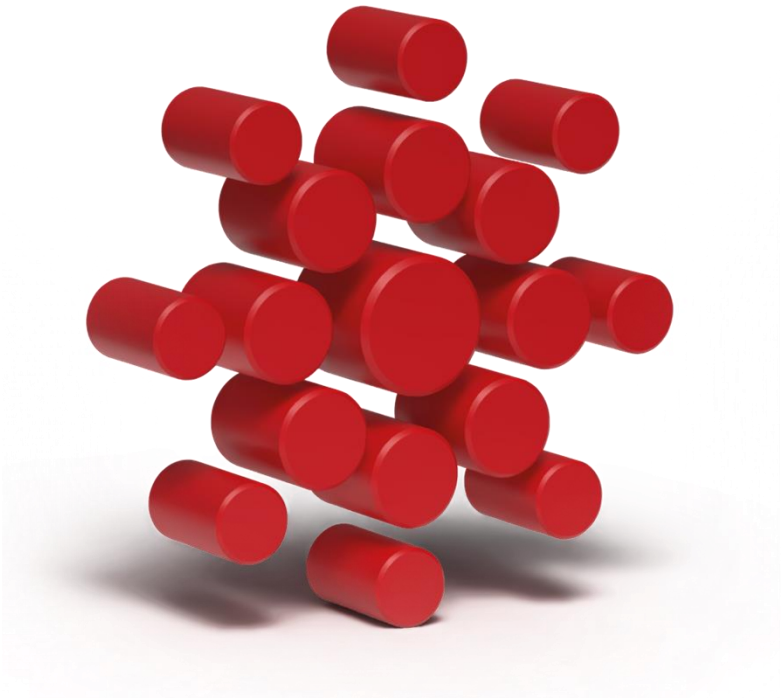

PERSONAL DATA PROTECTION POLICY

11.2020

TABLE OF CONTENTS

Introduction

1.1. Introduction

The protection of personal data is of great importance to our company and is one of our priorities. The most crucial aspect of this matter is the protection of personal data belonging to our job applicants, company shareholders, company executives, visitors, employees of institutions we collaborate with, customers, shareholders, and executives, and third parties. Activities related to the protection of our employees' personal data are conducted in parallel with the principles outlined in this Policy.

According to the Constitution of the Republic of Turkey, everyone has the right to request the protection of their personal data. In accordance with this constitutional right, our company demonstrates the necessary care regarding the protection of personal data through this Policy and makes it a part of its corporate policy.

In this context, administrative and technical measures are taken by our company to ensure the protection of personal data processed in accordance with the relevant legislation. This Policy will provide detailed explanations regarding the fundamental principles adopted by our company in the processing of personal data, as outlined below:

- Processing personal data in accordance with the law and honesty principles,
- Keeping personal data accurate and up-to-date when necessary,
- Processing personal data for specific, explicit, and legitimate purposes,
- Processing personal data in a manner that is relevant, limited, and proportionate to the purpose for which it is processed,
- Storing personal data for the period required by the relevant legislation or the purpose for which it was processed,
- Informing and enlightening data subjects,
- Establishing a system to allow data subjects to exercise their rights,
- Taking necessary measures for the protection of personal data,
- Ensuring that the transfer of personal data to third parties complies with the relevant legislation and KVK Board regulations,
- Demonstrating necessary care in processing and protecting special categories of personal data.

1.2. Purpose of the Policy

The primary purpose of this policy is to provide explanations regarding personal data processing activities carried out by our company in a lawful manner and the systems adopted for the protection of personal data. It aims to inform individuals whose personal data is processed by our company, including job applicants, shareholders, executives, visitors, employees of institutions we collaborate with, customers, and third parties, and to ensure transparency in the data processing process.

1.3. Scope

This Policy applies to all personal data processed either automatically or through non-automatic means that form part of a data filing system.

The scope of this Policy may cover the entire policy for the categories of personal data subjects mentioned above (e.g., job applicants who are also visitors) or may apply only to certain provisions (e.g., only visitors).

1.4. Application of the Policy and Relevant Legislation

In the matter of processing and protecting personal data, the applicable legal regulations will take precedence. If there is any inconsistency between the applicable legislation and this Policy, our company accepts that the applicable legislation will prevail.

This Policy has been created by detailing the rules set forth by the relevant legislation within the scope of our company's practices. Our company ensures that it complies with the deadlines set forth in the Personal Data Protection Law (KVKK) and takes the necessary steps accordingly.

1.5. Effectiveness of the Policy

Our Policy, which was established and entered into force on January 1, 2018, is published on our website and is made available to data subjects upon request.

2. PERSONAL DATA PROTECTION ISSUES

2.1. Ensuring the Security of Personal Data

2.1.1. Technical and Administrative Measures Taken to Ensure the Lawful Processing of Personal Data

To ensure the lawful processing of personal data, technical and administrative measures are taken according to technological capabilities and implementation costs.

Technical Measures Taken to Ensure the Lawful Processing of Personal Data:
The main technical measures taken to ensure the lawful processing of personal data are as follows:

- Personal data processing activities carried out within our company are monitored within the framework of internationally recognized standards through the established technical systems.
- The technical measures taken are periodically reported to the relevant authorities, as required by the ISO 27001 internal audit mechanism.
- Personnel with expertise in technical matters are employed.

Administrative Measures Taken to Ensure the Lawful Processing of Personal Data:
The main administrative measures taken to ensure the lawful processing of personal data are as follows:

- Employees are informed and trained on the protection of personal data and the lawful processing of personal data.
- All activities carried out by our company are analyzed in detail across all departments. Based on these analyses, personal data processing activities specific to the business operations of each department are identified.
- Personal data processing activities carried out by our departments are assessed to ensure compliance with the Personal Data Protection Law (GDPR), and the required actions for each department are determined.
- To ensure compliance with legal requirements for personal data processing, awareness is raised within each department, and implementation rules are set. Administrative measures are implemented through internal policies and training to ensure ongoing compliance and monitoring.
- In the agreements and documents managing the legal relationship between our company and employees, records are included that impose the obligation not to process, disclose, or use personal data, except for the instructions of the company or legal exceptions. Employee awareness is created on this matter, and audits are conducted.

2.1.2. Technical and Administrative Measures Taken to Prevent Unlawful Access to Personal Data

To prevent the unauthorized disclosure, access, transfer, or any other form of unlawful access to personal data, technical and administrative measures are taken based on the nature of the data, technological capabilities, and implementation costs.

Technical Measures Taken to Prevent Unlawful Access to Personal Data:
The main technical measures taken by our company to prevent unlawful access to personal data are as follows:

- Technical measures are taken in accordance with technological advancements, and these measures are updated and renewed regularly.
- Access permissions are restricted, and these permissions are regularly reviewed.
- Technical measures are periodically reported to the relevant authorities as part of the ISO 27001 internal audit mechanism, and any risk factors are reassessed to develop necessary technological solutions.
- Antivirus systems and security firewall software and hardware are installed.
- Personnel with expertise in technical matters are employed.

Administrative Measures Taken to Prevent Unlawful Access to Personal Data:
The main administrative measures taken by our company to prevent unlawful access to personal data are as follows:

- Employees are trained on technical measures to prevent unlawful access to personal data.
- Access and authorization processes for personal data are designed and implemented within each department in accordance with legal compliance requirements for personal data processing.
- Employees are informed that they cannot disclose personal data they learn to others or use it for purposes

other than processing, and that this obligation continues even after they leave their positions. Necessary commitments are obtained from employees in this regard.
- In contracts with third parties to whom personal data is lawfully transferred, provisions are included to ensure that the third parties take the necessary security measures for the protection of personal data and enforce these measures within their organizations.

2.1.3. Storing Personal Data in Secure Environments
Our company takes the necessary technical and administrative measures to ensure that personal data is stored in secure environments and to prevent its unlawful destruction, loss, or alteration.

Technical Measures Taken to Store Personal Data in Secure Environments:
The main technical measures taken by our company to store personal data in secure environments are as follows:

- Technological systems in line with technological developments are used to store personal data securely.
- Expert personnel are employed in technical matters, and external support is obtained if necessary.
- Technical security systems are installed in storage areas, and the technical measures are periodically reported to the relevant authorities as part of the internal audit mechanism. Any risk factors are reassessed, and necessary technological solutions are developed.
- Backup programs are used to securely store personal data in a lawful manner.
- Access to data storage areas is logged, and inappropriate access or access attempts are promptly reported to the relevant authorities.

Administrative Measures Taken to Store Personal Data in Secure Environments:
The main administrative measures taken by our company to store personal data in secure environments are as follows:
- Employees are trained to ensure the secure storage of personal data.
- If an external service is procured for the storage of personal data due to technical requirements, contracts with the relevant companies are signed, including provisions stating that these companies will take necessary security measures for the protection of personal data and ensure the enforcement of these measures within their organizations.

2.1.4. Monitoring the Measures Taken to Protect Personal Data
In accordance with Article 12 of the Personal Data Protection Law, our company conducts internal audits and/or commissions third-party audits. The results of these audits are reported to the relevant department within the company's internal processes, and actions are taken to improve the measures based on the findings.

2.1.5. Measures Taken in the Event of Unauthorized Disclosure of Personal Data
In compliance with Article 12 of the Personal Data Protection Law, our company operates a system to notify the relevant data subject and the Personal Data Protection Board as soon as possible in the event of personal data being unlawfully obtained by unauthorized persons.
If deemed necessary by the Personal Data Protection Board, this situation may be published on the Board's website or through other methods.

2.2. Safeguarding the Rights of Data Subjects; Creating Channels for Data Subjects to Submit Their Requests and Evaluating Their Requests
Our company implements the necessary channels, internal processes, and technical and administrative regulations in compliance with Article 13 of the Personal Data Protection Law to evaluate the rights of data subjects and provide the required information to them.
Data subjects can submit written requests regarding the following rights to our company. Our company will respond to the request within thirty days free of charge, depending on the nature of the request. However, if a fee is determined by the Personal Data Protection Board, our company will charge the fee according to the tariff specified by the Board. Data subjects have the right to:

- Learn whether their personal data is processed,
- Request information about personal data processed,
- Learn the purpose of processing personal data and whether it is used in accordance with its purpose,
- Know the third parties to whom their personal data is transferred,

- Request the correction of personal data if it is incomplete or inaccurate and have the correction communicated to third parties,
- Request the deletion or destruction of personal data when the reasons for processing no longer exist, and have the deletion or destruction communicated to third parties,
- Object to the processing of personal data by exclusively automated means, which results in a consequence detrimental to the individual,
- Request compensation for damages arising from the unlawful processing of personal data.

Further detailed information regarding the rights of data subjects is provided in Section 10 of this policy.

2.3. Protection of Special Categories of Personal Data
Special categories of personal data are given particular importance under the Personal Data Protection Law due to the risk of causing harm or discrimination if processed unlawfully. These include data regarding race, ethnicity, political opinions, philosophical beliefs, religion, sect, or other beliefs, membership in associations, foundations, or trade unions, health, sexual life, criminal convictions, and security measures, as well as biometric and genetic data. Our company handles personal data classified as "special categories" by the Personal Data Protection Law with extra care. In this regard, the technical and administrative measures taken for the protection of personal data are strictly applied to special categories of personal data, and necessary audits are carried out. Further information regarding the processing of special categories of personal data is provided in Section 3 of this policy.

2.4. Raising Awareness and Monitoring the Protection and Processing of Personal Data Among Business Units
Our company ensures that awareness is raised regarding the unlawful processing, unauthorized access, and safe storage of personal data by providing necessary training to business units.
Awareness of the protection of personal data is raised through orientation training for current and newly hired employees, and when necessary, professional consultants are employed to assist in the process.
Top management evaluates participation in training, seminars, and informational sessions and conducts necessary audits. Our company updates and renews its training in accordance with any updates to relevant regulations.

2.5. Raising Awareness and Monitoring the Protection and Processing of Personal Data Among Business Partners and Suppliers
Our company raises awareness about preventing unlawful processing and access to personal data, as well as ensuring its safe storage, by including relevant clauses in contracts with business partners and suppliers regarding the Personal Data Protection Law (GDPR). The company also indicates that it may conduct audits if deemed necessary.

3. Key Principles of Personal Data Processing

3.1. Processing of Personal Data in Compliance with Legal Principles

3.1.1. Processing in Accordance with the Law and Principles of Fairness
Our company ensures that personal data is processed in accordance with the legal principles set out by relevant regulations and the general principle of trust and fairness. In this regard, our company takes into consideration the proportionality requirements in the processing of personal data and does not use personal data for purposes beyond what is required for the intended purpose.

3.1.2. Ensuring the Accuracy and Timeliness of Personal Data
Our company ensures that the personal data processed is accurate and up-to-date, taking into account the fundamental rights of the data subjects and its legitimate interests. To achieve this, necessary measures are taken. For instance, our company has implemented a system that allows data subjects to correct and verify the accuracy of their personal data. Detailed information on this topic is provided in Section 10 of this policy.

3.1.3. Processing for Specific, Clear, and Legitimate Purposes
Our company clearly defines the legitimate and lawful purpose of processing personal data. We only process personal data to the extent necessary for the commercial activities we undertake and the objectives associated with them.

3.1.4. Processing in a Relevant, Limited, and Proportionate Manner
Our company processes personal data in a manner that is suitable for achieving the specified purposes and avoids processing personal data that is not related to or necessary for the achievement of these purposes. For example, we do not engage in personal data processing activities aimed at meeting potential future needs.

3.1.5. Retention of Personal Data for the Duration Required by Relevant Legislation or for the Purpose of Processing
Our company retains personal data only for the duration specified in the relevant legislation or for as long as necessary to fulfill the purpose for which it was processed. In this context, our company first determines whether the relevant legislation specifies a retention period for personal data. If a retention period is specified, we comply with it; if no retention period is specified, personal data is kept only for as long as necessary for the purpose of processing. Our company does not retain personal data for potential future use. Detailed information on this topic is provided in Section 9 of this policy.

3.2. Processing Personal Data Based on One or More of the Personal Data Processing Conditions Specified in Article 5 of the GDPR
The protection of personal data is a constitutional right. Fundamental rights and freedoms can only be restricted, without affecting their essence, for reasons specified in the relevant articles of the Constitution, and only by law. According to the third paragraph of Article 20 of the Constitution, personal data can only be processed in cases specified by law or with the explicit consent of the individual. In line with this, and in accordance with the Constitution, our company processes personal data only in cases specified by law or with the explicit consent of the data subject. Detailed information on this topic is provided in Section 7 of this policy.

3.3. Informing and Notifying the Data Subject
In accordance with Article 10 of the KVK Law, our company informs data subjects during the collection of their personal data. Detailed information on this topic is provided in Section 10 of this policy.
International agreements and Article 20 of the Constitution guarantee the right of every individual to be informed about their personal data. In this regard, Article 11 of the GDPR includes the right of the data subject to request information. In compliance with Article 20 of the Constitution and Article 11 of the GDPR, our company provides the necessary information to the data subject if they request it. Detailed information on this topic is provided in Section 10 of this policy.

3.4. Processing of Special Categories of Personal Data
Our company carefully adheres to the provisions outlined in the GDPR regarding the processing of personal data categorized as "special categories of personal data."
Article 6 of the GDPR identifies certain types of personal data as "special categories of personal data" due to the risk of causing harm or discrimination if processed unlawfully. These include data related to race, ethnicity, political opinion, philosophical belief, religion, sect, or other beliefs, dress, membership in associations, foundations, or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.
In accordance with the GDPR, our company processes special categories of personal data only in the following cases, with sufficient measures determined by the KVK Board:

- If the data subject's explicit consent is obtained, or
- If the data subject’s explicit consent is not obtained:
    - Special categories of personal data, other than health and sexual life, can be processed in cases specified by law.
    - Special categories of personal data concerning the data subject's health and sexual life may only be processed for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment, and care services, planning, and management of healthcare services and financing, by persons or institutions under an obligation of confidentiality.

3.5. Transfer of Personal and Special Categories of Personal Data
In accordance with the lawful purposes of processing personal data, and by taking necessary security measures (see Section 2/Title 2.1), our company may transfer the personal data and special categories of personal data of data subjects to third parties. Our company acts in compliance with the provisions set forth in Article 8 of the

GDPR. Detailed information on this topic is provided in Section 6 of this policy.

3.5.1. Transfer of Personal Data

Our company may transfer personal data to third parties in a lawful and legitimate manner, based on one or more of the conditions specified in Article 5 of the GDPR, as outlined below:

- If the data subject's explicit consent is obtained,
- If there is an explicit legal provision regarding the transfer of personal data,
- If it is necessary to protect the life or physical integrity of the data subject or another person and the data subject is unable to give consent due to practical impossibility or if their consent is not legally valid,
- If the transfer of personal data is necessary for the establishment or performance of a contract directly related to the parties of the contract,
- If the transfer of personal data is required for the company to fulfill its legal obligations,
- If the personal data has been made public by the data subject,
- If the transfer of personal data is necessary for the establishment, exercise, or protection of a legal right,
- If the transfer of personal data is necessary for the legitimate interests of the company, provided it does not harm the fundamental rights and freedoms of the data subject.

3.5.2. Transfer of Special Categories of Personal Data

Our company, with due diligence and necessary security measures in place (see Section 2/Title 2.1), and in compliance with the sufficient measures determined by the KVK Board, may transfer the data subject's special categories of personal data to third parties in the following cases:

- If the data subject's explicit consent is obtained, or
- If the data subject's explicit consent is not obtained:
    - Special categories of personal data (such as race, ethnicity, political opinion, philosophical belief, religion, sect, or other beliefs, clothing, membership in associations, foundations, or unions, criminal convictions, security measures, and biometric and genetic data), excluding health and sexual life, may be transferred in cases specified by law.
    - Special categories of personal data regarding the health and sexual life of the data subject may only be transferred by persons or institutions under an obligation of confidentiality for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment, and care services, health services, and the planning and management of their financing.

3.6. Transfer of Personal and Special Categories of Personal Data Abroad

Our company may transfer personal data and special categories of personal data to third parties abroad, in a lawful manner, and by taking necessary security measures (see Section 2/Title 2.1).
Our company may transfer personal data to foreign countries that are declared by the KVK Board to provide adequate protection ("Foreign Countries with Adequate Protection") or, in cases where adequate protection is not available, to foreign countries where both the data controllers in Turkey and the relevant foreign country's data controllers have committed to provide adequate protection and have obtained the KVK Board's approval ("Foreign Countries with Adequate Protection Committed by Data Controllers"). Our company acts in compliance with the provisions set forth in Article 9 of the GDPR. Detailed information on this subject is provided in Section 6 of this policy.

3.6.1. Transfer of Personal Data Abroad

Our company may transfer personal data to countries with adequate protection or to foreign countries where data controllers have committed to provide adequate protection, in accordance with the lawful purposes of personal data processing, if one of the following conditions exists:

- If there is an explicit legal provision regarding the transfer of personal data,
- If the transfer is necessary to protect the life or physical integrity of the data subject or another person and the data subject is unable to give consent due to practical impossibility or if their consent is not legally valid,
- If the transfer of personal data is necessary for the establishment or performance of a contract directly related to the parties of the contract,

- If the transfer of personal data is required for the company to fulfill its legal obligations,
- If the personal data has been made public by the data subject,
- If the transfer of personal data is necessary for the establishment, exercise, or protection of a legal right,
- If the transfer of personal data is necessary for the legitimate interests of the company, provided it does not harm the fundamental rights and freedoms of the data subject.

3.6.2. Transfer of Special Categories of Personal Data Abroad

Our company, with due diligence and necessary security measures in place (see Section 2/Title 2.1), and in compliance with the sufficient measures determined by the KVK Board, may transfer the data subject's special categories of personal data to foreign countries with adequate protection or to foreign countries where data controllers have committed to provide adequate protection, under the following conditions:

- If the data subject's explicit consent is obtained, or
- If the data subject's explicit consent is not obtained:
    - Special categories of personal data (excluding health and sexual life) may be transferred in cases specified by law,
    - Special categories of personal data regarding the health and sexual life of the data subject may only be transferred for purposes such as public health protection, preventive medicine, medical diagnosis, treatment, and care services, and health services planning and management, by persons or institutions under an obligation of confidentiality.

4. PERSONAL DATA CATEGORIZATION, PROCESSING PURPOSES, AND RETENTION PERIODS PROCESSED BY OUR COMPANY

4.1. Categorization of Personal Data

In our company, personal data is processed based on one or more of the personal data processing conditions specified in Article 5 of the GDPR, within the framework of legitimate and lawful purposes. These data are processed in accordance with the principles outlined in Article 4 of the GDPR, and the general principles specified in the GDPR, as well as all obligations regulated by the GDPR.

The processing of personal data, as outlined in this policy, involves limited processing of the following categories, as defined in the **VERBIS** registry. The data subjects related to the personal data processed in these categories are specified in Section 5 of this policy.

CATEGORIZATION OF PERSONAL DATA

Personal Data Category	Description of Personal Data Category
Identity Information	Data that identifies a specific or identifiable individual, processed either automatically or manually as part of a data recording system. It includes information such as first name, last name, Turkish ID number, nationality, mother's name, father's name, place and date of birth, gender, and documents like driver's license, identity card, passport, tax number, social security number, signature, vehicle license plate, etc.
Contact Information	Data related to contact details, which identifies a specific or identifiable individual, processed either automatically or manually. This includes phone numbers, addresses, email addresses, fax numbers, and IP addresses.
Location Data	Data that identifies a specific or identifiable individual, processed either automatically or manually. It includes information related to the location of the data subject, such as GPS location, travel data, etc., collected during operations or product and service use within the company or by cooperating institutions.
Family Members and Relatives Information	Data about the family members (e.g., spouse, parents, children) or other close persons and emergency contacts, processed either automatically or manually, related to the protection of legal or other interests of the company and the data subject, in relation to the company's products and services.
Physical Space Security Information	Data collected in physical spaces (e.g., camera recordings, fingerprint records, security access records), which identify a specific or identifiable individual. These are processed for security purposes during entry, exit, or while present within the premises.
Financial Information	Data that identifies a specific or identifiable individual, processed either automatically or

Personal Data Category	Description of Personal Data Category
	manually. This category includes information such as bank account number, IBAN number, credit card details, financial profiles, assets, income information, and other financial data related to the legal relationship established with the data subject.
Visual/Audio Information	Data that identifies a specific or identifiable individual, processed either automatically or manually, including photographs, video recordings (other than security footage), voice recordings, or copies of documents containing personal data.
Employment Information	Data relating to the employment relationship between the company and an individual. This includes information that supports the creation of employment rights for the data subject, processed either automatically or manually, such as work-related details and records.
Special Categories of Personal Data	Personal data that includes sensitive information about a specific or identifiable individual, processed either automatically or manually. This includes data specified in Article 6 of the GDPR (e.g., health information, blood type, biometric data, religious affiliation, and membership in associations).
Request/Complaint Management Information	Data related to any request or complaint directed to the company. This includes personal data processed to receive and assess any demands or complaints from the data subject.

4.2. Purposes of Personal Data Processing

Our company processes personal data in accordance with the conditions and purposes specified in the GDPR, and strictly within the scope of these purposes and conditions. These purposes and conditions include:

- Processing personal data when it is explicitly required by laws for the company's activities.
- Processing personal data when necessary for the establishment or performance of a contract directly related to the data subject.
- Processing personal data when necessary for the company to fulfill its legal obligations.
- Processing personal data when it has been made public by the data subject, limited to the purpose for which it was made public.
- Processing personal data when necessary for the establishment, use, or protection of the rights of the company, the data subject, or third parties.
- Processing personal data when it is necessary for the legitimate interests of the company, provided that it does not harm the fundamental rights and freedoms of the data subject.
- Processing personal data when it is necessary for the protection of life or physical integrity of the data subject or another person, and the data subject is unable to give explicit consent due to factual or legal invalidity.
- Processing personal data related to the health and sexual life of the data subject in accordance with the law for public health protection, preventive medicine, medical diagnosis, treatment and care services, planning, and management of health services and financing, by persons or authorized institutions who are under an obligation of confidentiality.

Based on these conditions, our company processes your personal data for the following purposes:

- Defining and implementing the company's strategies and ensuring the execution of human resources policies.
- Ensuring human resource policies are followed, including recruitment for open positions, conducting HR operations in compliance with company policies, and ensuring compliance with Occupational Health and Safety regulations.
- Performing services related to independent audits, accounting, consulting, and other services provided by our company.
- Ensuring legal and commercial security for the company and individuals with whom the company has a business relationship, including administrative operations related to communication, auditor independence, risk management, and quality control.
- Managing relationship, account, internal financial reporting, and providing IT services (including storage, hosting, maintenance, support, and the use of centralized distributed server systems).
- Implementing commercial and business strategies, including financial operations, communication, market research, social responsibility activities, and procurement processes (request, offer, evaluation, order, budgeting, contracts).
- Managing company internal systems, applications, and implementation of commercial strategies.

- Planning, auditing, and implementing information security processes, and managing IT infrastructure.
- Planning and executing employee satisfaction and/or loyalty processes, benefits and rights planning, access control to information, tracking and/or monitoring employee activities.
- Following up on finance, accounting, and legal matters.
- Planning and executing market research and promotional activities for the sale and marketing of business services.
- Planning and implementing access control for partners and/or suppliers, managing relationships with business partners and suppliers.
- Planning and executing corporate communication activities, corporate risk management, sustainability, and corporate governance processes.
- Managing customer relationship management (CRM) processes, customer satisfaction, and handling customer demands and complaints.
- Fulfilling obligations arising from employment contracts and legal regulations for employees.
- Ensuring the security of company assets and resources.
- Organizing and executing external training activities.
- Planning and executing operational activities to ensure the company's operations comply with company procedures and relevant legislation.
- Ensuring the accuracy and updating of data.
- Planning and executing talent and career development activities.
- Providing information to authorized individuals or institutions as required by law.
- Maintaining visitor logs and ensuring the security of company premises and facilities.

The purposes of data processing are further detailed in the VERBIS registry.
If a processing activity does not meet any of the conditions outlined in the GDPR, explicit consent is obtained from the relevant data subject before proceeding with the data processing.

4.3. Retention Periods of Personal Data
Our company retains personal data for the duration specified in relevant laws and regulations when such retention periods are prescribed by law.
If no retention period is specified in the relevant legislation, personal data is processed only for as long as required by the activities being carried out by the company in accordance with company practices and the customs of its commercial life. After this period, the data is deleted, destroyed, or anonymized. Detailed information about this process is provided in Section 9 of this policy.
If the purpose of processing personal data has expired, and the retention periods defined by the relevant legislation or by our company have also ended, personal data may still be retained solely for the purpose of legal disputes (as evidence or to assert or defend legal rights). In such cases, the retention period is determined based on the statute of limitations for such claims or the examples of previous requests made to the company regarding similar matters, even if the statute of limitations has passed. During this time, personal data will not be accessed for any other purpose and will only be accessible when necessary for the legal dispute. Once this period has passed, personal data will be deleted, destroyed, or anonymized.

5. Categories of Personal Data Owners Processed by Our Company
Our company processes the personal data of individuals belonging to the following categories. The scope of this policy is limited to customers, visitors, third parties, employees, job candidates, shareholders, company officials, and employees, shareholders, and officials of institutions we collaborate with.
Although the categories of individuals whose personal data is processed are limited to the ones mentioned above, individuals outside these categories may also submit requests under the GDPR, and their requests will be evaluated within the framework of this Policy.
The following section clarifies the terms related to the categories of personal data owners mentioned in this Policy.

Personal Data Owner Category	Description
Company Customers	Real persons whose personal data is obtained during the operations carried out by the company's business units, regardless of whether they have a contractual relationship with our company.
Visitor	Real persons who have entered the physical premises of our company for various purposes or visited our website.
Third Party	Real persons who do not fall under the scope of this Policy and the company's Employee Personal Data Protection and Processing Policy (e.g., guarantors, companions, family members, relatives, former employees).
Job Candidate	Real persons who have applied for a job with our company or have made their CV and related information available for review by our company.
Company Shareholder	Real persons who are shareholders of the company.
Company Official	Real persons who are members of the company's board of directors or other authorized individuals.
Employees, Shareholders, and Officials of Collaborating Institutions	Real persons who are employees, shareholders, and/or officials of institutions with which our company is in business relations (e.g., partners, suppliers, but not limited to them).

The following table provides further details about the types of personal data processed within the categories of data owners mentioned above.

Personal Data Owner Category	Related Personal Data
Identity Information	Company Customers, Job Candidates, Company Shareholders, Company Officials, Visitors, Employees, Shareholders, and Officials of Collaborating Institutions, Third Parties.
Contact Information	Company Customers, Job Candidates, Company Shareholders, Company Officials, Visitors, Employees, Shareholders, and Officials of Collaborating Institutions, Third Parties.
Location Data	Employees, Shareholders, and Officials of Collaborating Institutions, Company Officials.
Family Members and Relatives Information	Company Customers, Visitors, Job Candidates, Third Parties, Employees, Shareholders, and Officials of Collaborating Institutions.
Physical Security Information	Visitors, Job Candidates, Company Shareholders, Company Officials, Employees, Shareholders, and Officials of Collaborating Institutions, Third Parties.
Financial Information	Company Customers, Job Candidates, Company Shareholders, Company Officials, Employees, Shareholders, and Officials of Collaborating Institutions, Third Parties.
Visual/Audio Information	Company Customers, Job Candidates, Company Shareholders, Company Officials, Visitors, Employees, Shareholders, and Officials of Collaborating Institutions, Third Parties.
Personnel Information	Employees, Shareholders, and Officials of Collaborating Institutions, Job Candidates, Third Parties.
Sensitive Personal Data	Company Customers, Job Candidates, Company Shareholders, Company Officials, Employees, Shareholders, and Officials of Collaborating Institutions, Third Parties.
Request/Complaint Management Information	Company Customers, Job Candidates, Company Shareholders, Company Officials, Visitors, Employees, Shareholders, and Officials of Collaborating Institutions, Third Parties.

6. Third Parties to Whom Personal Data Processed by Our Company Is Transferred and the Purposes of Transfer

Our company, in accordance with Articles 8 and 9 of the GDPR (see Section 3/Title 3.5), may transfer personal data of data owners managed by this Policy to the following categories of recipients:

(i) Business partners of our company,
(ii) Suppliers of our company,
(iii) Group companies,
(iv) Shareholders of our company,
(v) Company officials,
(vi) Public authorities and institutions authorized by law,
(vii) Private law entities authorized by law.

The scope of these recipients and the purposes of data transfer are detailed below.

Data Transfer Recipients	Description	Purpose of Data Transfer
Business Partners	Parties with whom our company has established a partnership for various projects, services, or other activities, either directly or in collaboration with group companies.	Limited to fulfilling the purposes of the partnership.
Suppliers	Parties providing services to our company based on contracts, following our instructions and orders, and necessary for the company's operations.	Limited to ensuring the provision of services necessary for our company's commercial activities.
Group Companies	Other companies within our corporate group.	Limited to ensuring the conduct of commercial activities that require the participation of group companies.
Shareholders	Real persons who are shareholders of our company.	Limited to purposes related to corporate law, corporate governance, and communication processes.
Company Officials	Members of the company's board of directors and other authorized individuals.	Limited to purposes related to strategy design, management, and oversight of commercial activities.
Authorized Public Authorities and Institutions	Public institutions and organizations authorized by law to request information and documents from our company.	Limited to the lawful requests made by public authorities.
Authorized Private Law Entities	Private law entities authorized by law to request information and documents from our company.	Limited to the lawful requests made by authorized private entities.

7. PROCESSING OF PERSONAL DATA BASED ON LEGAL GROUNDS AND LIMITED TO THESE GROUNDS

7.1. Processing of Personal Data and Special Categories of Personal Data

7.1.1. Processing of Personal Data

The explicit consent of the data subject is one of the legal grounds that allows the lawful processing of personal data. In addition to explicit consent, personal data can also be processed if one of the following conditions is met. The legal grounds for personal data processing can be based on any one of the conditions listed below, and more than one of these conditions may be applicable for a single personal data processing activity. If the processed data is considered special categories of personal data, the conditions under section 7.1.2 below apply.
Although the legal grounds for processing personal data may vary within our company, all personal data processing activities are carried out in compliance with the general principles stated in Article 4 of the Personal Data Protection Law (GDPR) (see Section 3.1).

(i) **The Data Subject's Explicit Consent**:
One of the conditions for processing personal data is the explicit consent of the data subject. The data subject's consent must be based on specific information and given freely.
For personal data processing activities outside the primary purpose of data collection (secondary processing), at least one of the conditions listed in sections (ii), (iii), (iv), (v), (vi), (vii), or (viii) below must be met. If none of these conditions apply, the processing of personal data will be based on the data subject's explicit consent.
Personal data is processed based on the explicit consent of the data subject, obtained through appropriate methods.

(ii) **Explicitly Foreseen by Law**:
Personal data can be processed in accordance with the law if explicitly provided for by legislation.
Example: Under Article 230 of the Tax Procedure Law, the name of the relevant person is required to be included on the invoice.

(iii) **Inability to Obtain the Data Subject's Explicit Consent Due to Physical Impossibility**:
If it is impossible to obtain the explicit consent of the data subject due to physical impossibility, and the processing of personal data is necessary to protect the life or bodily integrity of the data subject or another person, personal

data can be processed.

(iv) **Directly Related to the Conclusion or Performance of a Contract**:
Personal data can be processed if it is necessary for the conclusion or performance of a contract with the data subject or other parties involved in the contract.

(v) **Compliance with Legal Obligation of the Company**:
Personal data can be processed if it is required for the company to fulfill its legal obligations as a data controller.

(vi) **The Data Subject Has Made Personal Data Public**:
If the data subject has made their personal data public, the data can be processed.

(vii) **Necessity for the Establishment or Protection of a Legal Right**:
If the processing of personal data is necessary for the establishment, exercise, or protection of a legal right, personal data can be processed.

(viii) **Necessity for the Legitimate Interests of the Company**:
Personal data can be processed if it is necessary for the legitimate interests of the company, provided that it does not violate the fundamental rights and freedoms of the data subject.

7.1.2. Processing of Special Categories of Personal Data
Special categories of personal data may only be processed with the explicit consent of the data subject, unless adequate measures specified by the Personal Data Protection Authority (KVK Authority) are taken. In the following cases, personal data may be processed:

(i) Special categories of personal data, excluding health and sexual life, may be processed in cases provided for by law.

(ii) Personal data related to health and sexual life may only be processed for public health protection, preventive medicine, medical diagnosis, treatment and care services, the planning and management of health services and financing, and only by individuals or institutions under an obligation of confidentiality.

8. PERSONAL DATA PROCESSING ACTIVITIES
To ensure security, our company carries out personal data processing activities related to surveillance through security cameras and tracking the entry and exit of visitors at our buildings and facilities.

8.1. Security Camera Surveillance at Our Company's Buildings and Facilities
This section explains our company's surveillance system using cameras and how personal data privacy and the individual's fundamental rights are protected. The company conducts surveillance using security cameras for the purpose of ensuring the safety of the company and other individuals.

8.1.1. Surveillance with Security Cameras According to GDPR
Our company operates surveillance through security cameras in compliance with the regulations in the Personal Data Protection Law. The surveillance is conducted for security purposes, in accordance with applicable laws, and under the conditions stated in the Personal Data Protection Law.

8.1.2. Notification of Surveillance Activities
In accordance with Article 10 of the Personal Data Protection Law, the data subject is informed. Our company ensures transparency and informs the data subject through multiple methods regarding the surveillance activities with security cameras. This ensures that the fundamental rights and freedoms of the data subject are not violated.

8.1.3. Purpose of Surveillance Activities and Limitation to Purposes
In line with Article 4 of the Personal Data Protection Law, personal data is processed only for the specified and limited purposes. The areas, number of cameras, and times for surveillance are set to achieve the security objectives, and the surveillance is conducted in a manner that is sufficient and limited to the purpose.

8.1.4. Security of Data Obtained from Surveillance
In compliance with Article 12 of the Personal Data Protection Law, necessary technical and administrative measures are taken to ensure the security of personal data obtained through surveillance.

8.1.5. Who Has Access to the Data Collected from Surveillance and Who the Data is Transferred To
Only a limited number of company employees have access to live camera feeds and recorded data. These employees are required to sign confidentiality agreements, ensuring they protect the confidentiality of the data. The data may be transferred to authorized public institutions and organizations upon request.

8.2. Record Keeping of Internet Access for Visitors at Our Company's Buildings and Facilities
For security purposes and the objectives mentioned in this policy, our company may provide internet access to visitors at our buildings and facilities. Internet access logs are kept in accordance with the provisions of Law No. 5651 and related regulations. These records are processed only for the fulfillment of legal obligations or in response to requests from authorized public institutions.
Access to these records is limited to a small number of employees, who may only use them for legal purposes or compliance with public institution requests.

8.3. Website Visitors
For the purpose of providing appropriate services to visitors, customizing content, and engaging in online advertising, our company may track internet activities of visitors on our websites through technical means.

9. CONDITIONS FOR THE DELETION, DESTRUCTION, AND ANONYMIZATION OF PERSONAL DATA

9.1 Obligation to Delete, Destroy, and Anonymize Personal Data
The company is required to delete, destroy, or anonymize personal data in accordance with the relevant legal provisions when the reasons for processing no longer exist, either upon the company's decision or at the request of the data subject.

9.2 Techniques for Deleting, Destroying, and Anonymizing Personal Data

9.2.1 Deletion and Destruction Techniques

- **Physical Destruction:** Personal data may be destroyed physically, ensuring that it cannot be reused.
- **Secure Deletion from Software:** Digital data is permanently deleted using methods that make recovery impossible.

9.2.2 Anonymization Techniques

- **Masking:** Removes identifying information from personal data.
- **Aggregation:** Combines data in a way that prevents identification of any individual.
- **Data Derivation:** Creates a generalized version of the data that can't be linked to any person.

10. RIGHTS OF PERSONAL DATA SUBJECTS; METHODOLOGY FOR THE USE AND EVALUATION OF THESE RIGHTS

10.1. Rights of the Data Subject and Their Exercise

10.1.1. Rights of the Personal Data Subject
Personal data subjects have the following rights:

1. To learn whether their personal data is being processed,
2. To request information if their personal data has been processed,
3. To learn the purpose of processing personal data and whether the data is being used for its intended purpose,
4. To know the third parties to whom personal data is transferred, both domestically and internationally,
5. To request correction of personal data if it is inaccurate or incomplete and to request that the correction be communicated to the third parties to whom the data was transferred,

6. To request the deletion or destruction of personal data when the reasons for processing no longer exist, even though the data has been processed in compliance with the GDPR and other relevant laws, and to request that the deletion or destruction be communicated to third parties to whom the data was transferred,
7. To object to any decision based solely on automated processing of personal data, which results in an adverse outcome for the data subject,
8. To request compensation for damages incurred due to the unlawful processing of personal data.

10.1.2. Cases in Which the Personal Data Subject Cannot Assert Their Rights
Personal data subjects cannot assert the rights mentioned in 10.1.1 in the following cases, as per Article 28 of the GDPR:

1. Processing of personal data for research, planning, and statistical purposes, provided that the data is anonymized for official statistics.
2. Processing of personal data for artistic, historical, literary, or scientific purposes, or in the scope of freedom of expression, without violating national defense, national security, public security, public order, economic security, the privacy of personal life, or personality rights.
3. Processing of personal data by public institutions and organizations assigned with duties and authority by law in the course of preventive, protective, and intelligence activities related to national defense, national security, public security, or economic security.
4. Processing of personal data by judicial authorities or enforcement agencies in relation to investigation, prosecution, trial, or enforcement procedures.

According to Article 28/2 of the GDPR, personal data subjects cannot assert their rights outlined in 10.1.1, except for the right to claim damages, in the following cases:

1. Processing of personal data when necessary for the prevention of a crime or the investigation of a crime.
2. Processing of personal data that has been made public by the data subject themselves.
3. Processing of personal data by public authorities and organizations authorized by law for the execution of monitoring, regulatory tasks, or disciplinary investigations and prosecutions.

10.1.3. Processing of Personal Data for Budget, Tax, and Financial Matters to Protect the State's Economic and Financial Interests

10.1.4. Exercising the Rights of the Data Subject
Personal data subjects can submit requests regarding the rights listed in section 10.1.1 using identity verification information and the methods outlined below, or by other methods defined by the Personal Data Protection Board. The requests can be sent to the company free of charge by completing and signing the Application Form:

- By submitting a signed hard copy of the form, either in person or via notary, to **Güzeloba Mh. Çağlayangil Cad. Şirin İş Merkezi N° 34/D 07230 Muratpaşa/Antalya Türkiye.**
- By sending the signed form to remed@hs03.kep.tr

To make a request on behalf of a personal data subject, a notarized special power of attorney must be provided.

10.1.5. The Data Subject's Right to File a Complaint with the Personal Data Protection Board
In accordance with Article 14 of the GDPR, if a request is rejected, the response is deemed insufficient, or no response is given within the prescribed time, the personal data subject may file a complaint with the Personal Data Protection Board within thirty days from the date they are informed of the response or within sixty days from the date of their application.

10.2. Responding to Applications
Applications should only be submitted to our company if we are the data controller under the GDPR. This can occur when we directly collect personal data from the individual or if personal data is transferred between us and a Group company under the GDPR, which is considered a data transfer between data controllers.

10.2.1. Procedure and Timeframe for Responding to Applications

If a personal data subject submits a request following the procedure outlined in section 10.1.3, our company will respond to the request within thirty days, free of charge, depending on the nature of the request. However, if the Personal Data Protection Board determines a fee, our company will charge the applicant according to the Board's determined tariff.

10.2.2. Information the Company May Request from the Data Subject

To verify whether the applicant is the personal data subject, our company may request information from the individual. Our company may also ask questions to clarify the details of the request.

10.2.3. Right to Reject the Data Subject's Application

Our company has the right to reject the personal data subject's application for the following reasons, providing an explanation:

1. Processing of personal data for research, planning, and statistical purposes with anonymization for official statistics.
2. Processing of personal data for artistic, historical, literary, or scientific purposes, or within the scope of freedom of expression, without violating national defense, national security, public security, public order, economic security, or personality rights.
3. Processing of personal data by public authorities in relation to national defense, national security, public security, or economic security, as part of preventive, protective, and intelligence activities.
4. Processing of personal data for investigation, prosecution, trial, or enforcement procedures by judicial authorities or enforcement agencies.
5. Processing of personal data when necessary to prevent crime or for crime investigation.
6. Processing of personal data made public by the data subject.
7. Processing of personal data by authorized public institutions and organizations for regulatory tasks or disciplinary investigations and prosecutions.
8. Processing of personal data for budget, tax, and financial matters to protect the state's economic and financial interests.
9. If the data subject's request would infringe upon the rights and freedoms of others.
10. If the request imposes disproportionate effort.
11. If the requested information is publicly available.

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

Our company establishes fundamental policies for Group companies, in addition to internal policies related to the principles outlined in this Policy. The aim is to ensure transparency and accountability in the company's personal data processing activities.
The KVK Policy is in alignment with our company's Information Security Management System (ISMS) policy and is audited within the ISMS internal audit system.

12. GOVERNANCE STRUCTURE OF THE PERSONAL DATA PROTECTION AND PROCESSING POLICY

A Personal Data Protection Committee ("Committee") has been established by the decision of the senior management to manage this Policy and related policies (see Section 11) within the company.
The Committee's responsibilities are as follows:

- To prepare and implement fundamental policies on personal data protection and processing, including any necessary amendments, and submit them for approval to senior management.
- To decide how the implementation and audit of personal data protection and processing policies will be carried out and submit the related internal assignments and coordination for senior management approval.
- To identify necessary actions for compliance with the GDPR and relevant legislation and submit them to senior management, ensure implementation, and oversee coordination.
- To increase awareness of personal data protection and processing within the company and among institutions the company collaborates with.
- To identify risks related to personal data processing activities and ensure that necessary precautions are taken, with improvement suggestions submitted to senior management.
- To ensure the training of employees on personal data protection and processing to inform personal data

subjects about their legal rights and the company's data processing practices.

- To resolve personal data subjects' requests at the highest level.
- To monitor developments and regulations regarding personal data protection and submit suggestions for necessary actions within the company.
- To manage the relationship with the Personal Data Protection Board and Institution.
- To carry out any other duties assigned by the senior management regarding personal data protection.