Date : 13.01.2020
Version : 02

Mesa Protection of Personal Data and Privacy Statement

CONTENTS

We, Mesa Mesken, care about the privacy and security of your personal data. With this in mind, we would like to inform you how we collect, process, use and protect the personal data that we receive from our customers, suppliers, business partners, their employees and officials as well as all other third parties in the context of our business relationships.

For all terms and expressions used in this declaration, reference is made to the meaning assigned to them in Act No. 6698 on the Protection of Personal Data ("**KVKK**") and other legislation. The form of address "you" in this statement refers to your person. The use of the term 'personal data' also covers specific personal data. Explanations of the terms and abbreviations used in the 'Policy' can be found in the Appendix 'Abbreviations'.

Please note that your personal data should not be shared with us if you do not agree with the statement. If you opt not to share your personal data with us, we may not be able in some cases to offer you our services, respond to your requests, or provide you with the full functionality of our services.

Please be reminded that it is your responsibility to ensure that the personal data you provide to our company are accurate, complete and up to date. In addition, if you share data with us about other persons, it is your responsibility to collect such data in accordance with local legal requirements. In this case, this means that you have obtained all necessary permissions for us to collect, process, use and disclose personal data from the relevant third parties and our company cannot be held liable in this respect.

ABOUT MESA MESKEN

Mesa Mesken began its journey in 1969 under the name Mesa Mesken Sanayii with the goal of adding value to lives and breaking new ground in its industry. Having achieved this goal with courage and innovation in every sector in which it operates to this day, Mesa's most important value is the happiness of hundreds of thousands of Mesa people and their confidence in the Mesa brand. All along its journey, Mesa designed its buildings with all their components and created the concept of the "residential brand", completely changing the approach of mass housing.

More than 100,000 residences in a 12,000,000 m2 residential area with Mesa signature in all phases of production, from initial design to delivery and post-delivery commissioning, including infrastructure and landscaping, are the result of Mesa's uncompromising approach to quality. The number of employees, which today has reached 4,500, adds more and more experience to the general knowledge and culture of Mesa.

Mesa delivers the buildings it constructs with an "unconditional guarantee of customer satisfaction", and its "after-sales service department" immediately eliminates any defects that occur during the use phase and adds a new dimension to the understanding of quality service. With firsts such as "tunnel formwork technology", "after-sales service department", "housing estate services" it has introduced into the Turkish housing industry, Mesa gets strength from the previous successes for the first steps into new industries and is proud to have created a future of 50 years, relying upon its solid principles.

The words "we" or "the company" or "Mesa Mesken" in the statement relate to the processing activities of personal data by the company Mesa Mesken Sanayii A.Ş (**"Mesa Mesken"**) registered in the trade

register Ankara under the number 382274with headquarters in Ihlamur Cad, No:2 Çayyolu, Çankaya/Ankara.

PRINCIPLES OF PROCESSING PERSONAL DATA

All personal data processed by our company are treated in accordance with the KVKK and the relevant legislation. The basic rules and principles that we take into account when processing your personal data in accordance with Article 4 of the KVKK are as follows:

- **Processing in good faith and in accordance with the law:** When processing personal data, our company acts in accordance with the principles set out by legal regulations and general trust and good faith. To this end, our company takes into consideration the requirements of proportionality in the processing of personal data and does not use personal data for any purpose other than that for its intended purpose.
- **Ensuring that personal data is accurate and update:** Our company ensures that personal data it processed are accurate and up-to-date, taking into account the fundamental rights of personal data subjects and their legitimate interests.
- **Data processing for specific, open and legitimate purposes:** Our company states clearly and precisely that it will process personal data solely for legitimate and lawful purposes. Our company processes personal data only in connection with and in relation to the products and services it offers.
- **Being limited, proportional and expedient to purpose of data processing:** Our company processes personal data in a way to achieve the identified purposes, and avoids the processing of personal data that are not required or not related to the realization of the purpose.
- **Maintenance of personal data for the time required for the purpose foreseen in the relevant legislation or for the purpose for which it was processed:** Our company mantains personal data only for the period specified in the relevant legislation or for the purpose for which they were processed. In this context, our company primarily determines whether a period has been stipulated for the storage of personal data in the relevant legislation; if this is the case, it takes into account this period; otherwise it retains personal data for the time period required for the purpose for which they were processed. When the period expires or the reasons for processing cease to exist, personal data will be deleted, destroyed or anonymized by our company.

DATA OWNER CATEGORIES

The following table lists the categories of data owners other than employees (including trainees and employees of subcontractors) whose personal data are processed by our company. For the processing of personal data of our employees, a separate policy has been adopted and implemented within the company. Persons falling outside the following categories may also submit requests to our company within the scope of the KVKK, which will also be considered as part of the policy.

RELATED PERSON CATEGORY	DESCRIPTION
Customer	Natural or legal persons purchasing our residences and services
Potential customer	Natural or legal persons requesting or interested in the purchase of our apartments and/or use of our services, or deemed to have an interest following an evaluation in accordance with the practices and rules of integrity.
Visitor	Natural or legal persons entering the physical premises owned by our company or in which it conducts an organization (offices, construction sites, etc.) or visiting our Internet sites.
Third person	Natural third persons (e.g. guarantors, companions, family members and relatives) associated with persons acting to ensure the security of our company's business transactions with the above-mentioned parties or to protect the rights of the above-mentioned persons or to afford an advantage, as well as all natural persons (e.g. former employees) whose personal data have to be processed by our company for a specific purpose, even if this is not explicitly stated in the policy.
Candidate employee / candidate trainee	Natural persons having applied for a job with our company in any way or having made their personal background and related information available for inspection by our company.
Group Company employee	Employees and representatives of the domestic Mesa Group companies, which also includes our company
Employees, shareholders and officials of institutions we cooperate with	Natural persons, including shareholders and officials of institutions with which our company maintains all kinds of business relations (including but not limited to project partners, suppliers, etc.)

WHEN DO WE COLLECT PERSONAL DATA ABOUT YOU?

We usually collect your personal data in the following situations:

- When you buy or use our residences and/or services,
- When you sell goods or provide services to us,
- When you subscribe to our newsletters and opt to receive our marketing messages
- When you contact us through our website, e-mail, social media platforms, other online media or by telephone,
- When you apply for a job with our company,
- When you participate in activities and organizations of our company,
- Indirectly, for example through the use of cookies and when you adapt the Website to your specific preferences and personalize the software you use, or by tracking your use of certain pages of the Website (e.g. through your IP address) or by other technical means that allow us to track your use of the Website,
- When you contact us for any purpose as a potential customer/supplier/partner/subcontractor.

The personal data obtained in the aforementioned cases will only be processed by us in accordance with this statement.

WHAT PERSONAL DATA ABOUT YOU DO WE PROCESS?

It depends on the nature of the business relationship between us (e.g. customer, supplier, business partner, etc.) and the way you contact us (e.g. by telephone, e-mail, website, printed documents, etc.) which personal data about you we process.

We process personal data primarily through our website, by telephone or e-mail, by means of customer-specific electronic applications, in cases where you participate in our business events, competitions, promotions and surveys or interact with us in any other way. In this regard, your personal data processed by us can be explained under the following categories:

Data categories	**Examples**
Identity information:	Information in identification documents such as first name, surname, title, date of birth
Contact information	Email, phone number, address
Pictures and/or videos, allowing your identity to be established	For security reasons, we process photos, video images and audio data as well as visual data from CCTV footage when you visit our company or participate in events organized by our company.
Financial data	Credit card details, bank account details, information about accommodation and expenses, billing information
Any other information that you voluntarily choose to share with Mesa Mesken	Personal data that you share on your own initiative, feedback that you provide us with via social media, online platforms or other media, opinions, requests and complaints, evaluations, comments and our assessments thereof, uploaded files, areas of interest, information provided to us for a detailed review before establishing a business relationship with you
Automatically collected electronic data	In addition to the information that you submit directly to us, when you visit or use our website or applications, subscribe to our newsletters or interact with us through other electronic channels, we may collect electronic information that is transmitted to us from your computer, mobile phone or other access device (e.g., device hardware model, IP address, operating system version and settings, the time and duration you used our digital channel or product, your actual location, links you clicked on, motion sensor data, etc. that may be collected when activating location-based products or features)
Information on legal	Your personal data processed within the scope of determination and

Data categories	Examples
proceedings and compliance	follow-up of our legal claims and rights, payment of our debts, and compliance with legal obligations and policies of our Company
Corporate customer/supplier data	Information obtained and created about customers / suppliers as data owners or employees / authorized signatories as data owners within the company structures of customers / suppliers as part of services provided by the business units,
Incident management and safety information	Collected information and evaluations about the events that have the potential to affect our employees, managers or shareholders, vehicle license plate and vehicle information, transportation and travel information, organization of airport transportation and transfer
Personal data collected from other sources	We may also collect your personal data in accordance with applicable laws and regulations through public databases, social media platforms and by methods and platforms which allow our business partners to collect personal data on our behalf. Before entering into business relations with you, for example, we may conduct research in publicly available sources to ensure the technical, administrative and legal security of our business activities and transactions. Besides that, it is also possible that you share certain personal data of third persons with us (e.g. personal data of guarantors, companions, family members and relatives). We may process your personal data using methods that comply with generally accepted legal and commercial practices and integrity rules in these areas in order to manage our technical and administrative risks. In addition, we collect and process personal data that you voluntarily transmit to us via platforms such as telephone, website etc. (e.g. when you call us and request information about our projects).

PROCESSING PERSONAL DATA OF CANDIDATE EMPLOYEES

In addition to the categories of personal data mentioned above, we collect personal data about candidates such as educational background, previous work experience, disability status, etc. in order to be able to assess their knowledge and qualifications, to evaluate their suitability for a position to be filled, to verify the information provided, if necessary, to contact and investigate with third parties whose contact details the candidate has provided, to contact the candidates concerned regarding the application process, to carry out recruitment in accordance with the position to be filled, to comply with legal requirements and to implement the recruitment rules and personnel policy of our company.

Personal data about employee candidates is processed through written and electronic application forms, the Company's electronic application platform, physical or e-mail applications sent to our Company, employment and consulting firms, personal or electronic interviews that the Company conducts with the candidate, and recruitment tests conducted by human resources professionals to assess the suitability of the candidate during the recruitment process.

When applying for a job, candidate employees are informed in detail by means of a separate document in accordance with the KVKK before their personal data are transmitted, and their express consent to the necessary processing of personal data is obtained.

OUR POLICY ON COOKIES

For more information about how we use cookies and other tracking technologies, please read our cookie policy at www.mesa.com.tr. As a general term, "cookie" refers to the information that is sent to a user's computer by an Internet service provider and stored there. The information contained in the cookies can be used when the user re-visits the website in question. Cookies may contain a variety of information, including the number of times a user has visited the website in question. Individual session cookies for each user allow us to monitor how you use the site in a single session. Using cookies we can determine which browser you are using and offer you some special services.

The information stored in the cookies may contain, among other things, the date and time of the visit, the pages viewed, the time spent in the Online Service Center, and the websites visited immediately before and after the visit of the Online Service Center. The data collected through cookies during your visit of the online service center are evaluated and can later be used during your visit of other websites to promote products that might be of interest to you. It is possible to block cookies through your Internet browser.

You can use the “help” function found in most browsers to learn how to prevent your computer from receiving cookies, to see if a cookie is sent and to disable them completely. However, please note that you will not be able to use this website fully if cookies are disabled.

This website uses cookies for a variety of purposes, including:

- Accessing your specific information after entering the website to provide you with personalized content;
- Tracking your preferences you have specified when using this website, such as your preferred date and number formats. We respect the confidentiality of your information. We have adopted the following rules to protect the confidentiality and security of your confidential information at the highest possible level:
- This website does not store persistent cookies on your hard disk. Cookies are removed when you close your browser or leave the website.
- The information in all cookies are sent from this website to your computer in encrypted form.

PROCESSING THE PERSONAL DATA OF VISITORS IN OUR OFFICES AND FACTORIES

Our company processes personal data for the purpose of ensuring its physical security, employees and visitors and to monitor the workplace rules when visitors enter and leave the buildings and construction sites. The visitors' first and last names are checked against their identity cards to monitor their entry and exit, and the license plates are entered in the guest book where deemed necessary. However, the identity card will not be kept during the visitor's stay in the business premises and on the construction sites, and will be returned to the visitor once it has been entered in the guest book. Before being identified, the visitor is informed about the processing of his personal data by an information sheet during the security check at the entrance. However, as our company has a legitimate interest in this context, it is not required

to obtain the express consent of the visitor in accordance with Article 5/2/f of the KVKK. These data are only physically stored in the guestbook and not transferred to any other medium, unless there is a suspicion that there are circumstances endangering the security of the company. However, this information may be used in cases such as crime prevention and corporate security.

Apart from this, for the purpose of ensuring corporate security and in line with the purposes of the Policy, our company provides Internet access with guests who request during their stay in our business premises and on the construction sites In this case, log records of your internet access are saved in accordance with the Law No. 5651 and the imperative provisions of the legislation regulated by this Law; and these records are processed only if requested by authorized state institutions and organizations, or required for the audit process within the company in order to fulfill its legal obligation.

Only a limited number of Mesa Mesken employees have access to the log records obtained in this context. Company employees having access to the mentioned records have access to these records only for use in the demand from the authorized state institutions and organizations, or for use in the audit processes, and they share the records with legally authorized persons.

PROCESSING PERSONAL DATA THROUGH CLOSED CIRCUIT CAMERA FOOTAGE

The security cameras are used to ensure the security of our company and our facilities and personal data are processed accordingly. The objectives of our company in monitoring with surveillance cameras are to improve the quality of the services provided, to ensure the safety of life and property of persons in the company's premises, to prevent abuse and to protect the legitimate interests of data owners.

The processing of personal data carried out by our company through security cameras is in accordance with the Constitution, the KVKK, Law No. 5188 on private security services and related legislation.

In accordance with Article 4 of the KVKK, our Company processes personal data in a limited and restrained manner in connection with the purpose for which they were processed. Where personal privacy takes precedence of the security goals, no surveillance is carried out. To this end, data owners are informed by installing warning signs in the common areas where video surveillance is carried out. However, due to the legitimate interest of our Company in keeping CCTV footage, it is not required to obtain the express consent of the data owners. Furthermore, in accordance with Article 12 of the KVKK, technical and administrative measures are taken in order to ensure the security of the personal data obtained by the surveillance activities.

In addition, a procedure for areas with CCTV cameras, surveillance areas of cameras and recording times has been developed and implemented in our company. This procedure is taken into consideration before installing the CCTV camera. It is not allowed to install cameras in a way that goes beyond the purpose of security and violates the privacy of individuals. Only a certain number of the company's employees have access to the images from the CCTV cameras, and their authorizations are regularly checked. Employees having access to these records sign a written commitment to protect personal data in accordance with the law.

To ensure the security of the building, video recordings are made by cameras installed in our company offices and on the construction sites, at the entrance doors, on the outside of the building, in the cafeteria,

in the visitors' lounge, in the parking lot, in the security cabin and in the floor corridors, and the recording is monitored by the appropriate units.

FOR WHAT PURPOSES DO WE USE YOUR PERSONAL DATA?

The use of your personal data varies depending on the nature of the business relationship between us (e.g. customer, supplier, partner, etc.). Our basic purposes for processing your personal data are listed below. The personal data processing activities relating to candidate employees are described in the section "Personal data processing of candidate employees" above.

Personal data processing objectives	**Examples**
Evaluating potential suppliers/business partners	Conducting our review and conflict of interest process in accordance with our risk rules, managing the purchase and sale of real estate, negotiations with you to establish construction contracts on flat for land basis, location, function and feasibility studies of the relevant real estate and checking official documents, preparation of the relevant official documents, such as the power of attorney and carrying out the relevant procedure with the notary public for this purpose, carrying out licensing procedures, drawing up and execution of contracts, establishment of floor easement, obtaining the certificate of occupancy, carrying out transition to condominium ownership and land use conversion, constitution of servitude, transfer of title deed, management of processes in public institutions and organizations such as the land registry, carrying out accounting, invoicing and payment transactions, protection of our rights and obligations on real estates, preparation of the necessary contractual and commercial documents
Development and management of customer relationships	Carrying out deposit processes related to the projects you are interested in, drawing up preliminary contracts for real estate sale with you, receiving apartment requests, filling of sheets, delivery of apartments and transfer of title deeds, establishment of subscriptions, creating payment plans, managing the processes with banks in connection with tied loans, managing the processes related to promissory notes, transferring preliminary contracts for sale of real estate, conducting name change or revocation processes, carrying out the work and transactions stipulated in the Consumer Protection Act, carrying out invoicing an d payment transactions, preparation of the necessary contractual and commercial documents, meeting your demands, ensuring the security of legal and commercial transactions, submitting proposals for our projects, invoicing, drawing up and execution of contracts, ensuring the legal transaction security after the contract, development of products and services, using new technologies and applications, determination and implementation of our company's commercial and business strategies, management of operations

Personal data processing objectives	Examples
	(demand, proposal, evaluation, order, budgeting, contract), product / project / manufacturing / investment quality processes and operations, in-house system and application management operations, financial operations, financial management
Conducting and concluding the contract process with our suppliers/business partners	Supply of goods and services, shipment of goods and samples, invoicing, managing the registration process for our website applications, establishment and execution of contracts, management of logistics processes, ensuring the legal transaction security after the contract, shipment of goods and samples, improvement, development, diversification of our products and services, offering alternatives for legal / natural persons having business relations with us, development of products and services, using new technologies and applications, determination and implementation of our company's commercial and business strategies, managing operations (demand, proposal, evaluation, order, budgeting, contract), in-house system and application management operations, financial operations, financial management
Management of direct marketing processes	Making marketing notifications regarding our services by email, SMS and telephone, conducting satisfaction surveys or evaluating your opinions and comments on social media, online platforms or other media, informing our customers about our innovations, campaigns and promotions, conducting periodic campaign activities, designing special promotional activities for customer profiles and conducting advertising, promotion and marketing activities to be created through customer "classification" and personal information to prevent unwanted email messages, determination and implementation of our company's commercial and business strategies, planning of organizations
Communication and support (upon your request)	Responding to requests for information about our services, providing support for requests received through our communication channels, and updating our records and database.
Compliance with legal obligations	Execution of tax and insurance processes, performance of our legal obligations under the relevant legislation and especially Law No.5651 and other legislation, Law No.6563 on the Regulation of Electronic Commerce and other legislation, the Turkish Penal Law No.5237 and the Personal Data Protection Law No.6698, performance of the legal obligations under the relevant legislation, management of the processes in the official institutions, in particular with the land registry, obtaining project licenses, audit and inspection of the official authorities, follow-up and conclusion of our legal rights and lawsuits, and performance of the necessary processes in accordance with the laws and regulations that we are subject to such as data disclosure upon request of the

Personal data processing objectives	Examples
	official authorities, fulfilment of the requirements and obligations established to ensure compliance with the legal obligations laid down in the KKVK as required or requested by the regulatory and supervisory institutions and legal provisions
Protection of benefits of the company and provision of security	Performance of any necessary inspection activities within the scope of the requirements and obligations, conducting the conflict of interest controls, ensuring the legal and commercial security of the persons who are in business relationship with our company, keeping the CCTV records for the protection of the company devices and assets, taking the technical and administrative security measures, conducting the satisfaction surveys after accommodation services, to carry out the necessary works for the development of the services we provide, implementation and supervision of workplace rules, management of quality processes, planning and execution of social responsibility activities, protection of the commercial reputation of the Mesa Mesken Group companies, reporting the occurrence of all incidents, accidents, complaints, lost and stolen cases, carrying out the necessary intervention and taking precautions, transferring the rules to be followed for the dangerous situations that may occur during the maintenance and repair and measuring the professional competencies of the subcontractors, ensuring the order of the entry and exit of the company employees and obtaining the necessary information in terms of security and quality, performance of reporting and other obligations determined by laws and regulations.
Design and implementation of the commercial activities of the Company	Budgeting, determining and implementing the commercial policies of the Company in the short, medium and long term, communication, market research and social responsibility activities carried out by our company for purposes of determining and implementing commercial and business strategies of the Company, purchase
Reporting and audit	Establishing communication with the domestic Mesa Group companies, and carrying out necessary activities, internal audit and reporting processes.
Protection of the rights and benefits	Defense against legal claims such as lawsuits filed against our company, investigations, etc.

HOW DO WE USE YOUR PERSONAL DATA FOR MARKETING?

As marketing activities are not subject to the exceptions provided for in article 5/2 and 6/3 of the KVKK, we usually always receive your consent to the processing of your personal data within the framework of

marketing activities Our company may send you promotional communications about products, services, events and promotions at regular intervals. Such promotional communications nay be sent to you by different means such as email, phone, SMS text messages, mail and social networks and online platforms of third parties.

To provide you with the best personalized experience, sometimes these communications may be adapted to your preferences (for example, as you talk us about them based on results from your website visits or links that you click on in our emails)

Upon your approval, we may carry out any marketing activities for purposes of processing any personal data such as internet advertising, targeting, re-targeting, cross-selling, campaign, opportunity and product/service advertisements for specific products and service for you, using the cookies for this purpose, making you commercial offers by considering your preferences and recent purchases, and furthermore monitoring your usage habits according to your previous records during your visit to web applications [corporate website, project websites, blog site, social media accounts of Mesa, mesa and life mobile app] and providing any specific products for you, submitting any specific advertising, campaigns, advantages and other benefits for you especially for sales and marketing activities, performing other marketing and CRM activities, creating new products and services, forwarding any electronic commercial messages (campaign, newsletter, customer satisfaction surveys, product and service ads), sending gifts and promotions, and organizing and keeping informed about corporate communication and other activities and invitations within this scope.

When the applicable legislation requires, we will ask for your consent before we start the above activities. You will also be given the opportunity to revoke (stop) your consent at any time. In particular, you can always stop sending marketing notifications to you by following the unsubscribe instruction in each email and SMS message.

If you log in a Mesa Mesken account, you may be given the option to change your communication preferences under the relevant section of our website or application. You can always contact us to stop sending marketing communications to you (you can find the contact details below in the following section "What Are Your Rights to Your Personal Data?").

ON WHAT LEGAL BASIS DO WE PROCESS YOUR PERSONAL DATA?

We process your personal data on the following legal basis under article 5 of the KVKK and especially the Turkish Commercial Law No. 6102, Turkish Law of Obligations No. 6098, Tax Procedure Law No. 213, and the electronic commerce legislation:

Legal basis	**Examples**
We process your personal data by obtaining your express consent pursuant to the KVKK and other legislations in any circumstances that require your express consent (in this case, we would like to remind that you may withdraw your consent at your desired time).	We obtain your consent to carry out our marketing activities.
In any circumstances allowed under the current legislation	Name of the relevant person must be

Legal basis	Examples
	written on the invoice under article 230 of the Tax Procedural Law.
Where it is compulsory to protect the vital benefits of any person	Provision of the medical information of the member of the Board of Directors, who feel faint, to a physician.
Where we enter into and perform the contract with you and perform our obligation under a contract	The identity information of the customer is obtained under a contract with the customer.
Where we perform our legal obligations	We perform our legal obligations and submit any information required by the decree to the court.
If your personal data is made public by you	You must send us an email message, enter the contact information of the candidate employee to the website containing the job applications and use your personal information made public by means such as social media, etc. to contact you.
When we must process any data to create or protect any right, exercise our legal rights and defend against any legal claims made against us.	Protection and when necessary, use of the documents having a nature of proof/evidence.
Where our legitimate benefits require, provided that they never harm any basic rights and remedies	Provision of security of our company networks and information, performance of our company activities, determination of any suspicious procedures and checking if the procedures comply with our risk rules, and utilizing any storage, accommodation, maintenance and support services for purpose of providing the IT services in technical and security aspects, using cloud technology to ensure the efficiency of our business activities and take advantage of the benefits of technology

We would like to emphasize that, if your personal data is processed upon your express consent, and you withdraw your consent, you will be removed from the commercial membership program, where such data processing based on an express consent is required, and you will not be able to benefit from the advantages that you receive through such transactions as of the respective date.

WHEN DO WE SHARE YOUR PERSONAL DATA?

Domestic data transfer

Our Company is responsible for acting in accordance with the decisions and related regulations, in particular, as prescribed in article 8 of the KVKK and made by the Committee on transfer of personal data. As a rule, our Company cannot transfer any personal data and special data of the data owners to other natural or legal persons without the express consent of the related person.

Furthermore, in circumstances stipulated in Articles 5 and 6 of the KKVK, it is possible to transfer the personal data without the consent of the related person. Our company may transfer the personal data to third persons and companies under the umbrella of Mesa Mesken in accordance with the conditions set forth in the KVKK and other relevant legislation and by taking all safety precautions specified in the legislation, it is specified otherwise in such agreement if there is an agreement entered into between us and data owner, or in the said contract and in the law or other relevant legislation.

International transfer of personal data

Our company may transfer any personal data to any third parties in Turkey and process and store it in Turkey or outside Turkey and transfer it to abroad including outsourcing in accordance with the conditions set forth in the Personal Data Protection Law and other relevant legislation and by taking all safety precautions specified in the legislation. In order to carry out our company's activities in the most efficient way and to benefit from the opportunities of technology, we transfer your personal data abroad by taking necessary technical and administrative measures through cloud information technology.

As a rule, we seek the express consent of the data owners pursuant to article 9 of the KVKK to transfer any personal data to abroad. However, it is prescribed that any personal data may be transferred to abroad without seeking the express consent of the data subject, provided that one of the provisions specified in article 9 and article 5/2 or article 6/3 of the KVKK is available and

a) adequate protection is available in a foreign country, to which the personal data will be transferred,
b) in absence of adequate protection, the data supervisors in Turkey and in the relevant foreign country undertake the adequate protection in written and the consent of the Committee is available.

Accordingly, in the exceptional cases where the express consent is not sought for the transfer of the personal data mentioned above, in addition to the conditions of unauthorized processing and transfer, our Company is required to have adequate protection in accordance with the KVKK. The Personal Data Protection Committee will determine whether adequate protection is provided; in the case of the absence of adequate protection, the data supervisors in Turkey and in the relevant foreign country undertake the adequate protection in written and the consent of the Personal Data Protection Committee is available.

Parties at home and abroad we share personal data with

We share your personal data only for the purposes listed below and only to the extent necessary. Except in these cases, we take special care not to share your personal data. The parties we share personal data with are the following:

- **Mesa group companies:** As we operate under the Mesa group of companies, your data may be shared or made available to the companies of the Mesa group located in Turkey. This sharing will only be made with authorized employees of the relevant Mesa group company. In some special cases, we may share personal data with Mesa group companies rather than sharing anonymous information. The Mesa Residential Data Sharing Agreement regarding the transfer of your personal data to the Mesa Group companies has been signed and necessary measures have been implemented.

- **Service providers and business partners:** They include the parties, with whom our Company establishes business partnerships for the purposes of sales, promotion and marketing of our Company's services, after-sales support, while we carry out any commercial activities of our Company Just like many businesses, we can also work with the reliable third parties such as information and communication technology providers, consultancy service providers, cargo companies and travel agencies to conduct any functions and services in the most efficient manner and in accordance with current technologies within the scope of some data processing activities. In this context, we may share any data to carry out our business activities. This sharing is limited in order to ensure the fulfillment of the objectives of establishing and performing the business partnership. We use cloud information technologies in order to carry out the activities of our company in the most efficient way and to benefit from the opportunities of the technology at the maximum level, and we may process your personal data at home and abroad through the companies providing cloud information services. The marketing service support company, with whom we share the data, may be established abroad. In this context, we share the data internationally in accordance with the provisions of articles 8 and 9 of the KVKK on international data sharing.

- **Official authorities:** We share your personal data with the relevant governmental, judicial and administrative authorities, as required by law or when we need to protect our rights (e.g. tax authorities, law enforcement agencies, courts and enforcement offices).

- **Private judicial entities:** Pursuant to the provisions of the relevant legislation, any personal data may be shared under the legal powers of any private judicial entities, which are authorized to obtain any information and documents from our Company, for limited purposes (e.g. an Occupational Health and Safety Company).

- **Professional consultants:** We may share your personal data with any professional consultants such as banks, insurance companies, auditors, lawyers, financial advisers and other consultants.

- **Other persons in connection with corporate transactions:** We may share your personal data from time to time for purposes of carrying out any corporate procedures such as the sale, restructuring, merger, joint venture or other use of our business, assets or shares (including those related to any bankruptcy or similar process).

HOW LONG DO WE STORE YOUR PERSONAL DATA?

We store your personal data only for necessary period to fulfill the purpose for which they were collected. We set these periods separately for each business process and if we do not have any other reason to store

your personal data at the end of the relevant period, we will destroy your personal data and/or anonymize in accordance with the KVKK.

We consider the following criteria when we determine the destruction and/or anonymization times of your personal data:

- Within the scope of the purpose of processing the relevant data category, the period of time accepted as a general practice in the industry where the data supervisor operates,
- The time required for the processing of personal data in the relevant data category and when the legal relationship established with the relevant person shall continue,
- The period in which the legitimate benefit obtained by the data supervisor shall be valid in accordance with the law and the good faith rules, depending on the purpose of the relevant data category being processed;
- The period in which the risks, costs and responsibilities that may arise from the storage of the relevant data category for the purpose of processing them shall continue legally,
- Whether the maximum period to be determined is appropriate to keep the relevant data category accurate and up-to-date when necessary,
- The period in which the data supervisor is obliged to keep personal data in the relevant data category due to his legal obligation,
- The timeout set by the data supervisor to assert a right depending on a personal data in the relevant data category.

HOW DO WE DISPOSE YOUR PERSONAL DATA?

Although any personal data have been processed in accordance with the provisions of the relevant law, Article 138 of the Turkish Penal Code and Article 7 of the KVKK, if any reasons that require processing the personal are eliminated, it is deleted, destroyed or made anonymous at our Company's own discretion or if the personal data subject requires so.

In this context, the Personal Data Storage and Destruction Policy has been prepared. Our company reserves the right not to fulfill the request of the data owner, in cases where it has the right and/or obligation to maintain personal data in accordance with the relevant legislation. When the personal data is also processed in non-automated ways, provided that it is part of any data recording system, the system that destruct of the personal data physically in a way that cannot be subsequently used when data is deleted/destroyed is implemented. When our company agrees with a person or organization to process personal data on its behalf, the personal data is deleted securely by such person or organization so that it cannot be recovered. Our company is able to make personal data anonym when the reasons that require the processing of personal data processed in accordance with the law are eliminated.

TECHNIQUES OF DESTRUCTING THE PERSONAL DATA

Deletion of personal data

Although our company has been processed in accordance with the provisions of the relevant law, it may delete personal data at its own discretion or upon the request of the personal data owner in case the reasons requiring processing are eliminated. Deletion of personal data is the process of making personal

data inaccessible and non-reusable by the relevant users. Our company takes all technical and administrative measures to ensure that the deleted personal data cannot be accessed and reused for the relevant users.

Process of deleting the personal data

The process of deleting the personal data is as follows:

- Determination of the personal data that will be subject to deletion.
- Identification of the relevant users for each personal data by using the access authorization and control matrix or similar system.
- Determination of the authorizations of the relevant users and methods such access, retrieval and reuse.
- Closing and eliminating the authorizations and methods of access, retrieval and reuse of the relevant users within the scope of personal data.

Methods of deleting the personal data

Data recording media	Description
Personal data available in the servers	Among the personal data available in the servers, for ones, which require storage and which period expires, the access authorization of the relevant users is cancelled by the system administer and the deletion operation is conducted.
Personal data available in the electronic media	Among the personal data available in the electronic media, ones, which require storage and which period expires, may never be accessed and reused by other employees (relevant users) except the database administrator.
Personal data available in the physical media	Among the personal data stored in the physical media, ones, which require storage and which period expires, may never be accessed and reused by other employees except the department manager responsible for document archive Furthermore, it is stroke out/dyed/deleted and the blackening operation is applied so that is cannot be read.

Destruction of personal data

Although our company has been processed the personal data in accordance with the provisions of the relevant law, it may destroy it at its own discretion or upon the request of the personal data owner, where the reasons requiring processing the personal data are eliminated. Destruction of the personal data is the process, in which personal data cannot be accessed, retrieved or reused by anyone in any way. The data supervisor is obliged to take all necessary technical and administrative measures for the destruction of personal data.

Data recording media	Description
Personal data available in the physical media	Among the personal data stored in the physical media, ones, which require storage and which period expires, are destroyed in a shredder so that it cannot be recycled.
Personal data available in the optical / magnetic media	Among the personal data stored in the optical media and magnetic media, ones, which require storage and which period expires, are melted, incinerated or pulverized and thus destroyed physically so that they are no longer legible.

Physical destruction: The personal data can be processed in non-automated ways, provided that they are part of any data recording system. While such data is deleted/destroyed, a system is implemented, which destroys the personal data physically so that they cannot be reused afterwards.

Secure deletion from the software: While any data processed in fully or partially automated ways and stored in digital media are deleted/destroyed, the methods, which deleting the data from the related software so that they cannot be recovered, are used.

Secure deletion by a specialist: In some cases, you can engage a specialist to delete the personal information on your behalf. In this case, the personal data are deleted/destroyed securely by the person skilled in the art so that it cannot be recovered.

Blackening: It is a process, which makes any personal data physically unreadable.

Anonymization of personal data

Anonymization of personal data means that the personal data cannot be attributed to any other determinable or identifiable person, even by comparison with other data. Our company is able to make personal data anonym when the reasons that require the processing of personal data processed in accordance with the law are eliminated. In order to make the personal data anonymous, the personal data must be rendered unrelated to a specific or identifiable natural person, even by using the suitable techniques for the recording medium and relevant field of activity, such as the return of data by the data supervisor or recipient groups and/or matching the data to other data. Our company takes all technical and administrative measures necessary to make the personal data anonym.

Any personal data made anonym in accordance with Article 28 of the KVKK can be processed for research, planning and statistical purposes. Such operations are outside the scope of the KVKK and will not require express consent of the personal data subject.

Methods of personal data anonymization

Anonymization of personal data that the personal data cannot be associated with any determinable or identifiable natural person, even if it is matched with other data.

In order to make the personal data anonymous, the personal data must be rendered unrelated to a specific or identifiable natural person, even by using the suitable techniques for the recording medium and relevant field of activity, such as the return of data by the data supervisor or recipient groups and/or matching the data to other data.

Anonymization of personal data means that all direct and/or indirect identifiers in a data set are removed and replaced and thus prevent the relevant person from being identified or loses their property to distinguish such person in a group or crowd so that such person cannot be associated with a natural person. Any data that does not indicate a particular person as a result of blocking or losing these features is considered as data made anonym. In other words, anonymized data is the information that identifies a natural person before this process, but after this process, it cannot be associated with the relevant person and has been disconnected from the person. The purpose of making the personal data anonym is to break the link between the data and the person, whom this data defines. All of the bond breaking operations carried out by automatic or non-automatic methods such as grouping, masking, derivation, generalization, randomization, etc. are applied to the records in the data recording system where the personal data are stored. The data obtained as a result of the application of these methods should not be able to identify a particular person.

The exemplary anonymization methods are described as follows:

Anonymization methods that do not provide any value irregularity: In methods that do not provide value irregularity, no change or addition, subtraction is applied to the values of the data in the cluster; instead, changes are made to all rows or columns in the cluster. Thus, while the overall data changes, the values in the fields keep their original state.

Removing the variables

It is a method of anonymization provided by completely deleting one or more of the variables from the table. In this case, the entire column in the table will be removed completely. This method can be used for reasons such as the fact that the variable is a highly descriptive variable, that there is no more appropriate solution, that the variable is too sensitive to be disclosed to the public, or that it does not serve analytical purposes.

Removing the records

In this method, anonymity is reinforced by subtracting a line containing singularity in the data set and the probability of generating assumptions about the data set is reduced. Often, the records that are extracted are those that do not have a common value with other records and can easily be guessed by those who have an idea of the data set. For example, in a data set that includes survey results, only one person from any sector is included in the survey. In such a case, it may be preferable to remove only the record of this person rather than to subtract the "sector" variable from all survey results.

Regional masking

The objective of the regional masking method is to make the data set more secure and to reduce the risk of predictability. If the combination of the values of a particular record creates a very visible condition,

and it is likely to cause the individual to become distinguishable in the relevant community, the value that creates the exception is changed to "unknown".

Generalization

It is the process of converting the relevant personal data from a special value to a more general value. It is the most commonly used method for generating cumulative reports and performing operations based on total figures. The resulting new values show the total values or statistics a group that makes it impossible to access to a natural person. For example, assume that a person with Turkish ID No. 12345678901 buys diapers from the e-commerce platform, and then also buys wet napkins. In the anonymization process, it can be concluded that xx % of people, who buy diapers from the e-commerce platform, also buy the wet napkin by using the generalization method.

Lower and upper limit coding

The upper and lower limit coding method is defined by defining a category for a given variable and combining the remaining values within the grouping created by this category. Usually, the low or high rates of the values in a given variable are added together and a new definition is made.

Global coding

The global coding method is a grouping method used in datasets with values that cannot be applied to lower and upper bound codes, do not contain numerical values or cannot be numerically sorted. It is generally used when certain values make it easier to make assumptions and suppositions by clustering. All records in the data set are replaced by this new definition by creating a common and new group for the selected values.

Sampling

In the sampling method, a subset from the cluster is described or shared, rather than the entire data set. This reduces the risk of generating accurate estimates of individuals since it is not known whether a person known to be in the entire data set is included in the disclosed or shared sample subset. Simple statistical methods are used to determine the subset to be sampled. For example, it may be meaningful to make scans and make estimates in the relevant data set of a woman who is known to live in Istanbul if anonymously discloses or shares a dataset of demographic information, occupations and health status of women living in Istanbul. However, only the records of the women, who are registered in the civil registration office in Istanbul, are left in the relevant data set and the anonymization is removed from the data set and the data is disclosed or shared, and the malicious person who accesses the data has a population record of a woman who knows that she lives in Istanbul, since it is estimated whether the information in the hands of the information belonging to this person cannot make a reliable estimate.

Anonymization methods that provide a value irregularity: Unlike the above mentioned methods, distorting the values of the data set is created by changing the existing values. In this case, since the values of the records are changing, it is necessary to calculate the benefit planned from the data set correctly. Even if the values in the data set are changing, it is still possible to benefit from the data by ensuring that the total statistics remain intact.

Micro joining

With this method, all records in the data set are first arranged in a meaningful order and then the whole set is subdivided into a certain number of subsets. Then, the value of each subset of that variable is replaced with the average value by taking the average of the value of the specified variable. Thus, the average value of that variable for the entire dataset will not change.

Data exchange

The data exchange method is the record changes obtained by exchanging values of a variable subset between the pairs selected from the records. This method is mainly used for categorized variables and the main idea is to transform the database by changing the values of the variables between records of individuals.

Adding noise

With this method, additions and subtractions are performed in order to achieve the determined distortions in a selected variable. This method is often applied to data sets that contain numeric values. Distortion is applied equally to each value.

Statistical methods to strengthen anonymization

In some data sets made anonym, the combination of some values in the records with individual scenarios may lead to the identification of persons in the records or the assumption that their personal data can be derived.

For this reason, anonymity can be strengthened by using various statistical methods in the data sets made anonym by minimizing the singularity of the records in the data set. The main purpose of these methods is to minimize the risk of anonymity deterioration while keeping the benefit of the data set at a certain level.

Anonymity

In the data sets made anonym, the fact that the identities of the persons in the records are identifiable or that the information about a particular person becomes easily predictable if the indirect identifiers are combined with the correct combinations has shaken confidence in the anonymization processes. Accordingly, the datasets made anonym by the various statistical methods had to be made more reliable.

Anonymity has been developed to allow the identification of more than one person with specific fields in a data set, to prevent the disclosure of information specific to individuals that exhibit unique characteristics in certain combinations. If there are multiple records of combinations of some of the variables in a data set, the likelihood of identifying the persons corresponding to that combination is reduced.

Diversity

The L-diversity method, which is developed by the studies conducted on the deficiencies of K-anonymity, takes into account the diversity of the sensitive variables corresponding to the same variable combinations.

Proximity

Although the L-diversity method provides diversity in personal data, there are situations in which it cannot provide adequate protection because the method does not deal with the content and sensitivity of personal data. In this form, the process of calculating the degree of closeness of personal data and values among themselves and subdividing the data set according to these degrees of proximity is called as T-proximity method.

Choosing the anonymization method

Our company decides which of the above methods will be applied by looking at the data at their disposal and considering the following features of the data set:

Nature of the data,
Size of the data,
Structure of data in physical media,
Data diversity,
Benefit/processing purpose of the data,
Processing frequency of data,
Reliability of the party to which the data will be transferred,
The meaningful efforts to make the data anonymous,
The magnitude of the damage that may arise in case of anonymity of the data, and its impact area,
The distribution/centrality ratio of the data,
Control of users' access to relevant data, and
The likelihood that an effort to construct and launch an attack that would disrupt anonymity would make sense.

While it makes a data anonymous, the Company checks the data whether it is a re-identifier by using known or publicly available information from other institutions and organizations to which it transmits personal data by means of contracts and risk analyzes.

Anonymity assurance

When it decides to make it anonym instead of deleting or destroying a personal data, our company does not disrupt the anonymity by combining the data set made anonym with any other data sets, without creating one or more values in a way that it can make a record unique and anonym. We want consider the fact that the values in the data set cannot be combined and produce an assumption or result. As our company makes anonymous data, any controls are made as the features listed in this article change and anonymity is maintained.

Risks of corruption of anonymization by reverse processing of anonymous data

Since anonymization is a process of destroying the distinguishable and identifiable characteristics of personal data, there is a risk that these operations can be reversed by various interventions and that the anonymized data will become re-identifiable and distinguishable again. This is referred to as disruption of anonymity. The anonymization processes can be accomplished only by manual or automated processes, or by hybrid processes consisting of a combination of both types. It is important, however, that after the

data made public is shared or disclosed, any measures are taken to prevent anonymity from being compromised by new users who can access or own the data. The actions carried out consciously about the disruption of anonymity are called "attacks against the disruption of anonymity". In this context, our Company investigates whether there is a risk that the personal data made public may be reversed by various interventions, and that the data made public may become re-identifiable and distinguishable from the natural persons, and an operation is established accordingly.

HOW DO WE PROTECT YOUR PERSONAL DATA?

In order to protect your personal data and prevent unlawful access, the Company takes necessary administrative and technical measures in line with the Personal Data Security Guideline published by the Personal Data Protection Committee, prepares the procedures in the company, prepares the clarification and express consent texts, conducts any necessary audits to ensure the implementation of the provisions of the KVKK in accordance with article 12/3 of the KVKK, or procure any external service. The results of these audits are evaluated within the scope of the internal operation of the Company and necessary actions are taken to improve the measures taken.

Your personal data mentioned above will be transferred to physical archives and information systems of our Company and/or our suppliers and kept in both digital and physical media. The technical and administrative measures taken to ensure the security of personal data are described in detail below under two headings:

Technical measures

We use generally accepted standard technologies and operational security methods, including the standard technology called Secure Socket Layer (SSL), to protect the personal information collected. However, due to the nature of the Internet, information can be accessed by unauthorized persons over networks without the necessary security measures. We take technical and administrative measures to protect your data from risks such as destruction, loss, tampering, unauthorized disclosure or unauthorized access, depending on the current state of technology, the cost of technological implementation, and the nature of the data to be protected. Within this scope, we conclude data security agreements with the service providers we work with. Detailed information on these service providers can be found at [related link].

1) Ensuring cyber security: We use the cyber security products to ensure personal data security, but our technical measures are not limited to this. The first line of defense against attacks from environments such as the Internet is established through measures such as firewall and gateway. However, almost every software and hardware is subjected to a number of installation and configuration operations. Considering that some of the commonly used software, especially older versions, may have documented security vulnerabilities, unused software and services are removed from the devices. Therefore, such unused software and services are primarily preferred because of their ease of deletion rather than keeping them up to date. The patch management and software upgrades ensure that the software and hardware work properly and that the security measures taken for the systems are sufficient to check regularly.

2) Access restrictions: Access rights to systems containing personal data are restricted and reviewed regularly. Within this scope, employees are granted access rights to the extent necessary for their work and duties and their powers and responsibilities, and access to related systems is provided by

using user name and password. When creating these codes and passwords, combinations of uppercase and lowercase letters, numbers and symbols are preferred instead of numbers or letter sequences related to personal information that can be easily guessed. Accordingly, the access authorization and control matrix is established.

3) Encryption: In addition to using strong codes and passwords, limiting the number of password entry attempts to protect against common attacks such as the use of brute force algorithm (BFA), ensuring that codes and passwords are changed periodically, and administrator account and admin privileges are opened only for use when needed and for employees who have been dismissed from the data supervisor, access is restricted without delay, such as deleting an account or closing entries.

4) Antivirus software: In order to protect against malware, products such as antivirus, antispam, which regularly scans the information system network and detect hazards are used, and the required files are regularly scanned. If personal data will be obtained from different internet sites and/or mobile application channels, it is ensured that the connections are made via SSL or more secure way.

5) Monitoring of personal data security: Checking which software and services are operating in information networks, determining whether there is any infiltration or non-infiltration in IT networks, keeping the transaction transactions of all users regularly (such as log records), security problems are reported as fast as possible. A formal reporting procedure is also set up for employees to report security weaknesses in systems and services or threats using them. Evidence is collected and stored securely in the event of undesired events such as information system crash, malicious software, decommissioning attack, missing or incorrect data entry, violations of privacy and integrity, abuse of information system.

6) Ensuring the security of personal data environments: If personal data is stored on the devices of the responsible persons or in the media, physical security measures are taken against threats such as theft or loss of these devices and papers. The physical environments containing personal data are protected against external risks (fire, flood, etc.) by appropriate methods and the entrances / exits to these environments are controlled.

   If personal data is in electronic form, access between network components can be restricted or separated to prevent personal data security breach. For example, if personal data is being processed in this area by limiting it to a specific portion of the network in use, which is reserved for this purpose, the available resources can be reserved for the security of this limited area, not the entire network.

   Measures at the same level are also taken for paper media, electronic media and devices containing personal data of the Company located outside the Company campus. As a matter of fact, although personal data security violations frequently occur due to theft and loss of devices containing personal data (laptop, mobile phone, flash disk, etc.), personal data to be transmitted by e-mail or mail is also sent carefully and with adequate precautions. Sufficient security measures are also taken in case employees provide access to the information system network with their personal electronic devices.

   The use of access control authorization and / or encryption methods is applied in case of loss or theft of devices containing personal data. In this context, the password key is stored only in the environment accessible to authorized persons and unauthorized access is prevented.

Paper documents containing personal data are also stored in a locked and accessible environment only, and unauthorized access to these documents is prevented.

If any personal data is obtained by others by unlawful means, the Company shall inform the Personal Data Protection Committee and the data owners of this fact as soon as possible pursuant to article 12 of KVKK. If they see necessary, the Personal Data Protection Committee may announce this situation at the website or in by any other means.

7) Storage of personal data in the cloud: In the event that personal data is stored in the cloud, it is necessary for the Company to assess whether the security measures taken by the cloud storage service provider are adequate and appropriate. Access to data storage areas containing personal data is logged and unauthorized access or attempted access is immediately communicated to those concerned.

8) Information technology systems procurement, development and maintenance: Security requirements are taken into consideration when determining the requirements related to the procurement, development or improvement of new systems by the Company.

9) Backing up of personal data: In case of personal data being damaged, destroyed, stolen or lost due to any reason, the Company makes use of the backed up data as soon as possible. The backed up personal data is accessible only by the system administrator, and data set backups are excluded from the network.

Administrative measures

- All activities carried out by our company have been analyzed in detail in all business units and as a result of this analysis, a process-based personal data processing inventory has been prepared. Risky areas in this inventory are identified and necessary legal and technical measures are taken continuously. (For example, the documents to be prepared within the scope of KVKK have been prepared considering the risks in this inventory)
- Personal data processing activities carried out by our company are audited by information security systems, technical systems and legal methods. Policies and procedures regarding personal data security are determined and regular controls are conducted within this scope.
- From time to time, our company may provide services from external service providers to meet information technology needs. In this case, we ensure that these data processing external service providers meet at least the security measures provided by our Company. In this case, a written agreement is signed with the Data Processor and the contract includes at least the following points:
    - The Data Processor acts only in accordance with the instructions of the Data supervisor, the purpose and scope of the data processing specified in the agreement, the KVKK and other legislation,
    - The Data Processor acts in accordance with the Personal Data Retention and Destruction Policy,
    - The Data Processor is obliged to keep any data confidential indefinitely in relation to the personal data processed,
    - In the event of any data violation, the Data Processor is obliged to inform the Data supervisor of it immediately,

- Our Company will perform or have the necessary audits performed on the Data Processor's systems containing personal data, and may review the reports and service provider on the spot,
- Our Company will take the necessary technical and administrative measures for the security of personal data, and
- Furthermore as long as the nature of the relationship between the Data Processor and us is suitable, the categories and types of the personal data transferred to the Data Processor are also specified in a separate article.

- As emphasized in the guidelines and publications of the Authority, personal data is reduced as much as possible within the framework of the data minimization principle, and personal data that is not required, outdated and does not serve a purpose are not collected and if collected in the previous period of the KVKK, a data in accordance with the Personal Data Retention and Disposal Policy is destroyed.
- The employees specialized in technical issues are employed.
- Our Company has set provisions on confidentiality and data security in the Employment Agreements to be signed during the recruitment process of its employees and requests that the employees comply with these provisions. The employees are regularly informed and trained about the personal data protection law and taking necessary measures in accordance with this law The roles and responsibilities of the employees have been revised and their job descriptions have been revised.
- Technical measures are taken in accordance with technological developments, and the measures taken are periodically checked, updated and renewed.
- The access authorizations are limited and reviewed regularly.
- The technical measures taken are regularly reported to the authorized person, and the issues that constitute risk are reviewed and efforts are made to produce the necessary technological solutions.
- Software and hardware including virus protection systems and firewalls are installed.
- The backup programs are used to ensure the safe storage of personal data.
- Security systems are used for storage areas, technical measures taken are periodically reported to the person concerned as a result of internal controls, risk issues are re-evaluated and necessary technological solutions are produced. The files/printouts stored in the physical environment are stored by the supplier companies and then disposed of in accordance with the established procedures.
- The protection of personal data is also accepted by the top management, a special Committee (the Personal Data Protection Committee) has been established and started to work. A management policy regulating the working rules of the Company's KVK Committee has been put into effect within the Company and the duties of the KVK Committee have been explained in detail.

HOW DO WE PROTECT YOUR SENSITIVE PERSONAL DATA?

A separate policy on the processing and protection of sensitive personal data has been prepared and put into force.

Article 6 of the KVKK is arranged as data of a special quality on race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, disguise and dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data as they carry the risk of causing the victimization or discrimination of persons when processed in contradiction, and is subject to the processing of this data more sensitive protection.

Pursuant Article 10 of the KVKK, our Company enlightens the Related Persons during the collection of personal data. Special personal data are processed by taking appropriate measures and performing the necessary audits. As a rule, one of the conditions for the processing of sensitive personal data is the express consent of the data subject. Our company offers data subjects the opportunity to disclose their express consent on a specific issue, based on information and freewill.

As a rule, our Company obtains the express consent of the Related Persons in writing for the processing of sensitive personal data. However, pursuant to article 6/3 of the KVKK and in case of the existence of any of the conditions specified in article 5/2 of the KVKK, the express consent of the Related Persons is not required. Besides, in article 6/3 of the KVKK, it stated that the personal data on health and sexual life is processed by the persons or authorities and institutions under the confidentiality obligation for purposes of protecting of the public health, conducting the preventive medicine, medical diagnosis, treatment and care services, and planning and managing healthcare service and financing without the express consent of the relevant person. Regardless of the reason, the general data processing principles are always taken into account in the processing processes and they are complied with.

Our company takes special measures to ensure the security of personal data. Due to the principle of data minimization, sensitive personal data is not collected and processed only when necessary, unless it is necessary for the relevant business process. In case of processing of personal data of special quality, technical and administrative measures are taken to comply with the legal obligations and to comply with the measures determined by the Personal Data Protection Committee.

WHAT ARE YOUR RIGHTS ABOUT YOUR PERSONAL DATA?

Pursuant to article 11 of the KVKK as the data subjects, you have the following rights on your personal data:

- To find out whether your personal data is processed by our Company,
- To request information if your personal data has been processed,
- To learn the purpose of processing your personal data and whether they are used properly,
- To know the third parties to whom your personal data is transferred at home or abroad,
- If your personal data is incomplete or processed incorrectly, to request that it be corrected, and request that the transaction be notified to the third parties to whom your personal data have been transferred,
- Although it has been processed in accordance with the KVKK and other relevant provisions of the law, to request the deletion or destruction of your personal data in case the reasons that need to be processed, and to request that the transactions made within this scope be notified to the third parties where your personal data is transferred,
- To object to the occurrence of a result against you by analyzing the processed data exclusively through automated systems, and
- To claim compensation if you have suffered damage as a result of unlawful processing of your personal data.

You can forward these requests to our Company free of charge in accordance with the Application Notice and by using the following methods:

1) To complete the form available at www.mesa.com.tr, to sign it with a wet signature and forward it personally to Mesa Mesken Sanayii A.Ş Kültür Ihlamur Cad., No:2 Çayyolu, Çankaya/Ankara (please, note that you must submit your identity card).
2) To complete the form available at www.mesa.com.tr , to sign it with a wet signature, and to forward it to Mesa Mesken Sanayii A.Ş Ihlamur Cad., No:2 Çayyolu, Çankaya/Ankara via a notary public.
3) To complete the application form at www.mesa.com.tr, to sign it with "secure electronic signature" under the Electronic Signature Law No. 5070, and send it the form with a secure electronic signature form mesameskensanayiias@hs01.kep.tr by e-mail; and
4) Delivering to our Company in writing by using your e-mail address previously notified and registered in our Company's system.

The application must

contain first name, last name, if the application is written, signature, Turkish ID Number for the citizens of the Republic of Turkey, nationality for foreigners, passport number or identification number (if any), residence or business address based on the notice, electronic mail address, telephone and fax number for the notice if any, and subject of the request. Any relevant information and documents are also added to the application.

It is not possible to make any request by third parties on behalf of the personal data owners. In order for a person other than the personal data owner to make a request, a special power of attorney issued by the personal data subject on behalf of the applicant must have a notarized copy with a wet signature. In the application that contains your explanations about the right that you have as a personal data owner and that you request to exercise your rights mentioned above. If you are acting on behalf on behalf of someone else, you must have a power on this matter and document your power, and the application must contain the identity and address information and the documents confirming your identity must be attached to the application.

Applications to be made by you within this scope will be finalized within the shortest possible time and within 30 days. These applications are free of charge. However, if the process requires additional costs, the fee in the tariff determined by the Personal Data Protection Committee may be charged.

If the personal data owner submits his/her request to our Company in accordance with the prescribed procedure, our Company shall conclude the request free of charge within the shortest time and no later within thirty days according to the nature of the request. However, if the process requires a separate cost, the fee in the tariff determined by the Personal Data Protection Committee will be charged by our Company. Our company may require the relevant person any information to determine whether the applicant is a personal data owner or not. To clarify the matters set forth in the application of the personal data subject, our company may ask questions about the application of the personal data owner.

If our Company rejects your application, you find our answer inadequate or we do not respond to the application within the period, you can make a complaint to the Personal Data Protection Committee within thirty days from the date, when you learn response of our company and in any case within sixty days from the date of application pursuant to article 14 of the KVKK.

WHAT ARE THE CONDITIONS THAT THE DATA OWNERS CANNOT PROVIDE THE RIGHTS OF?

The personal data owners cannot claim the rights of personal data owners mentioned above in accordance with Article 28 of the KVKK, since the following cases are excluded from the scope of the KVKK.

- Processing of personal data for purposes such as research, planning and statistics by making it anonym with the official statistics.
- To process any personal data for art, history, literature or scientific purposes or within the scope of freedom of expression, without prejudice to national defense, national security, public security, public order, economic security, privacy or personal rights.
- To process any personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to provide national defense, national security, public security, public order or economic security.
- The processing of personal data by judicial authorities or enforcement authorities with respect to investigations, prosecutions, proceedings or executions.

Pursuant to Article 28/2 of the KVKK, the personal data subjects cannot claim any other rights listed in article 9 except for the right to claim damages in the following cases:

- If any necessary personal data is processed for crime prevention or crime investigation.
- Any personal data made public by the personal data owner is processed.
- If any personal data must be processed for performance of supervisory or regulatory duties, and for disciplinary investigation or prosecution by the authorized public institutions and organizations and professional organizations in the nature of public institutions based on the authority granted by law.
- If any personal data must be processed for the protection of the economic and financial interests of the State in relation to budget, tax and financial matters.

OTHER PROVISIONS

As explained in detail above, your personal data can be stored, classified according to market research, financial and operational processes and marketing activities, updated in different periods, and to the extent permitted by the legislation, within the framework of the laws and confidentiality principles, and transferred to any third persons and/or suppliers and/or services providers and/or foreign shareholders, to which we are affiliated as the service requires. Any information may be transferred, stored, reported and processed in electronic or hardcopy media in accordance with the policies bound by us with and other reasons foreseen by other authorities.

In case of any inconsistency between the provisions of the KVKK and other relevant legislation and this Policy, the provisions of the KVKK and other relevant legislation shall prevail.

This Policy prepared by our Company entered into force in accordance with the decision taken by the Board of Directors of Mesa Mesken.

We would like to remind you that we may make updates to this statement due to changes in legislation and changes in our company policies. We will publish the most current version of the statement on our website.

Before they enter the website, the User/Users agrees/agree, states/state and undertakes/undertake irrevocably that the User/Users has/have read this Personal Data Protection Policy, will comply with all provisions stated here, and the contents of the website and all the electronic media and computer records of our Company will deemed as definitive evidences pursuant article 193 of the Law of Civil Procedure.

APPENDIX - ABBREVIATIONS

ABBREVIATIONS	
Law No. 5651	Law on the Regulation of the Publications Made on the Internet and Combat Against Crimes Committed through these Publications that was published in the copy dated of May 23, 2007 and numbered 26530 of the Official Gazette, and entered into force.
Constitution	Constitution dated of November 7, 1982 and numbered 2709 of Republic of Turkey that was published in the copy dated of November 9, 1982 and numbered 17863 of the Official Gazette, and entered into force.
Application notice	Notice on the Procedures and Principles of Application to the Data Supervisor that was published in the copy dated of March 10, 2019 and numbered 30356 of the Official Gazette, and entered into force.
Relevant person/Relevant persons or data owner	A natural person, whose personal data is processed, such as any customers of Mesa Mesken company and/or its group companies under the structure of Mesa Mesken, and corporate companies, companies, business partners, shareholders, officers, candidate employees, trainees, visitors, third persons and other persons including, but not limited to, ones listed here, with whom the company employs or has a business relation.
Regulation on deletion, destruction and anonymization of personal data	Regulation on Deletion, Destruction and Anonymization of Personal Data that entered into force as of January, 2018 that was published in the copy dated of October 23, 2017 and numbered 30224 of the Official Gazette.
KVKK	Personal Data Protection Law that was published in the copy dated of April 7, 2016 and numbered 29677 of the Official Gazette, and entered into force.
KVK Committee	Personal Data Protection Committee
KVK Authority	Personal Data Protection Authority
Art.	Article
e.g.	Example
Policy	This Personal Data Protection Policy of Mesa Mesken
Company / Mesa Mesken	Mesa Mesken Sanayii A.Ş
Turkish Penal Law	Turkish Penal Law dated of October 12, 2004 and numbered 25611 that was published in the copy dated of September 4, 2004 and numbered 5237 of the Official Gazette and entered into force.