management,
- ü Within the scope of the activities carried out by Antalya AVM as the data responsible, the employees working in the company and outside the company, customers, suppliers, business partners, employee candidates, visitors, platform users, subcontractors, subcontractors, subcontractors, etc. to coordinate communication, to provide the necessary organization for this purpose,
- ü To make the necessary activities and arrangements within the company regarding the demands, requests, complaints and notifications of the Personal Data Protection Board, to organize the processes,
- ü To accept the notifications and correspondence made by the Personal Data Protection Authority, to fulfill the requirements, to carry out the communication with the Authority on behalf of the Company,
- ü To make the necessary activities and arrangements within the company regarding the demands, requests, complaints and notifications from the related persons, to organize the processes, to ensure the communication with the relevant person,
- ü Updating the personal data processing inventory and following up the data processing activities, reporting, inventorying and, in case of changes, making the necessary updates in VERBİS (Data Responsible Registry Information System), performing all transactions related to VERBİS,
- ü To organize trainings for employee awareness, to ensure the continuity of the trainings, to measure the efficiency,
- ü Raising awareness and informing about the processing, storage, protection and destruction of personal data in Antalya Shopping Center and the institutions that Antalya Shopping Center cooperates with,
- ü Deciding how the audit of personal data processing activities will be performed and ensuring the necessary coordination in this context,
- ü To determine or ensure the determination of the technical and administrative measures taken by the persons who process personal data regarding data security, to conduct inspections or to have them done,
- ü To formulate policies, procedures or directives where necessary, and to make the necessary arrangements for their creation, to ensure that these documents are announced,
  
- ü To determine the risks that may occur in personal data processing activities and to ensure that necessary measures are taken; submit action plans and improvement proposals to the senior management for approval and coordinate their execution,
- ü To conduct internal audits within the scope of KVKK compliance, to make the necessary arrangements if external audits are to be taken, and to determine and evaluate the measures to be taken for the identified risks,
- ü Working together with Information Security units or consultancy firms for the protection of personal data, participating in evaluations, presenting reports,
- ü Direct reporting to senior management,
- ü To follow the announcements of the KVKK board and the developments related to the legislation, to ensure that they are put into practice and to make the necessary notifications,
- ü Managing processes for data privacy breaches, identifying responsible person / team and tasks, reporting and managing corrective actions

## **CHAPTER EIGHT - UPDATE, COMPLIANCE AND CHANGES**

### **8.1. Update and Compliance**

Antalyum AVM reserves the right to make changes in this Policy and other related and related policies in accordance with the decisions of the KVK Board or in line with the developments in the sector or IT field due to the amendments made to the Law.

Amendments to this Policy are immediately transcribed and explanations of the changes are disclosed at the end of the Policy.

### **8.2. Amendments**

**12/06/2019: A policy to process, store and dispose of personal data has been published.**

<b>ANNEX.1 - STORAGE AND DISPOSAL TIME TABLE OF PERSONAL DATA BUSINESS PROCESS</b>	<b>STORAGE TIME</b>	<b>DISPOSAL TIME</b>
<b>Documents relating to general company resolutions such as power of attorney, signature circular, general assembly resolutions, dismissals</b>	10 years from the date of first registration	Within 180 days after the end of storage period
<b>Information on the Company's shareholders and board members</b>	10 years from the end of the business relationship	Within 180 days after the end of storage period
<b>Agreements signed with third parties (Lease agreements, service agreements, organization agreements, etc.)</b>	10 years from the expiry date of the relevant contract	Within 180 days after the end of storage period
<b>Store Rental Forms, Rental Application Forms</b>	10 years from the date of first registration	Within 180 days after the end of storage period
<b>Tenant store contact forms</b>	1 year from the end of the business relationship	Within 180 days after the end of storage period
<b>Personal health data of employees</b>	30 years from the date of termination	Within 180 days after the end of storage period
<b>Employee recruitment files, personal data</b>	50 years from the date of termination	Within 180 days after the end of storage period
<b>Personal data obtained from occupational health and safety practices</b>	15 years from the date of termination	Within 180 days after the end of storage period

<b>Employee candidate application forms, CVs</b>	1 year from the date of application	Within 180 days after the end of storage period
<b>Responding to court / enforcement information requests related to the employee</b>	10 years from the end of the business relationship	Within 180 days after the end of storage period
<b>Personal data of subcontractor / subcontractor employees</b>	10 years from the expiry date of the relevant contract	Within 180 days after the end of storage period
<b>Data for subcontractor / subcontractor employees</b>	1 year from the date of first registration	Within 180 days after the end of storage period
<b>CCTV recordings processed for security purposes</b>	30 days	At the end of Storage Period
<b>Administrative reports regarding security such as due diligence report and event report</b>	5 years from the date of first registration	Within 180 days after the end of storage period
<b>Recording / Tracking Systems</b>	1 year from the date of first registration	Within 180 days after the end of storage period
<b>Data processed through forms for operation management (entry card form, night job tracking form, vehicle schedule, etc.)</b>	1 year from the date of first registration	Within 180 days after the end of storage period
<b>Business contacts</b>	10 years	Within 180 days after the end of storage period
<b>Data obtained during sales, marketing activities and demand / complaint management of customers (identity, communication, marketing and transaction data, etc.)</b>	10 years from the date of first registration	Within 180 days after the end of storage period
<b>Transaction records of customers (including valet services records, parking ticket records, etc. including identity and contact data)</b>	1 year from the date of first registration	Within 180 days after the end of storage period

<b>Parking subscriber registration forms</b>	1 year from the expiration date of the service relationship	Within 180 days after the end of storage period
<b>Records of financial / payment transactions</b>	10 years from the date of termination	Within 180 days after the end of storage period
<b>Consent for the use of social media</b>	5 years	Within 180 days after the end of storage period
<b>Data on wireless internet usage</b>	2 years from the date of first registration	Within 180 days after the end of storage period

<b>Technical service visitor records</b>	1 year from the date of first registration	1 year from the date of first registration Within 180 days from the end of the storage period
--	--	--

<b>Commercial Electronic Mail Records</b>	1 year from the date of first registration	1 year from the date of first registration Within 180 days from the end of the storage period
---	--	--

**ANNEX.2 - PERSONAL DATA PROTECTION COMMITTEE UNIT, TITLE AND DUTY LIST**

**ANTALIUM AVM PERSONAL DATA PROTECTION COMMITTEE**

.....			
.Attorney	Law	Data Responsible Representative / Personal Data Protection Manager / Data Responsible Contact	Management of the personal data destruction process in accordance with the periodic destruction period, ensuring compliance of the processes within the task with the retention period

..... ..... .Financial Affairs Department Manager	Financial affairs	Member of the Committee Responsible for Data Regarding the Shareholders and Authorities of the Company's Shareholders and Authorities and Business Connections (Including Stores)	Management of the personal data destruction process in accordance with the periodic destruction period, ensuring compliance of the processes within the task with the retention period
..... .....	Operation	Member of the Committee Responsible for Evaluating and Following Personal Data Inventory on the Basis of General Archiving and Destruction Processes and Storage and Data Destruction Periods and Coordinating Business Units	Management of the personal data destruction process in accordance with the periodic destruction period, ensuring compliance of the processes within the task with the retention period
Operations Department Manager	Corporate communications	Member of the Committee Responsible for Data Regarding Company Customers and Platform Users	Management of the personal data destruction process in accordance with the periodic destruction period, ensuring compliance of the processes within the task with the retention period
..... ..	Human resources	Member of the Committee Responsible for Data on Company Employees and Candidates	Management of the personal data destruction process in accordance with the periodic destruction period, ensuring compliance of the processes within the task with the retention period

Corporate Communications Department Manager	Administrative Affairs	Member of the Committee Responsible for the Data Regarding the Visitors of the Company and the Shopping Center Managed, Employees of the Store, Employees of All Subcontractors	Management of the personal data destruction process in accordance with the periodic destruction period, ensuring compliance of the processes within the task with the retention period
..... ....	Technical	Member of the Committee Responsible for Processed Data (Log Records) of Users within the Scope of the Use of Wireless Internet Services Provided in the Shopping Center Managed by Our Company	Management of the personal data destruction process in accordance with the periodic destruction period, ensuring compliance of the processes within the task with the retention period
Human Resources Department Manager	Information technologies	Regarding Information Security and Data Security	Periodic destruction by ensuring compliance of processes within the scope of duty with storage period
Big Customers Representing Information Services Company	Manager Lojistik and Textile Limited	Committee Responsible for Technologies and Measures	Member management of personal data destruction process in accordance with