BMS GERİ DÖNÜŞÜM SANAYİ VE TİCARET ANONİM ŞİRKETİ

PERSONAL DATA PROTECTION AND PROCESSING POLICY

Approved by the Board of Directors.

Effective Date: .../.../... (FILL IN)

TABLE OF CONTENTS

ACRONYMS AND CONCEPTS

KVKK/Law	Law on the Protection of Personal Data No. 6698 published in the Official Gazette dated April 7, 2016 and numbered 29677
GDPR	EU (European Union) General Data Protection Regulation
Constitution	Constitution of the Republic of Turkey dated November 7, 1982 and numbered 2709, published in the Official Gazette dated November 9, 1982 and numbered 17863
Data Processor	A person who processes personal data outside the organization of the data controller and in line with the authorization and instruction received from the data controller, except for the person or unit responsible for the technical storage, protection and backup of the data.
Data Subject/Relevant Person	Employees, customers, business partners, shareholders, officials, potential customers, candidate employees, interns, visitors, suppliers, employees of the institutions they cooperate with, third parties and other persons, including but not limited to those listed here, of the Data Controller/affiliates to which BMS GERI DÖNÜŞÜM SANAYİ VE TİCARET ANONİM ŞİRKETİ is affiliated and/or BMS GERI DÖNÜŞÜM SANAYİ VE TİCARET ANONİM ŞİRKETİ real people.

Data Controller	The natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system. In the eyes of this Policy, the information of BMS GERI DÖNÜŞÜM SANAYİ VE TİCARET ANONİM ŞİRKETİ will be referred to as the Data Controller hereinafter.
Explicit Consent	Consent on a specific subject, based on information and expressed with free will.
Annihilation	Deletion, destruction or anonymization of personal data.
Storage/Recording Media	Any medium containing personal data that is fully or partially automated or processed by non-automatic means, provided that it is part of any data recording system.
Personal data	Any information relating to an identified or identifiable natural person.
Sensitive Personal Data (Sensitive Data)	Data related to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, disguise and dress, membership to associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.
Processing of Personal Data	Obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic or non-automatic means, provided that it is a part of any data recording system.
Anonymization of Personal Data	Making personal data unrelated to an identified or identifiable natural person in any way, even by matching it with other data.
Deletion of Personal Data	Deletion of personal data; making personal data inaccessible and unusable in any way for the relevant users.
Destruction of Personal Data	The process of making personal data inaccessible, unrecoverable and unusable by anyone in any way.
Periodic Destruction	In the event that all of the conditions for processing personal data in the law disappear, the deletion, destruction or anonymization process to be carried out ex officio at repeated intervals.
Regulation	Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette No. 30224 dated October 28, 2017 and entered into force as of January 1, 2018.
KVK Board / Board	Personal Data Protection Board
KVK Institution	Personal Data Protection Authority
Policy	Data Controller Personal Data Protection and Processing Policy
Turkish Penal Code	Published in the Official Gazette dated 12 October 2004 and numbered 25611; Turkish Penal Code No. 5237 dated September 26, 2004.
Disclosure	The data controller refers to the relevant persons in obtaining

Obligation	personal data; Providing information about the identity of the Data Controller, the purpose for which the personal data will be processed, to whom the processed personal data can be transferred and for what purpose, the method and legal reason for collecting personal data, and the rights of the person concerned listed in Article 11 of the KVKK.
Data Controllers Registry Information System (VERBIS)	It is a data recording system established by the Presidency under the supervision of the Board, where data controllers register and declare information about data processing activities.

1. INTRODUCTION

1.1. Objective

As the Data Controller, we are aware of our responsibility for the protection and legal security of personal data, which is regulated as a constitutional right, and we attach importance to the safe use of your personal data.

The purpose of this policy is to regulate the methods and principles to be followed in order to ensure that BMS GERASe, DENYİM SANAYİ VE TİCARET ANONİM ŞİRKETİ processes and protects personal data in accordance with the Law on the Protection of Personal Data (KVKK) published in the Official Gazette dated April 7, 2016 and numbered 29677.

In this way, it is aimed to ensure full compliance with the legislation in the processing and protection of personal data carried out by the Data Controller and to protect all rights of personal data owners arising from the legislation regarding personal data.

1.2. Scope

This policy is implemented in the activities carried out for the processing and protection of all personal data, which is managed by BMS GERI DÖNÜŞÜM SANAYİ VE TİCARET ANONİM ŞİRKETİ.

This policy; It covers real persons whose personal data are processed by the Data Controller, by automatic or non-automatic means, provided that they are part of any data recording system. This Policy does not apply to legal entities and their data in any way.

Groups of Persons Whose Data Are Processed within the Scope of the Policy
Shareholder/Partner
Employee
Product or Service Recipient
Supplier Authority
Supplier Employee
Visitor

Potential Product or Service Buyer
Parent / Guardian / Representative
Intern
Employee Candidate
Switchboard - Telephone Call Call Side
Public Servant
Case, Enforcement File Party
Doctor
Occupational Health and Safety Specialist

The entire scope of application of this Policy will cover all personal data owners in the above-mentioned categories of relevant person groups; Some of its provisions may only be directed to certain groups of interested persons.

This policy is implemented by the Data Controller in the activities carried out for the processing and protection of all personal data, together with the relevant detailed data procedures.

1.3. Implementation of the Policy and Relavted Legislation

Within the scope of this Policy, the relevant legal regulations and data security principles in force in the national legislation on the processing and protection of personal data will primarily be applied. In case of inconsistency between the legislation in force and the Policy, he/she accepts that the current legislation will be applied as the Data Controller.

2. ISSUES RELATED TO THE PROTECTION OF PERSONAL DATA

In accordance with Article 12 of the KVK Law, the Data Controller takes the necessary technical and administrative measures to ensure the appropriate level of security in order to prevent the unlawful processing of the personal data it processes, to prevent unlawful access to the data and to ensure the protection of the data, and to carry out or have the necessary audits carried out in this context.

2.1. Ensuring the Security of Personal Data

2.1.1. Technical and Administrative Measures Taken to Ensure the Processing of Personal Data in Accordance with the Law, to Prevent Unlawful Access and to Store it in Secure Environments

Subject to the confidentiality of personal data, the Data Controller takes technical and administrative measures according to technological possibilities and implementation costs in order to ensure the appropriate level of security in order to ensure that personal data is processed in accordance with the law, to prevent unlawful access to this data, to prevent loss and destruction, and to ensure that it is stored and preserved in secure environments.

2.1.1.1. Technical Measures Taken to Ensure the Legal Processing of Personal Data, to Prevent Unlawful Access and to Store it in Secure Environments

The main technical measures taken by the Data Controller to ensure the appropriate level of security in order to ensure the processing of personal data in accordance with the law, to prevent unlawful access to this data, to prevent loss and destruction, and to ensure its storage and preservation in secure environments, subject to personal data confidentiality, are listed below:

Technical Measures
Network security and application security are ensured
Closed system network is used for personal data transfers via network
Key management is implemented
Security measures are taken within the scope of procurement, development and maintenance of information technology systems
Access logs are kept regularly
Data masking measures are applied when necessary
Up-to-date anti-virus systems are used
Firewalls are used
Personal data is backed up and the security of the backed up personal data is also ensured
User account management and authorization control system are implemented and these are also monitored
Log records are kept in such a way that there is no user intervention
Cyber security measures have been taken and their implementation is constantly monitored
Encryption is done

2.1.1.2. Administrative Measures Taken to Ensure the Lawful Processing of Personal Data, To Prevent Unlawful Access and to Store it in Secure Environments

The main administrative measures taken by the Data Controller to ensure the appropriate level of security in order to ensure the processing of personal data in accordance with the law, to prevent unlawful access to this data, to prevent loss and destruction, and to ensure its storage and preservation in secure environments, subject to personal data confidentiality, are listed below:

Administrative Measures
Disciplinary regulations with data security provisions are in place for employees
Training and awareness activities are carried out at regular intervals on data security for employees
An authorization matrix has been created for employees
Confidentiality commitments are made

Employees who have a job change or leave their job are removed from their authority in this area
The signed contracts contain data security provisions
Personal data security policies and procedures have been determined
Personal data security issues are reported quickly
Personal data security is monitored
Necessary security measures are taken regarding entry and exit to physical environments containing personal data
The security of physical environments containing personal data against external risks (fire, flood, etc.) is ensured
The security of environments containing personal data is ensured
Personal data is reduced as much as possible
Periodic and/or random audits are carried out and carried out in-house
Existing risks and threats have been identified
Protocols and procedures for the security of sensitive personal data have been determined and implemented
Data processing service providers are periodically audited on data security

2.1.2. Supervision of Measures Taken for the Protection of Personal Data

In accordance with Article 12 of the KVK Law, the Data Controller conducts or has the necessary audits carried out within its own body. The results of the precautionary audit carried out within the scope of the audit activities required to fulfill the obligations of the legal regulations constituting the planning for the protection of personal data are reported to the relevant department within the scope of the internal functioning of the Data Controller and necessary activities are carried out to improve the measures taken.

2.1.3. Measures to be Taken in Case of Unauthorized Disclosure of Personal Data

The Data Controller has an obligation to protect the personal data it processes against unauthorized access, unlawful processing, disclosure, loss and alteration. In the event that personal data processed in accordance with Article 12 of the KVK Law is obtained and used by unauthorized others illegally, it carries out the system that ensures that this situation is notified to the relevant personal data owner and the KVK Board as soon as possible.

2.2. Observing the Rights of the Data Owner; Creating Channels to Convey These Rights to the Data Controller and Evaluation of the Requests of Data Owners

The Data Controller carries out the necessary channels, internal functioning, administrative and technical arrangements in accordance with Article 13 of the KVK Law in order to evaluate the rights of personal data owners and to provide the necessary information to personal data owners.

If personal data owners submit their requests regarding their rights listed below in writing to us, the Data Controller, the application is concluded free of charge as soon as possible and

within thirty days at the latest, depending on the nature of the request. However, if the transaction requires an additional cost, the fee in the tariff determined by the KVK Board will be collected from the applicant data owner.

Personal data owners;

- To learn whether personal data is processed or not,
- If personal data has been processed, requesting information about it,
- To learn the purpose of processing personal data and whether they are used in accordance with their purpose
- To know the third parties to whom personal data is transferred in the country or abroad,
- Requesting correction of personal data in case of incomplete or incorrect processing and requesting notification of the transaction made within this scope to third parties to whom personal data has been transferred,
- Although it has been processed in accordance with the provisions of the KVK Law and other relevant laws, to request the deletion or destruction of personal data in the event that the reasons requiring its processing disappear, and to request the notification of the transaction made within this scope to the third parties to whom the personal data has been transferred,
- Objecting to the occurrence of a result against the person himself by analyzing the processed data exclusively through automated systems,
- In case of damage due to unlawful processing of personal data, it has the right to demand the compensation of the damage.

2.3. Protection of Sensitive Personal Data

With the KVK Law, special importance has been attached to some sensitive personal data due to the risk of causing victimization or discrimination of individuals in case of unlawful processing.

These data; race, ethnicity, political opinion, 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.

The Data Controller acts sensitively in the protection of sensitive personal data that is determined as "special quality" by the KVK Law and processed in accordance with the law. In this context, the technical and administrative measures taken by the Data Controller for the protection of personal data are carefully implemented in terms of sensitive personal data, necessary audits are provided within the Data Controller, and a Processing and Protection Policy for Sensitive Personal Data is also established.

2.4. Increasing the Awareness and Supervision of Business Units on the Protection and Processing of Personal Data

The Data Controller ensures that the necessary trainings are organized for business units in order to raise awareness in order to prevent unlawful processing of personal data, unlawful access to data and to ensure the protection of data.

Necessary systems are established to raise awareness of the Data Controller's existing employees of the business units and the employees who have just joined the business unit about the protection of personal data, and if necessary, professional people are worked on.

The results of the training carried out to raise awareness of the business units of the data controller on the protection and processing of personal data are reported to the Data Controller. In this direction, the Data Controller evaluates the participation in the relevant trainings, seminars and information sessions and conducts or has the necessary audits done. As the Data Controller, the trainings carried out by us in parallel with the update of the relevant legislation are updated and renewed.

3. ISSUES RELATED TO THE PROCESSING OF PERSONAL DATA

Data Controller, in accordance with Article 20 of the Constitution and Article 4 of the KVK Law, regarding the processing of personal data; in accordance with the law and the rules of good faith; accurate and up-to-date when necessary; pursuing specific, clear and legitimate purposes; It carries out personal data processing activities in a limited and measured manner in connection with the purpose.

The Data Controller retains personal data for the period stipulated by law or required by the purpose of processing personal data.

Pursuant to Article 20 of the Constitution and Article 5 of the KVK Law, the Data Controller processes personal data based on one or more of the conditions in Article 5 of the KVK Law regarding the processing of personal data.

In accordance with Article 20 of the Constitution and Article 10 of the KVK Law, the Data Controller enlightens personal data owners and provides the necessary information in case personal data owners request information.

The Data Controller acts in accordance with the regulations stipulated in terms of the processing of sensitive personal data in accordance with Article 6 of the KVK Law.

In accordance with Articles 8 and 9 of the KVK Law, the Data Controller acts in accordance with the regulations stipulated in the law and set forth by the KVK Board regarding the transfer of personal data.

3.1. Processing of Personal Data in Accordance with the Principles Stipulated in the Legislation

3.1.1. Processing in Accordance with the Law and Good Faith

Data Controller; In the processing of personal data, it acts in accordance with the principles brought by legal regulations and the general rule of trust and honesty. In this context, the Data Controller takes into account the proportionality requirements in the processing of personal data and does not use personal data for purposes other than its purpose.

3.1.2. Ensuring that Personal Data is Accurate and Up-to-Date When Necessary

Data Controller; It ensures that the personal data it processes is accurate and up-to-date, taking into account the fundamental rights of personal data owners and their own legitimate interests. It takes the necessary measures in this direction.

3.1.3. Processing for Specific, Explicit, and Legitimate Purposes

The Data Controller clearly and precisely determines the purpose of processing personal data that is legitimate and in accordance with the law. The Data Controller processes personal data in connection with the service it provides and to the extent necessary for them. The purpose for which personal data will be processed by the Data Controller is set forth before the personal data processing activity begins.

3.1.4. Being Relevant, Limited and Proportionate to the Purpose for which they are Processed

The Data Controller processes personal data in a manner suitable for the realization of the specified purposes and avoids the processing of personal data that is not related to the realization of the purpose or is not needed.

3.1.5. Retention for the Period Stipulated in the Relevant Legislation or Required for the Purpose for which they are Processed

The Data Controller retains personal data only for the period specified in the relevant legislation or required for the purpose for which they are processed. In this context, the Data Controller first determines whether a period of time is stipulated for the storage of personal data in the relevant legislation, if a period is determined, it acts in accordance with this period, and if a period is not determined, it stores personal data for the period required for the purpose for which they are processed. In the event that the period expires or the reasons requiring its processing disappear, the personal data is deleted, destroyed or anonymized by the Data Controller. Personal data is not stored by the Data Controller with the possibility of future use.

3.2. Personal Data, 5. Processing Based on One or More of the Personal Data Processing Conditions Specified in the Article and Limited to These Terms

The protection of personal data is a Constitutional right. Fundamental rights and freedoms can only be limited by law and only for the reasons specified in the relevant articles of the Constitution, without touching their essence. Pursuant to the third paragraph of Article 20 of the Constitution, personal data can only be processed in cases stipulated by law or with the explicit consent of the person. In this direction and in accordance with the Constitution, the Data Controller; It processes personal data only in cases stipulated by law or with the explicit consent of the person.

3.3. Informing the Personal Data Owner

In accordance with Article 10 of the Data Controller and KVK Law, it enlightens personal data owners during the acquisition of personal data. In this context, it clarifies the identity of the Data Controller and its representative, if any, for what purpose the personal data will be processed, to whom and for what purpose the processed personal data can be transferred, the method of collecting personal data and the rights of the personal data owner for legal reasons.

Article 20 of the Constitution stipulates that everyone has the right to be informed about their personal data. Accordingly, in Article 11 of the KVK Law, "requesting information" is also

listed among the rights of the personal data owner. In this context, in accordance with Article 20 of the Constitution and Article 11 of the KVK Law, the Data Controller provides the necessary information in case the personal data owner requests information.

While fulfilling its obligation to inform, the Data Controller acts in accordance with the Law No. 6698, the Communiqué on the Procedures and Principles to be Followed in the Fulfillment of the Obligation to Inform, the Board decisions published on the website of the Authority and the Guide to the Fulfillment of the Obligation to Inform prepared by the Authority.

3.4. Processing of Sensitive Personal Data

In the processing of personal data determined as "special quality" by the Data Controller with the KVK Law, the regulations stipulated in the KVK Law are strictly complied with.

In Article 6 of the KVK Law, a number of personal data that carries the risk of causing victimization or discrimination when processed unlawfully is determined as "special quality". These data; race, ethnicity, political opinion, 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.

By the Data Controller in accordance with the KVK Law; Sensitive personal data is processed in the following cases, provided that adequate measures to be determined by the KVK Board are taken:

- If the personal data owner has explicit consent

or

- If the personal data owner does not have explicit consent;

Sensitive personal data other than the health and sexual life of the personal data owner, in cases stipulated by law,

Sensitive personal data related to the health and sexual life of the personal data owner are processed only by persons or authorized institutions and organizations under the obligation of confidentiality for the purpose of protecting public health, conducting preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing.

In terms of the processing of sensitive personal data, a separate policy is created by the Data Controller.

3.5. Transfer of Personal Data

The Data Controller may transfer the personal data and sensitive personal data of the personal data owner to third parties by taking the necessary security measures in line with the personal data processing purposes in accordance with the law. Accordingly, the Data Controller acts in accordance with the regulations stipulated in Article 8 of the KVK Law.

3.5.1. Conditions for Transfer of Personal Data

In line with the legitimate and lawful personal data processing purposes, the Data Controller may transfer personal data to third parties based on and limited to one or more of the personal data processing conditions specified in Article 5 of the Law listed below:

- If the personal data owner has explicit consent;
- If there is a clear regulation in the laws regarding the transfer of personal data,
- If it is necessary for the protection of the life or bodily integrity of the personal data owner or someone else, and the personal data owner is unable to disclose his consent due to actual impossibility, or if his consent is not legally valid;
- If it is necessary to transfer the personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract
- If personal data transfer is mandatory for the Data Controller to fulfill its legal obligation,
- If the personal data has been made public by the personal data owner,
- If the transfer of personal data is mandatory for the establishment, exercise or protection of a right,
- Provided that it does not harm the fundamental rights and freedoms of the personal data owner, if the transfer of personal data is mandatory for the legitimate interests of the Data Controller.

3.5.2. Transfer of Sensitive Personal Data

The Data Controller takes the necessary care and takes the necessary security measures and adequate measures stipulated by the KVK Board; In line with the legitimate and lawful personal data processing purposes, it may transfer the sensitive data of the personal data owner to third parties in the following cases.

- If the personal data owner has explicit consent

or

- If the personal data owner does not have explicit consent;

Sensitive personal data other than the health and sexual life of the personal data owner (race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, disguise and dress, membership to associations, foundations or unions, criminal convictions and security measures, and biometric and genetic data), in cases stipulated by law,

Sensitive personal data related to the health and sexual life of the personal data owner are transferred to persons or authorized institutions and organizations under the obligation of confidentiality only for the purpose of protecting public health, conducting preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing.

3.6. Transfer of Personal Data Abroad

The Data Controller may transfer the personal data and sensitive personal data of the personal data owner to third parties abroad by taking the necessary security measures in line with the personal data processing purposes in accordance with the law.

As a result of the widespread use of company applications that provide information services today, communication is established through instant messaging or online communication channels through platforms and applications of foreign origin. For this reason, it is possible to transfer data abroad through these platforms.

Personal data by the Data Controller; It is transferred to foreign countries that are declared to have adequate protection by the KVK Board or, in the absence of adequate protection, to foreign countries where the data controllers in Turkey and the relevant foreign country undertake an adequate protection in writing and where the KVK Board has the permission ("Foreign Country where the Data Controller Undertaking Adequate Protection is Located"). In this direction, the Data Controller acts in accordance with the regulations stipulated in Article 9 of the KVK Law.

3.6.1. Conditions for the Transfer of Personal Data Abroad

If the Data Controller has the explicit consent of the personal data owner in line with the legitimate and lawful personal data processing purposes or if the personal data owner does not have explicit consent, it may transfer personal data to Foreign Countries with Adequate Protection or where the Data Controller Committing to Adequate Protection is located, in the presence of one of the following situations:

- If there is a clear regulation in the laws regarding the transfer of personal data,
- If it is necessary for the protection of the life or bodily integrity of the personal data owner or someone else, and the personal data owner is unable to disclose his consent due to actual impossibility, or if his consent is not legally valid;
- If it is necessary to transfer the personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract,
- If personal data transfer is mandatory for the Data Controller to fulfill its legal obligation

3.6.2. Transfer of Sensitive Personal Data Abroad

- If the personal data owner has explicit consent

or

- If the personal data owner does not have explicit consent;

Sensitive personal data other than the health and sexual life of the personal data owner (race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, disguise and dress, membership to associations, foundations or unions, criminal convictions and security measures, and biometric and genetic data), in cases stipulated by law,

Sensitive personal data related to the health and sexual life of the personal data owner can only be transferred within the scope of processing by persons or authorized institutions and organizations under the obligation of confidentiality for the purpose of protecting public

health, conducting preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing.

4. CATEGORIZATION, PROCESSING PURPOSES AND STORAGE PERIODS OF PERSONAL DATA PROCESSED BY THE DATA CONTROLLER

In accordance with Article 10 of the KVK Law, the Data Controller informs the personal data owner which groups of personal data owners process their personal data, the purposes of processing the personal data of the personal data owner and the retention periods within the scope of the disclosure obligation.

4.1. Categorization of Personal Data

By informing the Data Controller in accordance with Article 10 of the KVK Law, the Data Controller is based on one or more of the personal data processing conditions specified in Article 5 of the KVK Law in line with the legitimate and lawful personal data processing purposes, and to a limited extent, in accordance with the general principles specified in the KVK Law, especially the principles specified in Article 4 regarding the processing of personal data, and in accordance with all the obligations set out in the KVK Law. Personal data in the following categories are processed, limited to the subjects within the scope of the policy.

Personal Data Categorization	Explanation
Credential	clearly belonging to an identified or identifiable natural person; processed partially or fully automatically or non-automatically as part of a data recording system; data containing information about the identity of the person; (Documents such as driver's license, identity *card and passport containing information such as name-surname, TR identity number, nationality information, mother's name-father's name, place of birth, date of birth, gender, tax number, SSI number, signature information, vehicle license plate, etc. information)*
Audio/Visual Information	Clearly belongs to an identified or identifiable natural person; *(photo and camera recordings (except for recordings within the scope of Physical Space Security Information), audio recordings and data contained in documents that are copies of documents containing personal data)*
Personnel Information	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; *(; All kinds of personal data processed to obtain information that will be the basis for the formation of personal rights of real persons who have a working relationship with the Data Controller)*
Legal Process and Compliance Information	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; *(Information such as the data processed within the scope of the legal processes, determination of receivables and rights, follow-up and performance of debts and legal obligations of the Data Controller, information in correspondence with judicial*

	authorities, incoming and outgoing documents, case files.)
Contact Information	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; *(information such as phone number, address, e-mail address, fax number, IP address)*
Physical Space Security Information	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; *(Personal data regarding the records and documents taken at the entrance to the physical space, during the stay in the physical space; camera recordings, records taken at the security point, etc.)*
Criminal Conviction and Security Measures Information	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; *(Data such as the criminal record of the Personal Data Owner obtained within the framework of the operations carried out by the Data Controller's business units or in order to carry out the business processes of real persons who have a working relationship with the Data Controller or to protect the legal and other interests of the Data Controller and the Personal Data Owner)*
Financial Information	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; *(Personal data processed regarding information, documents and records showing all kinds of financial results created according to the type of legal relationship established by the Data Controller with the personal data owner, and data such as bank account number, IBAN number, credit card information, financial profile, asset data, income information)*
Location Data	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; *(information that determines the location of the personal data subject within the framework of operations carried out by business units, during the use of its products and services, or when employees use their vehicles; GPS location, travel data, etc.)*
Customer Transaction Information	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; *(Information such as call center records, invoice, promissory note check information, order information, request information, offer, service number obtained and produced about the data subject as a result of the commercial activities of the Data Controller and the operations carried out by the business units.)*
Risk Management Information	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; (Data processed for the *management of all kinds of commercial, technical and administrative risks created according to the type of legal*

	relationship established by the Data Controller with the Personal Data Owner.)
Health Information	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; *(Within the framework of the operations carried out by the business units of the Data Controller; Health Report of the Personal Data Owner and/or his family members, Disability tax exemption certificates, insurance documents, obtained in relation to the products and services offered or in order to carry out the business processes of real persons who have a working relationship with the Data Controller or to protect the legal and other interests of the Data Controller and the Personal Data Owner, health data such as military status certificate)*
Professional Experience Information	clearly belonging to an identified or identifiable natural person; processed partially or fully automatically or non-automatically as part of a data recording system; data containing information about the identity of the person; *(Data such as diploma information, courses attended, in-service training information, certificates, candidate application forms, reference interview information, job interview information, transcript information, processed according to the type of legal relationship established by the Data Controller with the Personal Data Owner.)*
Transaction Security Information	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; *(Personal data such as IP Address information, Website login and exit information, password and password information processed regarding the technical, administrative, legal and commercial security of both the Personal Data Owner and the Data Controller while carrying out the activities of the Data Controller)*
Marketing Information	clearly belongs to an identified or identifiable natural person; processed in whole or in part automatically or non-automatically as part of a data recording system; *(Shopping history information obtained and produced about the data subject as a result of the commercial activities of the Data Controller and the operations carried out by the business units, surveys, cookie records, data obtained through campaign work)*
Vehicle Information	Data that clearly belongs to an identified or identifiable natural person; processed partially or fully automatically or non-automatically as part of a data recording system (Vehicle License Plate, Vehicle License Plate, *Vehicle License Plate, Vehicle License Plate).*
Employee Family Member and Relative Information	Clearly belonging to an identified or identifiable natural person; processed partially or fully automatically or non-automatically as part of the data recording system *(Employee 1. Degree Relative Information, Employee 1. Degree Relative Information, Identity and Address Information of Working Family Members, Employee 1. Degree Relative Information, Identity and Address*

	Information of Working Family Members, Employee 1. Degree Relative Information, Working Family Members Identity and Address Information).

4.2. Purposes of Processing Personal Data

The Data Controller processes personal data limited to the purposes and conditions within the personal data processing conditions specified in paragraph 2 of Article 5 and paragraph 3 of Article 6 of the KVK Law. These purposes and conditions are;

- It is clearly stipulated in the Laws that the Data Controller will carry out the relevant activity regarding the processing of your personal data
- The processing of your personal data by the Data Controller is directly related and necessary for the establishment or performance of a contract
- The processing of your personal data is mandatory for the Data Controller to fulfill its legal obligation
- Provided that your personal data has been made public by you; processing of you by the Data Controller in a limited manner for the purpose of making it public
- The processing of your personal data by the Data Controller is mandatory for the establishment, exercise or protection of the rights of the Data Controller or you or third parties
- Provided that it does not harm your fundamental rights and freedoms, it is mandatory to carry out personal data processing activities for the legitimate interests of the Data Controller.
- It is mandatory for the protection of the life or bodily integrity of the personal data owner or someone else to carry out personal data processing activities by the Data Controller, and in this case, the personal data owner is unable to disclose his consent due to actual or legal invalidity
- It is stipulated in the laws in terms of sensitive personal data other than the health and sexual life of the personal data owner
- In terms of sensitive personal data related to the health and sexual life of the personal data owner, it is processed by persons or authorized institutions and organizations under the obligation of confidentiality for the purpose of protecting public health, conducting preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing.

In this context, the Data Controller processes your personal data for the following purposes:

Processing Purposes
Execution / Supervision of Business Activities
Execution of Finance and Accounting Affairs

Execution of Management Activities
Follow-up and Execution of Legal Affairs
Execution of Audit / Ethics Activities
Conducting Internal Audit / Investigation / Intelligence Activities
Execution of Goods / Services After-Sales Support Services
Execution of goods / services production and operation processes
Execution of Goods / Services Procurement Processes
Execution of Supply Chain Management Processes
Ensuring the security of movable property and resources
Fulfillment of Obligations Arising from Employment Contract and Legislation for Employees
Creation and follow-up of visitor records
Ensuring Physical Space Security
Execution of Logistics Activities
Execution of Communication Activities
Execution of Goods / Services Sales Processes
Execution of Business Continuity Activities
Providing information to authorized persons, institutions and organizations
Execution of Contract Processes
Execution of Occupational Health / Safety Activities
Execution of Activities in Accordance with the Legislation
Execution of Risk Management Processes
Ensuring the Security of Data Controller Operations
Execution of Customer Relationship Management Processes
Follow-up of Requests / Complaints
Planning Human Resources Processes
Receiving and Evaluating Suggestions for the Improvement of Business Processes
Execution of Benefits and Benefits Processes for Employees
Execution of Wage Policy
Execution of Employee Candidate / Intern / Student Selection and Placement Processes
Execution of Application Processes of Employee Candidates
Execution of Assignment Processes
Execution of Educational Activities

Execution of Termination Proceedings
Execution of Human Resources Processes
Execution of Emergency Management Processes
Execution of Information Security Processes
Execution of Access Authorizations
Execution of Company / Product / Services Loyalty Processes
Execution of Marketing Analysis Studies

If the processing activity carried out for the aforementioned purposes does not meet any of the conditions stipulated under the KVK Law, your explicit consent is obtained by the Data Controller regarding the relevant processing process.

4.3. Retention of Personal Data

4.3.1. Retention Periods of Personal Data

If stipulated in the relevant laws and regulations, the Data Controller stores personal data for the period specified in these legislations. The retention periods determined by the Data Controller are as follows:

Data Category	Retention Period
Identity	15 years from the termination of the employment contract 10 years from the termination of the legal relationship 10 years from the termination of the purpose of data processing 10 Years from the end of the activity 10 Years from the termination of the purpose of processing 15 Years from the termination of the employment contract 10 Years from the termination of the legal relationship 15 Years from the termination of the employment relationship 15 Years from the termination of the employment contract 5 years from the termination of the purpose of processing 1 Year
Audiovisual Recordings	15 years from the termination of the employment contract
Aslam	15 years from the termination of the employment contract

	10 years from the termination of the legal relationship
Legal Action	15 years from the termination of the employment contract 10 years from the termination of the legal relationship
Communication	15 years from the termination of the employment contract 10 years from the termination of the legal relationship 10 years from the termination of the purpose of data processing 10 Years from the end of the activity 10 Years from the termination of the purpose of processing 10 Years from the termination of the legal relationship 15 Years from the termination of the employment relationship 5 years from the termination of the purpose of processing 1 Year
Physical Space Security	15 years from the termination of the employment contract 1 Month
Criminal Conviction and Security Measures	10 years from the termination of the legal relationship 15 years from the termination of the employment contract 10 years from the termination of the purpose of data processing
Finance	10 years from the termination of the purpose of data processing 15 years from the termination of the employment contract 10 years from the termination of the legal relationship 10 Years from the end of the activity 10 Years from the termination of the legal relationship
Location	10 years from the termination of the legal relationship 15 Years from the termination of the employment contract 15 years from the termination of the employment contract 15 Years from the termination of the employment contract 10 years from the termination of the purpose of data processing

Customer Transaction	10 years from the termination of the legal relationship 15 years from the termination of the employment contract 10 Years from the end of the activity
Risk Management	15 years from the termination of the employment contract 10 Years from the end of the activity 10 years from the termination of the legal relationship
Vehicle Information	15 Years from the termination of the employment contract 10 years from the termination of the legal relationship 15 Years from the termination of the employment contract
Health Information	10 Years from the end of the activity 15 years from the termination of the employment contract 15 Years from the termination of the employment relationship
Professional Experience	10 Years from the end of the activity 15 years from the termination of the employment contract
Employee Family Member and Relative Information	15 years from the termination of the employment contract
Transaction Security	10 years from the termination of the purpose of data processing 5 years from the termination of the purpose of processing
Marketing	10 years from the termination of the purpose of data processing

In this context, personal data are stored for the minimum storage periods stipulated within the framework of the Laws and required for the purpose for which they are processed:

If a period of time is not regulated in the legislation regarding how long personal data should be stored, Personal Data is processed for the period that requires it to be processed in accordance with the practices of the Data Controller and the practices of its commercial life, depending on the activity carried out by the Data Controller while processing that data, and then it is deleted, destroyed or anonymized. You can find detailed information on this subject in the Policy on Deletion, Destruction or Anonymization of Personal Data of the Data Controller.

The purpose of processing personal data has ended; If the retention periods determined by the relevant legislation and the Data Controller have come to an end; Personal data can only be stored for the purpose of constituting evidence in possible legal disputes or asserting the relevant right related to personal data or establishing a defense. In the establishment of the periods herein, the statute of limitations for asserting the aforementioned right and the

retention periods are determined based on the examples in the requests made to the Data Controller on the same issues before, despite the expiry of the statute of limitations. In this case, the stored personal data is not accessed for any other purpose and access to the relevant personal data is provided only when it is required to be used in the relevant legal dispute. Here, too, after the expiry of the aforementioned period, personal data is deleted, destroyed or anonymized.

4.3.2. Responsibilities and Distribution of the Duties in the Storage of Personal Data

All units and employees of the Data Controller are responsible for the proper implementation of the technical and administrative measures taken by the responsible units within the scope of the Policy, the training and awareness of the unit employees, monitoring and continuous supervision, and the prevention of unlawful processing of personal data, the prevention of unlawful access to personal data and data security in all environments where personal data is processed in order to ensure that personal data is stored in accordance with the law. It actively supports the responsible units in taking technical and administrative measures to ensure that they are provided.

4.3.3. Storage Environments

Personal data belonging to data owners are securely stored by the Data Controller in the environments listed in the table below, in accordance with the relevant legislation, especially the provisions of the KVKK:

Storage Media
Computer
Locked Archive Cabinet
Archive Cabinet
Archive Room
Double Locker in Controlled Zone
Locker
Hard Disk
Paper
Unit Archive
Business Server
Overseas Email Server
Domestic Email Server
Excel Program
Server
Flash Memory
Access Restricted File

5. CATEGORIZATION OF THE OWNERS OF PERSONAL DATA PROCESSED BY THE DATA CONTROLLER

The table below details the above-mentioned categories of personal data owners and the types of personal data processed by the persons within these categories.

Personal Data Owner Category and Disclosure	Category of Processed Personal Data of the Data Owner
Shareholder/Partner *(Real persons who are shareholders of the Data Controller)*	Identity Audiovisual Recordings Communication Physical Space Security Legal Action Risk Management Finance Vehicle Information Professional Experience Location Transaction Security
Employee *(real persons who have an employment contract with the Data Controller)*	Identity Aslam Legal Action Communication Audiovisual Recordings Physical Space Security Criminal Conviction and Security Measures Location Vehicle Information Health Information Finance Professional Experience Employee Family Member and Relative Information Transaction Security Marketing
Product or Service Buyer, *(Real persons whose personal data are obtained through the business relations of the Data Controller within the scope of the operations carried out by the Data Controller's business units, regardless of whether they have any contractual relationship with the Data Controller)*	Identity Communication Legal Action Physical Space Security Customer Transaction Finance Risk Management
Supplier Authority *(Real persons authorized to represent the Data Controller who are bound*	Identity Communication Legal Action Finance

to the Data Controller by a supply contract)	Risk Management Customer Transaction Physical Space Security
Supplier Employee *(Real persons who have an employment contract with the Data Controller who is bound to the Data Controller by a supply contract)*	Identity Communication Physical Space Security Finance
Visitor *(real persons who have entered the physical campuses owned by the Data Controller for various purposes or who visit our websites)*	Identity Communication Physical Space Security
Potential Product or Service Buyer *(Real persons whose personal data are obtained through the business relations of the Data Controller within the scope of the operations carried out by the Data Controller's business units, as a basis for the future legal relationship with the Data Controller)*	Physical Space Security Identity Communication Location Transaction Security Marketing
Parent / Guardian / Representative *(Person(s) authorized to act on behalf of a real or legal entity that has a legal relationship with the Data Controller)*	Identity Communication Legal Action
Intern *(Real persons who are in an intern relationship with the Data Controller)*	Identity Aslam Finance
Employee Candidate *(Real persons who have applied for a job with the Data Controller in any way or who have opened their resume and related information to the Data Controller's review)*	Identity Aslam Legal Action Criminal Conviction and Security Measures Audiovisual Recordings Communication Physical Space Security

Switchboard - Phone Call Call Side *(Other contact groups)*	Identity Communication
Public Officer *(Other groups of persons)*	Identity Communication
Litigation, Enforcement File Party *(Other groups of persons)*	Identity Communication
Doctor *(Other groups of people)*	Identity Professional Experience
Occupational Health and Safety Specialist *(Other groups of persons)*	Identity Communication Professional Experience

6. THIRD PARTIES TO WHOM PERSONAL DATA ARE TRANSFERRED BY THE DATA CONTROLLER AND PURPOSES OF TRANSFER

In accordance with Article 10 of the KVK Law, the Data Controller notifies the personal data owner of the groups of persons to whom personal data is transferred.

In accordance with Articles 8 and 9 of the KVK Law, the Data Controller may transfer the personal data of the data owners governed by the Policy to domestic and foreign recipient groups within the scope of the reasons for transfer on the basis of the data category listed below:

Data Category	Reason for Transfer		Recipient Group	
	Domestic	Abroad	Domestic	Abroad
Identity	Legal Obligation Information Operational Operations	Operational Operations Information	Legal Counsel Authorized Public Institutions and Organizations Natural Persons or Private Law Legal Entities Suppliers Financial Advisor - Accounting Company Attorney, Financial Advisor	Suppliers Natural Persons or Private Law Legal Entities
Audiovisual Recordings	Legal Obligation		Legal Counsel Authorized Public Institutions and Organizations	
Aslam	Legal Obligation		Authorized Public Institutions and Organizations	
Legal Action	Legal		Authorized Public	

	Obligation		Institutions and Organizations	
Communication	Legal Obligation Information Operational Operations	Operational Operations	Authorized Public Institutions and Organizations Natural Persons or Private Law Legal Entities Suppliers Legal Counsel Financial Advisor - Accounting Company Attorney, Financial Advisor	Suppliers
Physical Space Security	Legal Obligation		Authorized Public Institutions and Organizations	
Criminal Conviction and Security Measures	Legal Obligation		Authorized Public Institutions and Organizations	
Finance	Legal Obligation Information Operational Operations		Authorized Public Institutions and Organizations Natural Persons or Private Law Legal Entities Suppliers	
Location	Legal Obligation Operational Operations	Information	Authorized Public Institutions and Organizations Suppliers	Natural Persons or Private Law Legal Entities
Customer Transaction	Legal Obligation		Authorized Public Institutions and Organizations	
Risk Management	Legal Obligation Information		Authorized Public Institutions and Organizations Natural Persons or Private Law Legal Entities	
Vehicle Information	Operational Operations Legal Obligation	Information	Suppliers Authorized Public Institutions and Organizations	Natural Persons or Private Law Legal Entities
Health Information	Legal Obligation		Authorized Public Institutions and Organizations	

Professional Experience	Information Legal Obligation		Natural Persons or Private Law Legal Entities Authorized Public Institutions and Organizations	
Employee Family Member and Relative Information	Legal Obligation		Authorized Public Institutions and Organizations	
Transaction Security	Legal Obligation		Authorized Public Institutions and Organizations	
Marketing	Legal Obligation		Authorized Public Institutions and Organizations	

The definition and scope of the above-mentioned transferred recipient groups are set out in the table below.

Persons to whom data can be transferred	Definition of Persons to Whom Data Can Be Transferred
Authorized Public Institutions and Organizations	Public institutions and organizations authorized to receive information and documents from the Data Controller in accordance with the provisions of the relevant legislation (all ministries, judicial, administrative institutions and organizations affiliated to the Presidency, especially the Ministry of Justice, the Constitutional Court, the Court of Cassation, the Council of State, the Regional Courts of Appeal, Local Courts and other T.C. Courts, each department and degree of the Parliament's departments and institutions, other administrative and financial accident institutions, Governorships, District Governorships, Police Directorates, Consulates of the relevant countries, Population and Citizenship Affairs Directorates, Tax Offices, all central and provincial organizations and units of the Ministry of Finance, Customs Directorates and Chief Directorates, SSI, Undersecretariat of Foreign Trade General Directorate of Free Zones, Free Zones, All Public Banks and in short, all other authorized public institutions and organizations)
Natural Persons or Private Law Legal Entities	In accordance with the provisions of the relevant legislation, private law persons or real persons authorized to receive information and documents from the Data Controller
Suppliers	It defines the parties that provide services to the Data Controller on a contractual basis in accordance with the orders and instructions of the Data Controller while carrying out the commercial activities of the Data Controller

7. PROCESSING OF PERSONAL DATA BASED ON AND LIMITED TO THE PROCESSING CONDITIONS IN THE LAW

The Data Controller enlightens the personal data owner about the personal data it processes in accordance with Article 10 of the KVK Law.

7.1. Processing of Personal Data and Sensitive Personal Data

7.1.1. Processing of Personal Data

The explicit consent of the personal data owner is only one of the legal bases that make it possible to process personal data in accordance with the law. Apart from explicit consent, personal data may also be processed in the presence of one of the other conditions written below. The basis of the personal data processing activity may be only one of the conditions stated below, or more than one of these conditions may be the basis of the same personal data processing activity. If the processed data is sensitive personal data; The terms set out in heading 7.1.2 under this section below apply.

Although the legal bases for the processing of personal data by the Data Controller differ, all kinds of personal data processing activities are carried out in accordance with the general principles specified in Article 4 of the KVK Law.

7.1.1.1. Explicit Consent of the Personal Data Owner

One of the conditions for processing personal data is the explicit consent of the owner. The explicit consent of the personal data owner should be disclosed on a specific subject, based on information and with free will.

At least one of the conditions in 7.1.1.2 - 7.1.1.8 of this title is sought for personal data processing activities other than the purpose of processing (primary processing) for the reasons for obtaining personal data (secondary processing); If one of these conditions does not exist, these personal data processing activities are carried out by the Data Controller based on the explicit consent of the personal data owner for these processing activities.

In order for personal data to be processed subject to the explicit consent of the personal data owner, the explicit consent of the personal data owners is obtained by the relevant methods.

7.1.1.2. Explicitly Stipulated in the Laws

The personal data of the data owner may be processed in accordance with the law if it is expressly stipulated in the law.

7.1.1.3. Failure to Obtain the Explicit Consent of the Person Concerned Due to Actual Impossibility

The personal data of the data owner may be processed if it is necessary to process the personal data of the person who is unable to disclose his consent due to actual impossibility or whose consent cannot be validated in order to protect the life or physical integrity of himself or another person.

7.1.1.4. Being Directly Related to the Establishment or Performance of the Contract

Provided that it is directly related to the establishment or performance of a contract, it is possible to process personal data if it is necessary to process personal data belonging to the parties to the contract.

7.1.1.5. Fulfillment of the Legal Obligation of the Data Controller

If the processing is mandatory for the Data Controller to fulfill its legal obligations as a data controller, the personal data of the data owner may be processed.

7.1.1.6. Publicization of Personal Data by the Personal Data Owner

If the personal data of the data owner has been made public by him/her, the relevant personal data may be processed.

7.1.1.7. Data Processing is Mandatory for the Establishment or Protection of a Right

If data processing is mandatory for the establishment, exercise or protection of a right, the personal data of the personal data owner may be processed.

7.1.1.8. Data Processing is Mandatory for the Legitimate Interest of the Data Controller

Provided that it does not harm the fundamental rights and freedoms of the personal data owner, data data may be processed if it is necessary to process data for the legitimate interests of the Data Controller.

7.1.2. Processing of Sensitive Personal Data

By the Data Controller; If there is no explicit consent of the personal data owner, sensitive personal data is processed in the following cases, provided that adequate measures to be determined by the KVK Board are taken:

- Sensitive personal data other than the health and sexual life of the personal data owner, in cases stipulated by law,

- Sensitive personal data related to the health and sexual life of the personal data owner can only be processed by persons or authorized institutions and organizations under the obligation of confidentiality for the purpose of protecting public health, conducting preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing.

7.2. Personal Data Processing Activities Carried Out in the Building, Facility Entrances and Building Facility

Personal data processing activities carried out by the Data Controller at the entrances of the building facilities and within the facility are carried out in accordance with the Constitution, the KVK Law and other relevant legislation.

In order to ensure security by the Data Controller, personal data processing activities are carried out for the monitoring of guest entries and exits with security cameras in the buildings and facilities of the Data Controller.

Personal data processing activities are carried out by the Data Controller through the use of security cameras and recording of guest entrances and exits.

Cameras are divided into indoor and outdoor cameras. Indoor cameras; Except for sinks, rooms, changing cabins, and interior rooms, they are positioned at an angle that will not attract our direct employees or visitors. The locations of the cameras have been carefully

determined so that the monitoring activity can be maintained at a minimum and limited for the purpose of monitoring

7.2.1. Camera Monitoring Activity Carried Out at and Inside the Data Controller Building, Facility Entrances

In this section, explanations will be made about the camera monitoring system of the Data Controller and information will be provided on how personal data, privacy and fundamental rights of the person are protected.

Data Controller, within the scope of security camera monitoring activity; It has purposes such as protecting the interests of the Data Controller and other persons regarding the security of the Data Controller.

7.2.2. Conducting Security Camera Monitoring Activities According to KVK Law

The Data Controller acts in accordance with the regulations in the KVK Law in carrying out camera monitoring activities for security purposes. In order to ensure security in its buildings and facilities, the Data Controller carries out security camera monitoring activities for the purposes stipulated in the relevant legislation in force and in accordance with the personal data processing conditions listed in the KVK Law.

7.2.3. Announcement of Camera Surveillance Activity

10 of the KVK Law by the Data Controller. In accordance with the article, the personal data owner is enlightened. The Data Controller notifies by more than one method regarding the camera monitoring activity of the illumination it has made regarding general issues. Thus, it is aimed to prevent damage to the fundamental rights and freedoms of the personal data owner, to ensure transparency and to enlighten the personal data owner.

For camera monitoring by the Data Controller; This Policy is published on the website of the Data Controller (online policy regulation) and a notification letter stating that monitoring will be carried out is posted at the entrances of the areas where monitoring is carried out (on-site lighting).

7.2.4. Purpose of Execution of Camera Monitoring Activity and Limitation to Purpose

In accordance with Article 4 of the KVK Law, the Data Controller processes personal data in a limited and measured manner in connection with the purpose for which they are processed.

The purpose of maintaining the video camera monitoring activity by the Data Controller is limited to the purposes listed in this Policy. Accordingly, the monitoring areas of security cameras, the number and when they will be monitored are put into practice in a way that is sufficient to achieve the security purpose and limited to this purpose. It is not subject to monitoring in areas (e.g., toilets) that may result in interference with the privacy of the person in a way that exceeds security purposes.

7.2.5. Ensuring the Security of the Data Obtained

In accordance with Article 12 of the KVK Law, necessary technical and administrative measures are taken by the Data Controller to ensure the security of personal data obtained as a result of camera surveillance.

7.2.6. Retention Period of Personal Data Obtained by Camera Monitoring Activity

Detailed information about the retention period of the Data Controller for personal data obtained through camera surveillance is included in Article 4.3 of this Policy titled Personal Data Storage Periods.

If it is understood that the video recordings obtained from the security camera constitute evidence for the criminal investigation before the deletion period, if they constitute evidence for the criminal investigation, they are kept until they are submitted to the judicial authority.

Video recordings obtained from the security camera are kept for 10 years if it is understood that they constitute evidence of a legal dispute before the deletion period.

7.2.7. Who Has Access to the Information Obtained as a Result of Monitoring and To Whom This Information Is Transferred

Only a limited number of Data Controller employees have access to live camera images and records recorded and stored in digital environment. A limited number of people who have access to the records declare that they will protect the confidentiality of the data they access with a confidentiality commitment.

8. CONDITIONS FOR DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Although the Data Controller has been processed in accordance with the provisions of the relevant law as regulated in Article 138 of the Turkish Penal Code and Article 7 of the KVK Law, personal data is deleted, destroyed or anonymized upon the Data Controller's own decision or upon the request of the personal data owner, in the event that the reasons requiring its processing disappear.

In this context:

- Termination or invalidity of the contract based on processing,
- Withdrawal of consent in processing activities based on explicit consent,
- The Data Owner's application for deletion-destruction-anonymization and acceptance of this application,
- The decision that the request to be made by the Personal Data Protection Board as a result of the application of the Data Owner and the rejection of this application must be met,
- Expiration of the storage period,
- Periodic destruction operations carried out within the Data Controller,

As a result, the Data Controller deletes, destroys or anonymizes the Personal Data it has collected.

In terms of Deletion, Destruction or Anonymization of Personal Data, the Data Controller establishes a separate policy in detail within the scope of the Regulation on the Deletion, Destruction or Anonymization of Personal Data.

9. RIGHTS OF PERSONAL DATA OWNERS; METHODOLOGY OF THE USE AND EVALUATION OF THESE RIGHTS

9.1. Rights of the Data Owner and Exercise of These Rights

9.1.1. Rights of the Personal Data Owner

Personal data owners have the following rights:

- To learn whether personal data is processed or not
- If personal data has been processed, requesting information about it,
- To learn the purpose of processing personal data and whether they are used in accordance with their purpose,
- To know the third parties to whom personal data is transferred in the country or abroad,
- Requesting correction of personal data in case of incomplete or incorrect processing and requesting notification of the transaction made within this scope to third parties to whom personal data has been transferred,
- Although it has been processed in accordance with the provisions of the KVK Law and other relevant laws, to request the deletion or destruction of personal data in the event that the reasons requiring its processing disappear, and to request the notification of the transaction made within this scope to the third parties to whom the personal data has been transferred,
- Objecting to the occurrence of a result against the person himself by analyzing the processed data exclusively through automated systems,
- Requesting the compensation of the damage in case of damage due to unlawful processing of personal data.

9.1.2. Situations in which the Personal Data Owner cannot assert his rights

Pursuant to Article 28 of the KVK Law, personal data owners cannot assert the rights listed in 9.1.1. on these issues, as the following situations are excluded from the scope of the KVK Law:

- Processing of personal data for purposes such as research, planning and statistics by anonymizing them with official statistics.
- Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that it does not violate national defense, national security, public security, public order, economic security, privacy of private life or personal rights or does not constitute a crime.
- Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.

- Processing of personal data by judicial authorities or enforcement authorities in relation to investigation, prosecution, trial or execution proceedings.

Pursuant to Article 28/2 of the KVK Law; In the following cases, personal data owners cannot assert their other rights listed in 9.1.1., except for the right to demand compensation for the damage:

- The processing of personal data is necessary for the prevention of crime or for criminal investigation.

- Processing of personal data made public by the personal data owner.

- The processing of personal data is necessary for the execution of supervisory or regulatory duties and 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 the law.

- The processing of personal data is necessary for the protection of the economic and financial interests of the State in relation to budget, tax and financial issues.

9.1.3. Exercising the Rights of the Personal Data Owner

Personal Data Owners are required to submit to Article 9.1.1 of this section. They will be able to submit their requests regarding their rights listed under the heading to the Data Controller free of charge by filling out and signing the Application Form with information and documents that will identify their identities and by the following methods or other methods determined by the Personal Data Protection Board:

Complaint form is available at www.bmsgeridonusum.com.tr or at the address of KEMALPAŞA CADDESI NO: 289 IŞIKKENT BORNOVA/İZMİR. After filling out the form, which you can obtain from the address of the Data Controller, you can send a wet signed copy to the same address of the Data Controller personally or through a notary public.

In order for third parties to request an application on behalf of personal data owners, there must be a special power of attorney issued by the data owner through a notary public on behalf of the person who will apply.

9.1.4. The Right of the Personal Data Owner to File a Complaint with the KVK Board

In cases where the application is rejected in accordance with Article 14 of the KVK Law, the answer given is insufficient or the application is not answered in due time; It can file a complaint with the KVK Board within thirty days from the date of learning the response of the Data Controller and in any case within sixty days from the date of application.

9.2. Data Controller's Response to Applications

9.2.1. Procedure and Time of the Data Controller to Respond to Applications

In the event that the personal data owner submits his/her request to the Data Controller in accordance with the procedure set forth in section 9.1.3 of this section, the Data Controller will conclude the relevant request free of charge within thirty days at the latest, depending on the nature of the request. However, if a fee is stipulated by the KVK Board, the fee in the

tariff determined by the KVK Board will be collected from the applicant by the Data Controller.

9.2.2. Information that the Data Controller may request from the personal data owner who applied

The Data Controller may request information from the relevant person in order to determine whether the applicant is the owner of personal data. In order to clarify the issues in the application of the personal data owner, the Data Controller may ask the personal data owner about his application.

9.2.3 Data Controller's Right to Reject the Personal Data Subject's Application

The Data Controller may reject the application of the applicant by explaining the reason in the following cases:

- Processing of personal data for purposes such as research, planning and statistics by anonymizing them with official statistics.
- Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that it does not violate national defense, national security, public security, public order, economic security, privacy of private life or personal rights or does not constitute a crime.
- Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.
- Processing of personal data by judicial authorities or enforcement authorities in relation to investigation, prosecution, trial or execution proceedings.
- The processing of personal data is necessary for the prevention of crime or for criminal investigation.
- Processing of personal data made public by the personal data owner.
- The processing of personal data is necessary for the execution of supervisory or regulatory duties and 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 the law.
- The processing of personal data is necessary for the protection of the economic and financial interests of the State in relation to budget, tax and financial issues.
- The request of the personal data owner is likely to prevent the rights and freedoms of other persons
- Requests have been made that require disproportionate effort.
- The requested information is public information.

10. THE RELATIONSHIP OF THE DATA CONTROLLER PERSONAL DATA PROTECTION AND PROCESSING POLICY WITH OTHER POLICIES

The Data Controller may also create sub-policies for internal use regarding the protection and processing of personal data to which the principles set forth by this Policy are related, as well as other policies for certain groups of persons, especially employees.

The principles of the Data Controller's sub-policies for internal use are reflected in publicly available policies to the extent relevant, and it is aimed to inform those concerned within this framework and to ensure transparency and accountability regarding the personal data processing activities carried out by the Data Controller.Thank you for reviewing our KVKK Policy.

BMS GERİ DÖNÜŞÜM SANAYİ VE TİCARET ANONİM ŞİRKETİ

KEMALPASA CADDESI NO:289 ISIKKENT BORNOVA/IZMIR

0232 479 55 62

bms@bmsgeridonusum.com

https://www.bmsgeridonusum.com.tr/