Mesa Mesken Protection of Personal Data and Privacy Statement

TABLE OF CONTENTS

As Mesa Mesken, we attach importance to the privacy and security of your personal data. In this context, we would like to inform you about how we process the personal data we obtain from our customers, suppliers, business partners, their employees and officials and all other third parties while we conduct our business relations, and for what purposes we use them and how we protect this information.

All concepts and expressions used in this privacy statement shall have the meaning ascribed to them in the Personal Data Protection Law No. 6698 ("**KVKK")** and other legislation. "You" in this privacy statement refers to you personally. The term personal data is used in a way that includes the sensitive personal data. The meanings of the terms and abbreviations in the Policy take place in the Annex – Abbreviations section.

We would like to remind you that if you do not accept the privacy statement, you should not submit your personal data to us. If you choose not to submit to us with your personal data, in some cases we will not be able to provide you with our services and respond to your requests or ensure the full functionality of our services.

We would like to remind you that it is your responsibility to ensure that the personal data transmitted by you to our company is accurate, complete and up-to-date as far as you know. Beyond that, if you share other people's data with us, it will be your responsibility to collect such data in accordance with local legal requirements. In this case, it will mean that you have obtained all necessary permissions from the third party in question to ensure us to collect, process, use and disclose their information, and our Company cannot be held responsible in this context..

ABOUT MESA MESKEN

Mesa Mesken started its journey in 1969 under the name of Mesa Mesken Sanayii with the aim of adding value to lives and creating "firsts" in its sector. The most important value of Mesa, which has achieved this goal in every field in which it has operated so far with the brave and innovative steps taken by it, is the happiness of hundreds of thousands of Mesa employees and their trust in the Mesa brand. Throughout journey, Mesa designed its buildings with all their components and created the concept of "brand in housing", which completely changed the approach to mass housing.

More than 100,000 residences in an inhabited area of 12,000,000 m2, which bears Mesa'nın signature at every stage of their production from initial design to delivery and post-delivery operation including infrastructure and environmental regulations, are the product of Mesa's uncompromising quality approach. Its staff, whose number has reached 4,500 today, adds more experience to Mesa's general knowledge and culture every day.

Mesa delivers the buildings constructed by it to its owners with an "Unconditional Customer Satisfaction Guarantee" and its "Customer Services Unit" also adds a new dimension to its quality service concept by instantly correcting any defects that may arise during the use phase. Mesa, with its "being first" feature in areas such as "Tunnel Formwork Technology", "Customer Services Unit" and "Housing Sites Service and Maintenance Service" that it has brought to the Turkish mass housing sector, draws strength from its past successes while it steps into new sectors and takes pride in producing a 50-year future by relying on the solidity of its principles.

As of 31.08.2022, the title of "Mesa Mesken Sanayii Anonim Şirketi" has been changed to "Mesa Holding Anonim Şirketi" and simultaneously a capital company titled Mesa Mesken İnşaat Anonim Şirketi was established through partial division within the body of Mesa Holding Joint Stock Company with its new title in accordance with the 159th and subsequent articles of the Turkish Commercial Code and the 19th article of the Corporate Tax Law.

The terms "we" or "Company" or "Mesa Mesken" in the privacy statement are related to the personal data processing activities carried out as a Data Controller by Mesa Mesken İnşaat A.Ş. ("**Mesa Mesken"),** which operates at address of Ihlamur Cad., No:2 Çayyolu, Çankaya/Ankara and is registered in the Ankara Trade Registry under the number 479300.

OUR PRINCIPLES RELATED TO PROCESSING OF PERSONAL DATA

All personal data processed by our company is processed in accordance with the KVKK and the relevant legislation. Pursuant to Article 4 of the KVKK, the basic principles and rules that we pay attention to when processing your personal data are explained below:

- **Processing in Accordance with the Law and the Rule of Honesty**: Our company acts in accordance with the principles brought by legal regulations and the general rule of trust and honesty in the processing of personal data. In this context, our Company takes into account the proportionality requirements in the processing of personal data and it does not use for purposes other than its intended purpose.
- **Ensuring that Personal Data is Accurate and Up-to-Date When Necessary**: Our company ensures that the personal data processed by it is accurate and up-to-date by taking into account the fundamental rights of personal data owners and their own legitimate interests.
- **Processing for Specific, Explicit and Legitimate Purposes**: Our company clearly and precisely determines the purpose of processing personal data that is in conformity with legitimate and lawful. Our company processes personal data in connection with the products and services it offers and to the extent necessary for the products and services in question.
- **Being Relevant, Limited and Proportionate to the Purpose for which they are Processed:** Our company processes personal data in a way that is suitable for the realization of the specified purposes and avoids the processing of personal data that is not related to the realization of the purpose or is not needed.
- **Retention for the Period Stipulated in the Relevant Legislation or Required for the Purpose for which they are Processed**: Our company retains personal data only until the period specified in the relevant legislation or until period required for the purpose for which they are processed. In this context, our Company first determines whether a period of time is stipulated for the storage of personal data in the relevant legislation, if a period is determined, it acts in accordance with this period, and if a period is not determined, it stores personal data for the period required for the purpose for which they are processed. In the event that the period expires or the reasons requiring its processing disappear, personal data is deleted, destroyed or anonymized by our Company.

CATEGORIES OF DATA OWNERS

The categories of data owners other than employees (including interns and subcontractor company employees), the personal data of which are processed by our company, are listed in the table below. A separate policy regarding the processing of our employees' personal data has been created and started to be implemented within the company. Persons outside the categories below may also submit their requests to our Company within the scope of KVKK, and the requests of these persons will also be evaluated within the scope of the Policy.

RELEVANT PERSON CATEGORY	DESCRIPTION
Customer	Real persons or legal entities purchasing our housings and services
Potential Customer	Real persons or legal entities who requested to benefit from our residences and/or services or who are interested in our residences or who are thought to have this interest in accordance with the rules of custom and honesty.
Visitor	Real persons who have entered the physical facilities (offices, construction sites, etc.) which belong to our company or where our company carried out an organization for various purposes or real persons who visit our websites
Third Person	Third party real persons (e.g. guarantors, companions, family members and relatives) who are associated with these persons to ensure the security of commercial transactions between our company and the above-mentioned parties or to protect the rights of the above-mentioned persons and to obtain benefits or all real persons (e.g. former employees) whose personal data must be processed by our Company even though it is not expressly stated within the scope of the Policy.
Employee Candidate / Intern Candidate	Real persons who have applied for a job in our company by any means or real persons who submitted to their CV and relevant information to enable our Company to review them
Group Company's Employee	Employees and representatives of Mesa group companies which are located at home and are members of our company
Employees, Shareholders and Officials of the Institutions with which we make collaboration	Real persons working in institutions with which our company has all kinds of business relations (including but not limited to project partners, suppliers and similar persons and institutions), including the shareholders and officials of these institutions

WHEN DO WE COLLECT PERSONAL DATA ABOUT YOU?

We collect your personal data mainly in the following cases:

- When you purchase or use our housings and/or services,
- When you sell goods or offer services to us,
- When you subscribe to our newsletters, when you prefer to receive our marketing messages,
- When you establish communication with us via our website, e-mail, social media platforms, other online channels or by phone,
- When you apply for a job at our company,
- When you participate in our company events and organizations,
- Indirectly, for example through the use of "cookies" and when we customize the software used to tailor the website to your specific preferences, or when we monitor your use of certain pages of the site (e.g. your IP address) or by other technical means that enable us to monitor your use of the site,
- When you establish communication with us as a potential customer/supplier/business partner/subcontractor for any purpose.

We will only process the personal data we obtain in the above cases in accordance with this privacy statement.

WHAT KINDS OF PERSONAL DATA DO WE PROCESS ABOUT YOU?

The personal data we process about you varies according to the type of business relationship between us (e.g. customer, supplier, business partner, etc.) and your method by which you contact us (e.g. telephone, e-mail, via the website, printed documents, etc.).

Essentially, our personal data processing methods consist of some situations when you participate in our business events, competitions, promotions and surveys or when you interact with us via telephone or email, through electronic applications specific to our customers by using our website. In this context, the personal data we process about you may be disclosed under the following categories:

Data Categories	**Samples**
ID information	Information included in identity documents such as name, surname, title, date of birth
Contact information	Email, phone number, address
Photos and/or videos that can determine your identification	Photo and video images and audio data processed for security reasons when you visit our company or when you participate in events organized by our company and visual data processed with CCTV recordings when you visit our company facilities
Financial data	Credit card data, bank account data, accommodation and spending information, invoice information
Any other information you voluntarily decide to share with Mesa Mesken	Personal data you share on your own initiative or feedback, opinions, requests and complaints, evaluations, comments which you send to us via social media, online platforms or other channels and our evaluations regarding them, uploaded files, areas of interest, our detailed review process before establishing a business relationship with you.
Electronic data collected automatically	When you visit or use our website or applications and when you subscribe to our news bulletins, or when you interact with us through other electronic channels, we may collect electronic data sent to us by your computer, mobile phone or other access device in addition to the information you directly transmit to us (e.g. device hardware model, IP address, operating system version andsettings, time and duration of your use of our digital channel or product, your actual location which may be collected when you activate location-based products or features, links you click, motion sensor data, etc.)
Legal action and compliance information	Your personal data processed within the scope of compliance with our legal obligations and our Company's policies due to determining and pursuing of our legal receivables and rights and paying of our debts, audit and inspection data

Data Categories	Samples
Corporate customer/Supplier data	As a result of the operations carried out by our business units within the framework of our services, information obtained and produced about the data owner such as the customer/supplier or the employee or authorized signatory employed within in the body of customer/supplier,
Incident management and security information	Information and evaluations collected regarding events that have the potential to affect our company, its 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	To the extent permitted by applicable laws and regulations, we may also collect your personal data through public domain databases, social media platforms, and methods and platforms where our business partners collect personal data on our behalf. For example, we may conduct any research about you from public domain sources to ensure the technical, administrative and legal security of our commercial activities and transactions before establishing a business relationship with you. In addition, it may be possible to transmit some personal data belonging to third parties to us by you. (e.g.personal data of guarantors, companions, family members, etc.). In order to manage our technical and administrative risks, we may process your personal data through methods used in accordance with generally accepted legal, commercial practices and honesty rules in these areas. In addition, we record the personal data you transmit to us on your own initiative via phone, website and similar platforms, and process them to resolve your requests and problems (e.g., when you call us and want to get information about our projects or submit your complaints).

PROCESSING OF PERSONAL DATA OF EMPLOYEE CANDIDATES

We collect personal data of Employee Candidates such as the school from where they graduated, previous work experience, disability status and similar personal data in addition to the personal data categories listed above to understand the candidate's experience and qualifications and to evaluate the suitability of the candidate for the open position, to check the accuracy of the information transmitted, if necessary, and to make research about the candidate by contacting third parties to whom the candidate has given his/her contact information, to establish communication with candidate in concern with the job application process, to recruit in accordance with the open position, to comply with legal regulations and to implement our Company's recruitment rules and human resources policies.

Personal data of employee candidates is processed through job application form in written and electronic media, our Company's electronic job application platform, applications sent to our Company physically or

by e-mail, employment and consultancy companies, interviews conducted in face-to-face or electronic environment, checks made about the employee candidate by our Company, recruitment tests conducted by human resources experts to evaluate the suitability of the candidate in the recruitment process.

Employee candidates are informed in detail in accordance with the KVKK with a separate document before submitting their personal data while applying for a job, and their explicit consent is obtained for the necessary personal data processing activities.

OUR POLICY ON COOKIES

For more information about how we use cookies and other tracking technologies, please read our Cookie Policy on www.mesa.com.tr. In general, "cookie" is a name given to information which is sent by an Internet service provider and then they are stored in a user's computer. The information contained in 'cookies' can be used when the user returns to the website in question. 'Cookies' can contain various information, including how many times the user has visited the site in question. By using individual session 'cookies' for each user, we can track how you use the site during a single session. Thanks to 'cookies', we can determine which browser you are using and offer you some special services.

The information stored in cookies may cover the date of visit, the time of visit, the pages viewed, the time spent in the Online Operations Center, and the sites visited just before or after the visit to the Online Operations Center. The data collected through these cookies used during your visit to the Online Transactions Center is evaluated and then advertisements regarding products with which you may be interested in potentially can be displayed when you visit other websites. It is possible to block cookies through your internet browser.

By using the "help" function which is available in most browsers, you can learn how you can prevent your computer from receiving 'cookies' and you can understand whether 'cookies' are sent or not and you can deactivate them completely. However, we would like to remind you that if you deactivate the 'cookies', you will not be able to use this site fully.
This site uses 'cookies' for various purposes, including:

- Access your certain information in order to provide personalized content to you after you enter into the Site;
- Tracking your preferences indicated when you use this site such as your preferred date and number formats. We value the privacy of your information. In order to protect the privacy and security of your confidential information at the highest possible level, we apply the following rules:
- This site does not constantly have 'cookies' on your disk drive. When you close your browser or leave the site, 'cookies' are removed.
- The information in all 'cookies' sent from this site to your computer is sent encrypted.

PROCESSING OF PERSONAL DATA OF OUR VISITORS IN OUR OFFICES AND FACTORIES

During the entry and exit procedures of visitors visiting the buildings and construction sites, our company processes personal data to ensure the physical security of our employees and visitors and to check workplace rules.In this context, in order to track visitor entry and exit, the names and surnames of our visitors are confirmed with their identities and the vehicle license plate is noted in the guest book at the locations deemed necessary. However, the identity card is not kept during the visitor's stay in the

company's offices and construction sites, and the identity is returned to the visitor after the aforementioned registration is made in the guest book. Before the visitor's information is obtained, he/she is informed about the processing of his/her personal data through a disclosure text at the security entrance. However, in this context, since our company has a legitimate interest, the explicit consent of the visitor is not obtained in accordance with Article 5/2/f of the KVKK. These data are only kept physically in the visitor registry and are not transferred to another environment unless there is a suspicious situation that threatens the security of the Company. However, this information can be used in cases such as preventing crime and ensuring the security of the Company. In addition, our Company may provide internet access to our visitors upon their request during their stay in our Company offices and construction sites to ensure security and to comply with the purposes specified in the Policy.

Log records obtained within this framework can only be accessed by a limited number of Mesa Mesken employees. Company employees, who have access to the aforementioned records, access these records only for use in requests or audit processes from authorized public institutions and organizations and share them with legally authorized persons.

PROCESSING OF PERSONAL DATA THROUGH CLOSED CIRCUIT CAMERA RECORDING

Security cameras are used to ensure the security of our company and facilities and personal data is processed in this way. Our company, within the scope of security camera monitoring activity, aims to increase the quality of the service provided, to ensure the safety of the company's physical campuses and to assure life and property safety of the people in the company, to prevent abuses, and to protect the legitimate interests of data owners.

Personal data processing activities carried out by our company with security cameras are conducted in accordance with the Constitution, 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 measured manner in connection with the purpose for which they are processed. Personal data is not subject to monitoring in a way that would interfere with a person's privacy beyond security purposes. In this context, warning signs are placed in common areas where CCTV is recorded and in this way data owners are informed. However, due to the fact that our Company has a legitimate interest in keeping CCTV records, data owners' explicit consent is not obtained. In addition, in accordance with Article 12 of the KVKK, necessary technical and administrative measures are taken to ensure the security of personal data obtained as a result of CCTV monitoring activities.

In addition, a procedure has been prepared regarding the areas with CCTV cameras, the monitoring areas of the cameras, and the duration of keeping records, and it has been started to be implemented in our Company. This procedure is taken into account before the CCTV camera is placed and the camera is then placed. It is not allowed to place cameras that exceed the security purpose and the privacy of individuals. Only a certain number of Company personnel have access to CCTV camera footage and these authorizations are regularly reviewed. Personnel, who have access to these records, sign a commitment stating that they will protect personal data in accordance with the law.

The entrance doors, building exterior, dining hall, visitor waiting room, parking lot, security booth and floor corridors in our company offices and construction sites are recorded visually through the security

cameras in the service area in order to ensure the security of the building, and the recording process is supervised by the relevant units.

FOR WHAT PURPOSES DO WE USE YOUR PERSONAL DATA?

The purposes for which we use your personal data vary depending on the type of business relationship between us (e.g. customer, supplier, business partner, etc.). Our basic purposes for processing your personal data are listed below. Personal data processing activities regarding Employee Candidates are explained under the "Processing of Personal Data of Employee Candidates" section specified above.

Our Personal Data Processing Purposes	**Samples**
Evaluating potential suppliers/business partners	Pursuant to our risk rules, conducting our review and conflict of interest process, managing the purchase and sale process of real estate, negotiating with you for the purpose of establishing construction contracts in return for flats, conducting location, function and feasibility studies of the relevant real estate and checking official documents, issuing relevant official documents such as powers of attorney and for this purpose carrying out the relevant process before the notary, fulfilment of license transactions, signing and executing of contracts, managing of the process such as establishing floor easement, obtaining the occupancy permit and carrying out the transactions of transition to flat ownership and type change and establishing easement rights and carrying out the transfer of title deed before public institutions and organizations such as the Land Registry Directorate and carrying out accounting, invoicing and payment transactions, protecting our rights and obligations on real estate, collecting contractual and commercially necessary documents.
Establishing and managing customer relationships	Carrying out the deposit processes for the projects in which you are interested, establishing real estate sales promise contracts with you, receiving flat requests, filling out the slip of paper, delivering flats and transferring title deeds, establishing subscriptions, making payment plans, managing processes with banks regarding tied loans, managing processes related to promissory notes, transfer of real estate sales promise contracts, conducting the processes such as name change or its termination, carrying out works and transactions arising from the Law on Consumer Protection, fulfillment of invoicing and payment transactions, collecting contractual and commercially necessary documents, meeting your demands, ensuring legal and commercial transaction security, making offers regarding our projects. submission, invoicing, contract establishment and execution, ensuring legal transaction security after the contract enters into force, developing products and services, determining and implementing our Company's commercial and business strategies with the evaluation of new technologies and applications, managing operations (request, offer, evaluation, order, budgeting, contract),product/project/manufacturing/investment quality processes and operations, in-company system and application management operations, finance operations, management of financial affairs

Our Personal Data Processing Purposes	**Samples**
Execution and finalization of the contract process with our suppliers/business partners	Procurement of goods and services, providing and invoicing of the shipment of goods and samples, management of the registration process to our website applications, establishment and execution of contracts, management of logistics processes, ensuring legal transaction security after the contract is signed, ensuring the shipment of goods and samples, managing logistics processes, improving, developing, diversifying our products and services and offering alternatives to legal/real persons with whom they have commercial relations, developing the products and services, determination and implementation of our Company's commercial and business strategies through the evaluation of new technologies and applications, managing operations (request, offer, evaluation, order, budgeting, contract), product/project/manufacturing/investment quality processes and operations, in-company system and application management operations, finance operations, management of financial affairs
Execution of direct marketing processes	To make marketing notifications regarding our services via e-mail, telephone and SMS, to conduct satisfaction surveys or to evaluate and respond to your opinions, complaints and comments which you made via social media, online platforms or other channels, to inform our customers about company innovations, campaigns and promotions, and to periodically carrying out campaign activities, to design special promotional activities for customer profiles and to conduct advertising, promotion and marketing activities to be created through customer "classification" and personal information in order to prevent the transmission of unsolicited e-mails, to determine and implement our company's commercial and business strategies and to plan organization
Communication and support (based on 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, fulfilling our legal obligations arising from relevant legislation, especially the Law No. 5651 and other legislation, the Law No. 6563 on the Regulation of Electronic Commerce and other legislation, the Turkish Penal Code No. 5237 and Law No. 6698 on Protection of the Personal Data, carrying out the necessary processes before especially land registry offices and official institutions, obtaining project licenses, auditing and inspections of official authorities, following up and concluding our legal rights and lawsuits, disclosing data upon the request of official

Our Personal Data Processing Purposes	Samples
	authorities within the scope of compliance with the laws and regulations to which we are subject and ensuring that the legal obligations specified in the KVKK and required by legal regulations with regulatory and supervisory institutions are fulfilled within the scope of determined requirements and obligations,
Protecting company interests and ensuring security	Carrying out the necessary auditing activities to protect the company's interests and benefits, performing conflict of interest checks, ensuring the legal and commercial security of people who have business relations with our Company, keeping CCTV records to protect the company's devices and assets, taking technical and administrative security measures, conducting satisfaction surveys after accommodation, execution of the necessary work to improve the services we offer, implementing and inspecting workplace rules, managing quality processes, planning and executing social responsibility activities, protecting the commercial reputation and trust of Mesa Mesken group companies, reporting of all incidents, accidents, complaints, lost, stolen and similar situations occurring on the construction site and in the building and performance of the necessary intervention in this regard, taking precautions in concern with these matters, transfer of the rules to be followed in case of dangerous situations that may occur during maintenance and repair and measuring the professional competencies of subcontractors, ensuring the orderliness of the entrance and exit of the company employees and obtaining the necessary information in terms of security, carrying out the necessary quality and standard inspections or fulfilling our reporting and other obligations determined by laws and regulations
Planning and execution of company commercial activities	In accordance with budgeting activity, determining, planning and implementing the Company's short, medium and long term commercial policies and determining and implementing commercial and business strategies, execution of communication, market research and social responsibility activities carried out by our company and purchasing affairs
Reporting and auditing	Ensuring communication with Mesa group companies in the country and carrying out the necessary activities, implementation of internal audit and reporting processes
Protection of rights and interests	Making defense against lawsuits, investigations and similar legal claims filed against our company

HOW DO WE USE YOUR PERSONAL DATA FOR MARKETING PURPOSES?

As a rule, we always obtain your consent to process your personal data within the scope of marketing activities, as marketing activities are not considered within the scope of the exceptions regulated in Article 5/2 and Article 6/3 of the KVKK. Our company may periodically send you promotional communications about its products, services, events and promotions. Such promotional communications may be sent to you through different channels such as email, telephone, SMS text messages, postal mail, and third-party social networks and online platforms.

In order to provide you with the best personalized experience, sometimes these communications may be tailored according to your preferences (for example, as you indicate them to us, based on the conclusions we obtained from your website visits, or based on the links you click in our emails and rejection notification via SMS).
Based on your consent, we can carry out marketing activities for processing with the purpose of offering of opportunities for products and services specific to you such as internet advertisement targeting, re-targeting, cross-selling, campaigns, opportunities and product/service advertisements, using the Cookies for this purpose, making commercial offers by considering your preferences and recent purchases, in addition to these matters, a tracking your usage habits according to your previous records and offering you special products during your visit to [the Mesa Corporate website, project websites, blog site, social media, mesa and life mobile applications]; providing you with special advertisements, campaigns, advantages, information and other benefits for sales and marketing activities and processing of them for the purpose of carrying out other marketing and CRM activities, processing for the purpose of creating new product and service models, processing of electronic commercial messages (such as campaigns, e-bulletins, mailing, customer satisfaction surveys, product and service advertisements), sending gifts and promotions, establishment of corporate communication and organizing other events and invitations within this scope and providing information about them.

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

If you log into 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 receiving marketing-related communications (you can find contact details in the "What Are Your Rights Regarding Your Personal Data?" section taking place below).

FOR WHAT LEGAL REASONS DO WE PROCESS YOUR PERSONAL DATA?

We process your personal data within the framework of the following legal reasons in accordance with the relevant provisions of the Turkish Commercial Code No. 6102, the Turkish Code of Obligations No. 6098, the Tax Procedure Law No. 213, the electronic commerce legislation and Article 5 of the KVKK.

Legal reason	**Samples**
We process based on your consent in cases where we are required to obtain your explicit consent in accordance with KVKK and other legislation (In this case, we would like to remind you that you can withdraw your consent at any time)	We obtain your consent to carry out our marketing activities.

Legal reason	**Samples**
In any case permitted by applicable legislation	Writing the name of the relevant person on the invoice within the scope of Article 230 of the Tax Procedure Law
When there is an obligation to protect the vital interests of any person	Giving the health information of the member of board of directors, who fainted in the meeting of board of directors, to the doctor
In case that we need to establish a contract with you, to implement the contract and to fulfill our obligations under a contract.	Obtaining the customer's bank account information within the scope of the contractual relationship with the customer
Fulfilling our legal obligations,	Fulfilling our tax obligations, submitting the information requested by court decision to the court
In case that your personal data has been made public by you	Transmission to us of your e-mail address so that we can contact you, entering of contact information of the employee candidate on the website where job applications are collected and using personal data that you have made public through means such as social media channels for the purpose of making them public
In case that it is necessary for us to process data for the establishment or protection of a right or in the event that we need to exercise our legal rights and defend against legal claims filed against us.	Keeping documents that serve as proof/evidence and using them when necessary
In cases where our legitimate interests require it, provided that it does not harm your fundamental rights and freedoms.	To ensure the security of our company communication networks and information, to carry out our company activities, to detect suspicious transactions and conduct research to comply with our risk rules, to benefit from storage, hosting, maintenance and support services in order to provide technical and security IT services, to ensure the efficiency of our company activities and to benefit from cloud technology in order make use of the opportunities of technology.

In cases where your Personal Data is processed with your explicit consent, we would like to emphasize that if you withdraw your explicit consent, you will be removed from the commercial membership

program where the processing based on explicit consent is required and you will not be able to benefit from the advantages you have used due to such processing as of the relevant date.

WHEN DO WE SHARE YOUR PERSONAL DATA?

Transfer of Personal Data in Turkey

Our company is under the responsibility of acting in accordance with the decisions and relevant regulations stipulated in the KVKK, especially Article 8 of the KVKK, regarding the transfer of personal data. As a rule, personal data and sensitive data belonging to data owners cannot be transferred to other real persons or legal entities by our Company without the explicit consent of the person concerned.

In addition, in cases stipulated in Articles 5 and 6 of the KVKK, transfer is possible without the consent of the person concerned. Our company can be transferred personal data to third parties in Turkey and companies under the roof of Mesa Mesken in accordance with the conditions stipulated in the KVKK and other relevant legislation and by taking the security measures specified in the legislation; (If there is a current contract signed with the data owner in the contract in question) unless otherwise regulated by the law or other relevant legislation.

Transfer of Personal Data Abroad

Our company may transfer personal data to third parties in Turkey and in addition, our company may transfer personal data abroad by processing them in Turkey as stated above and in accordance with the conditions stipulated in the Law and other relevant legislation and by taking the security measures specified in the legislation including outsourcing to process and storage outside Turkey. In order to carry out our company activities in the most efficient way and to benefit from the opportunities of technology, we transfer your personal data abroad by taking the necessary technical and administrative measures via cloud computing technology.

Pursuant to Article 9 of the KVKK, as a rule, we seek the explicit consent of the data owners for the transfer of personal data abroad. However, pursuant to Article 9 of the KVKK, personal data may be transferred abroad without seeking the explicit consent of the data owner provided that one of the conditions set out in Article 5/2 or Article 6/3 of the KVKK is present and

a) If there is an adequate protection in the foreign country to which the personal data will be transferred,
b) In the absence of adequate protection, provided that data controllers in Turkey and in the relevant foreign country must undertake an adequate protection in writing and have the permission of the Board.

Accordingly, in exceptional cases where explicit consent is not sought for the transfer of personal data mentioned above, our Company requires adequate protection in the country where the data will be transferred in accordance with the KVKK, in addition to the conditions of processing and transfer without consent. The Personal Data Protection Board will determine whether adequate protection is provided or not and in case of the absence of adequate protection, data controllers both in Turkey and in the relevant foreign country must undertake an adequate protection in writing and it is required to obtain the permission of the Personal Data Protection Board

Parties Sharing at Home and Abroad

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

- **Mesa group companies**: Since we operate under the Mesa group of companies, your data may be shared with Mesa group companies established in Turkey or these data may be opened to access of the companies in question. This sharing will only be made with authorized employees in the relevant Mesa group company. In some special cases, it may be possible for us to share personal data instead of sharing anonymous information with Mesa group companies. Mesa Mesken Data Sharing Agreement has been signed regarding the transfer of your personal data to Mesa group companies and necessary measures have been implemented.

- **Service providers and business partners**: While our Company carries out its commercial activities, it defines the parties with whom it establishes business partnerships for purposes such as sales, promotion and marketing of our Company's services, and after-sales support. Like many businesses, we may work with reliable third parties such as information and communication technology providers, consultancy services providers, cargo companies, travel agencies in order to carry out functions and services in the most efficient way and in accordance with current technologies within the scope of some data processing activities, and in this context, we may share data in question to carry out our activities. This sharing is made on a limited basis to ensure that the purposes of establishing and implementation of the business partnership are fulfilled. Our company uses cloud computing technologies to carry out its activities in the most efficient way and to benefit from the opportunities of technology at the maximum level, and in this context, it can process your personal data at home and abroad through companies that provide cloud computing services. The marketing services support company with which we may make sharing may be established abroad, and in this context, data is shared abroad in accordance with the provisions regarding data sharing abroad in accordance with Articles 8 and 9 of the KVKK.

- **Public authorities**: When required by law or when we need to protect our rights, we may share your personal data with the relevant official, judicial and administrative authorities (eg. Land Registry Offices, tax offices, law enforcement agencies, courts and enforcement offices).

- **Private law persons:** In accordance with the provisions of the relevant legislation, personal data can be shared limited to the purpose requested by private law persons authorized to receive information and documents from our Company within their legal authority (e.g. Occupational Health and Safety Company).

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

- **Other parties in connection with corporate transactions**: From time to time, we may share your personal data in order to carry out corporate transactions, such as the sale of a business owned by our company, reorganization, merger, joint venture, or other disposition of our business, assets, or stock certificates (including in connection with any bankruptcy or similar proceeding).

HOW LONG DO WE KEEP YOUR PERSONAL DATA?

We only keep your personal data for as long as necessary to fulfil the purpose for which it was collected. We determine these periods separately for each business process, and if there is no other reason why we

need to keep your personal data at the end of the relevant periods, we destroy and/or anonymize your personal data in accordance with the KVKK.

When determining the destruction and/or anonymization periods of your personal data, we take into account the following criteria:

- Within the scope of the purpose of processing the relevant data category, the period accepted as a general practice in the sector in which the data controller operates,
- The period for which the legal relationship established with the person concerned will continue and which necessitates the processing of personal data in the relevant data category,
- Depending on the purpose of processing the relevant data category, the period during which the legitimate interest to be obtained by the data controller will be valid in accordance with the law and good faith,
- The period for which the risks, costs and responsibilities arising from the storage of the relevant data category depending on the purpose of processing will continue legally,
- Whether the maximum period to be determined is suitable for keeping the relevant data category as accurate and up-to-date when necessary,
- The period for which the data controller is obliged to keep the personal data in the relevant data category due to its legal obligation,
- The statute of limitations determined by the data controller for the assertion of a right related to personal data in the relevant data category.

HOW DO WE DESTROY YOUR PERSONAL DATA?

In accordance with Article 138 of the Turkish Penal Code and Article 7 of the KVKK, although personal data has been processed in accordance with the provisions of the relevant law, in the event that the reasons requiring its processing disappear, it is deleted, destroyed or anonymized upon our Company's own decision or if the personal data owner requests it.

In this context, the Personal Data Retention and Destruction Policy has been prepared. In cases where our company has the right and/or obligation to preserve personal data in accordance with the provisions of the relevant legislation, it has the right not to fulfill the request of the data owner. When personal data is processed non-automatically, provided that it is a part of any data recording system, a system of physical destruction of personal data is applied in a way that cannot be used later while the data is deleted /destroyed. When our company agrees with a person or organization to process personal data on behalf of it, personal data is securely deleted by these persons or organizations in a way that cannot be recovered. Our company can anonymize personal data when the reasons requiring the processing of personal data processed in accordance with the law disappear.

METHODS OF DESTRUCTION OF PERSONAL DATA

Deletion of Personal Data

Although it has been processed in accordance with the provisions of the relevant law, our company may delete personal data at its own discretion or upon the request of the personal data owner in the event that the reasons requiring its processing disappear. Deletion of personal data is a process through which personal data is made inaccessible and unusable for the relevant users in any way. Our company takes all necessary technical and administrative measures to ensure that the deleted personal data is inaccessible and non-reusable for the relevant users.

Process of Deletion of Personal Data

The process to be followed in the deletion of personal data is as follows:

- Determination of personal data that will form the subject of deletion process.
- Identification of relevant users for each personal data using an access authorization and control matrix or a similar system.
- Determining the authorizations and methods of the relevant users such as access, retrieval, reuse.
- Closure and elimination of the access, retrieval, reuse authorizations and methods of the relevant users within the scope of personal data.

Method of Deletion of Personal Data

Data Recording Environment	Description
Personal Data Taking Place Servers	If the period requiring the storage of personal data on the servers expires, its administrator removes the access authorization of the relevant users and deletes them.
Personal Data Taking Place in Electronic Media	If the period requiring the storage of personal data in the electronic environment expires, it becomes inaccessible and unusable for other employees (relevant users) except the database administrator.
Personal Data Taking Place in Physical Environment	If the period requiring the storage of personal data kept in the physical environment expires, it becomes inaccessible and unusable for other employees except the unit manager responsible for the document archive. In addition, blackening process is also applied by drawing/painting/erasing on it to ensure that it cannot be read.

Destruction of Personal Data

Our company may destroy personal data, based on its own decision or upon the request of the personal data owner, if the reasons requiring processing are eliminated, even though they have been processed in accordance with the provisions of the relevant law. Destruction of personal data is a process through which personal data is made inaccessible, irretrievable and unusable by anyone. The data controller is obliged to take all necessary technical and administrative measures regarding the destruction of personal data.

Data Recording Environment	Description
Personal Data Taking Place in Electronic Media	If the period reuqiring the storage of personal data as paper expires, they are irreversibly destroyed in paper shredding machines.
Personal Data Taking Place in Optical and Magnetic Environment	If the period reuqiring the storage of personal data on optical media and magnetic media expires, they are physically destroyed such as melting, burning or pulverizing, and the data on them is made unreadable.

Physical Destruction: Personal data can also be processed non-automatically, provided that it is a part of any data recording system. While deleting/destroying such data, the system of physical destruction of personal data is applied in a way that cannot be used later.

Secure Deletion from Software: When deleting/destroying data processed by fully or partially automated means and stored in digital media, methods are used to delete the data from the relevant software so that it cannot be recovered again.

Secure Deletion by Expert: In some cases, it may agree with an expert to delete personal data on its behalf. In this case, personal data is securely deleted/destroyed by the person, who is an expert in this field, in a way that cannot be recovered.

Blackening: It is to make personal data physically unreadable.

Anonymization of Personal Data

Anonymization of personal data means to ensure that personal data cannot be associated with an identified or identifiable real person in any way, even if personal data is matched with other data. Our company can anonymize personal data when the reasons requiring the processing of personal data processed in accordance with the law disappear. In order for personal data to be anonymized; it must be ensured that personal data cannot be associated with an identified or identifiable real person in any way even through the use of appropriate techniques in terms of the environment and the relevant field of activity such as returning personal data by the data controller or recipient groups and/or matching the data with other data. Our company takes all necessary technical and administrative measures to anonymize personal data.

Personal data anonymized in accordance with Article 28 of the KVK Law may be processed for purposes such as research, planning and statistics. Such processing is outside the scope of the KVK Law and the explicit consent of the personal data owner will not be sought.

Methods of Anonymization of Personal Data

Anonymization of personal data means to ensure that personal data cannot be associated with an identified or identifiable real person in any way, even if personal data is matched with other data.

In order for personal data to be anonymized; it must be ensured that personal data cannot be associated with an identified or identifiable real person in any way even through the use of appropriate techniques in terms of the environment and the relevant field of activity such as returning personal data by the data controller or third parties and/or matching the data with other data. Anonymization means the preventing the determination of identification of the person concerned or losing the ability to distinguish personal data within a group or crowd in a way that cannot be associated with a real person by removing or replacing all direct and/or indirect identifiers in a data set. Data, which does not point to a specific person as a result of blocking or losing these features, is considered anonymized data. In other words, anonymized data is information that identifies a real person before this transaction is made, After this process, it can no longer be associated with the relevant person and its connection with the person has been broken. The purpose of anonymization is to break the connection between the data and the person identified by this data. All breaking the connection processes carried out by using methods such as grouping, masking, derivation, generalization, randomization, whether automatic or non-automatic, applied to the records in the data recording system where personal data are kept, are called anonymization methods. The data obtained as a result of the application of these methods must not be able to identify a specific person.

Examples of anonymization methods are described as follows:

Anonymization Methods That Do Not Provide Value Irregularity: In methods that do not provide value irregularity, no change or addition or subtraction is applied to the values belonging to the data in the set, instead, changes are made to all of the rows or columns in the set. Thus, while a change occurs in the data in general, the values in the fields maintain their original state.

Removing Variables

It is an anonymization method provided by completely deleting one or more of the variables from the table. In such a case, the entire column in the table will be completely removed. If the variable is a high-grade identifier and there is no more suitable solution and the variable is too sensitive to be disclosed to the public, or it does not serve analytical purposes this method can be used

Extracting Records

In this method, anonymity is strengthened by removing a line containing a singularity in the dataset and the possibility of producing assumptions about the dataset is reduced. Generally, the extracted records are ones that do not have a common value with other records and that people who have an idea about the dataset can easily guess. For example, in a dataset where survey results take place, 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 removing the "sector" variable from all survey results.

Regional Hiding

The goal of regional hiding is to make the dataset more secure and reduce the risk of predictability. If the combination of values for a particular record creates a situation that is barely visible, and this is likely to cause that person to become distinguishable in the relevant community, the value that created the exceptional situation is changed to "unknown".

Generalization

It is the process of translating relevant personal data from a private value to a more general value. It is the most used method when producing cumulative reports and operations carried out on total figures. As a result of the new values obtained show the total values or statistics of a group which make it impossible to reach a real person. For example, a person with a TR Identity Number 12345678901 buys diapers from the e-commerce platform and also buys wet wipes. In the anonymization process, it can be reached conclusion that xx% of the people, who buy diapers from the e-commerce platform, also buy wet wipes by using the generalization method.

Lower and Upper Limit Coding

The upper and lower limit coding method is obtained by defining a category for a certain variable and combining the values in the grouping created by this category. Generally, the lower or higher values in a certain variable are collected together and a new definition is made to these values and thus proceeding is provided.

Global Coding

The global coding method is a grouping method used in datasets to which lower and upper limit coding cannot applied and that do not contain numerical values or that have values that cannot be sorted numerically It is generally used when certain values facilitate to make predictions and assumptions by clustering. A common and new group is created for the selected values, and all records in the dataset are replaced with this new definition.

Sampling

In the sampling method, instead of the whole data set, a subset taken from the set is disclosed or shared. In this way, the risk of producing accurate predictions about people is reduced, since it is not known whether a person known to be in the entire dataset is included in the disclosed or shared sample subset. Simple statistical methods are used to determine the subset to be sampled. For example; in case that a dataset on the demographic information, occupations and health status of women living in Istanbul is anonymized and disclosed or shared, it may be meaningful to scan in the relevant dataset about a woman known to live in Istanbul and to make a guess about this subject. However, if only the records of women whose registered province is Istanbul are left in the relevant dataset, and those whose population records are in other provinces are removed from the dataset and anonymization is applied and the data is disclosed or shared, since a malicious person who accesses the data cannot guess whether the civil registry of a woman, who he/she knows that she lives in Istanbul is registered in Istanbul or not, he/she will not be able to make a reliable guess about whether the information about this person is included in the data.

Anonymization Methods That Provide Value Irregularity: Unlike the methods mentioned above with the methods that provide value irregularity; By changing the existing values, the values of the dataset are distorted. In this case, since the values of the records change, the planned benefit from the dataset must be calculated correctly. Even if the values in the dataset are changing, it is still possible to benefit from the data by ensuring that the total statistics are not corrupted.

Micro Consolidation

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

Data Exchange

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

Adding Noise

With this method, additions and subtractions are made to provide distortions to the specified extent in a selected variable. This method is mostly applied to datasets that contain numeric values. Distortion is applied equally at each value.

Statistical Methods to Strengthen Anonymization

As a result of the combination of some values in the records with individual scenarios in anonymized datasets, it may be possible to identify the people in the records or to derive assumptions about their personal data.

For this reason, by using various statistical methods in anonymized data sets, the singularity of the records in the data set is minimized and thus anonymity can be strengthened. The main purpose of these methods is to minimize the risk of anonymity and to keep the benefit to be obtained from the data set at a certain level.

Anonymity

In anonymized datasets, the fact that the identities of the people in the records can be determined or the fact that the information about a particular person can be easily predicted has shaken the trust in anonymization processes in the event that indirect identifiers come together in the right combinations.

Accordingly, it was necessary to make the datasets anonymized by various statistical methods more reliable. K-anonymity has been developed to prevent the disclosure of information specific to individuals who show sibguler characteristics in certain combinations by enabling the identification of more than one person with certain fields in a dataset. If there is more than one record of combinations created by combining some of the variables in a data set, the probability of determination of identifications of the people who correspond to this combination decreases.

Diversity

The L-diversity method, which is formed by studies carried out on the deficiencies of anonymity, takes into account the diversity of sensitive variables that correspond to the same variable combinations.

Proximity

Although the diversity method provides diversity in personal data, there are situations where it cannot provide adequate protection because the method in question does not deal with the content and sensitivity of personal data. In this way, the process of calculating the degree of closeness of personal data and values in themselves and anonymizing the dataset by dividing it into subclasses according to these degrees of closeness in question is called the T-proximity method.

Selecting the Anonymization Method

When our company decides which of the above methods will be applied, it decides by looking at the data it has and taking into account the following features of the data set it has:

The nature of the data,
The size of the data,
The structure of the data in physical environments,
Diversity of data,
The benefit to be obtained from the data / the purpose of processing,
Frequency of data processing,
Reliability of the party to which the data will be transferred,
The fact that the effort to be spent on anonymizing the data is meaningful,

The magnitude of the damage that may occur in case of deterioration of the anonymity of the data, the area of its impact,
The distributed/centrality ratio of the data,
Users' access authorization control to the relevant data, and
The fact that an attack is designed to disrupt anonymity and the possibility that the effort to be spent to implement this attack will be meaningful.
While anonymizing a data, our company checks whether the data in question identifies a person again through contracts and risk analyses to be performed by it by using information known to be within other institutions and organizations to which personal data is transferred or publicly available information.

Anonymity Assurance

When our company decides to anonymize personal data instead of deleting or destroying it, it shows the necessary attention to ensure that the anonymity of the anonymized data set is not deteriorated by combining it with another data set and to ensure that one or more values do not form a meaningful whole that can make a record singular, and to ensure that the values in the anonymized data set do not combine and produce an assumption or conclusion. As long as the features listed in this article change in the data sets anonymized by our company, necessary checks are carried out and it is ensured that anonymity is protected.

Risks Related to Disruption of Anonymization by Making Inverse Processing of Anonymized Data

Since anonymization is the process of destroying the distinctive and identifying features of the dataset applied to personal data, there is a risk that these processes will be reversed by various interventions and that the anonymized data will become re-identifying and distinguishing real persons. This is referred to as a breakdown of anonymity. Anonymization can only be achieved through manual processes or automated processes, or hybrid processes consisting of a combination of both types of transactions. But the important matter is to take measures to prevent the disruption of anonymity by new users who can access or possess the data after the anonymized data is shared or disclosed. Actions carried out consciously to disrupt anonymity are called "attacks aimed at disrupting anonymity". In this context, our Company investigates whether there is a risk of reversing anonymized personal data through various interventions and whether there is a risk that anonymized data can be re-identified and distinguish real persons and necessary action is established in accordance with this situation.

HOW DO WE PROTECT YOUR PERSONAL DATA?
In order to protect your personal data and prevent unlawful access, necessary administrative and technical measures are taken by our Company in line with the Personal Data Security Guide published by the KVK Authority and necessary procedures are regulated within the Company and disclosure and explicit consent texts are prepared, and necessary audits are carried out to ensure the implementation of the provisions of the KVKK in accordance with Article 12/3 of the KVKK or these transactions are carried out by getting services from outside the company. The results of these audits are evaluated within the scope of the internal functioning of the Company and necessary activities are carried out to improve the measures taken.

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

Technical Measures

We use generally accepted standard technologies and business security methods, including 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. Depending on the current state of technology, the cost of technological application and the nature of the data to be protected, we take technical and administrative measures to protect your data from risks such as destruction, loss, falsification, unauthorized disclosure or unauthorized access. In this context, we conclude contracts regarding data security with the service providers with which we work. You can find detailed information about these service providers via [related link].

1) Ensuring Cyber Security: We use cyber security products to ensure personal data security, but the technical measures we take are not limited to this. With measures such as firewalls and gateways, the first line of defence is created against attacks from environments such as the internet. However, almost every software and hardware are subjected to a number of installation and configuration processes. Considering that some commonly used software, especially its older versions, may have documented security vulnerabilities, unused software and services are removed from the devices. For this reason, deleting unused software and services instead of keeping them up-to-date is primarily preferred due to its convenience. With patch management and software updates, it is ensured that the software and hardware work properly and that the security measures taken for the systems are regularly checked whether they are sufficient.

2) Access Limitations: Access authorizations to systems containing personal data are limited and they are regularly reviewed. In this context, employees are granted access authority to the extent necessary for their work and duties, powers and responsibilities, and access to the relevant systems is provided by using a crypto and password. While creating the cryptos and passwords in question, it is ensured that combinations of capital letters and small letters, numbers and symbols are preferred instead of numbers or letter sequences that are associated with personal information and can be easily guessed. Accordingly, an access authorization and control matrix are created.

3) Encryption: In addition to the use of strong crypto and passwords, access is limited by methods such as limiting the number of password entry attempts, changing cryptos and passwords at regular intervals, opening the administrator account and admin authority to be used only when necessary, and deleting the account or closing the logins without wasting time for employees whose relations with the data controller are terminated in order to protect against common attacks such as the use of brute force algorithm (BFA).

4) Anti-Virus Software: In order to be protected from malware, products such as antivirus and antispam, which regularly scan the information system network and detect dangers, are used, and they are kept up-to-date and the necessary files are regularly scanned. If personal data is to be obtained from different websites and/or mobile application channels, it is ensured that the connections are made via SSL or a more secure way.

5) Monitoring of Personal Data Security: Checking which software and services are running in information networks and determining whether there is an infiltration or movement that should not be in information networks and keeping a regular record of all users' transaction movements (such as log

records) and reporting security problems as quickly as possible are carried out. Again, an official reporting procedure is established for employees to report security vulnerabilities in systems and services or threats using them. Evidences are collected and stored securely in undesirable events such as collapse of information system, malicious software, out of service attack, incomplete or incorrect data entry, violations of confidentiality and integrity, and abuse of the information system.

6) Ensuring the Security of Environments Containing Personal Data: If personal data is stored on devices located in the premises of data controllers or in paper environment, physical security measures are taken against threats such as theft or loss of these devices and papers. Physical environments containing personal data are protected against external risks (fire, flood, etc.) with appropriate methods and entrances / exits to these environments are controlled.

   If personal data is in electronic environment, access between network components can be limited or separation of components is provided in order to prevent personal data security breaches. For example; if the network being used is limited to a certain section reserved for this purpose and personal data is processed in this area, available resources can be allocated only to ensure the security of this limited area rather than the entire network.

   The same level of precautions is also taken for paper environment, electronic environment and devices which are located outside the Company's campus and contains personal data belonging to the Company. As a matter of fact, although personal data security breaches often occur due to theft and loss of devices containing personal data (laptop, mobile phone, flash disk, etc.), personal data to be transferred by e-mail or mail is also sent carefully and by taking adequate precautions. In the event that employees access the information system network with their personal electronic devices, adequate security measures are taken for them.

   In cases such as loss or theft of devices containing personal data, the method related to using of the access control authorization and/or encryption methods is applied. In this context, the password key is stored in an environment that can only be accessed by authorized persons and unauthorized access is prevented.

   Paper documents containing personal data are also stored in a locked manner and in environments that can only be accessed by authorized persons and unauthorized access to these documents are prevented.

   Pursuant to Article 12 of the KVKK, our company notifies the KVK Board and data owners as soon as possible if personal data is obtained by others illegally. If the KVK Board deems it necessary, it may announce this situation on its website or by any other method.

7) Storage of Personal Data in the Cloud: In the event that personal data is stored in the cloud, the Company evaluates whether the security measures taken by the cloud storage service provider are sufficient and appropriate. Access to data storage areas where personal data is stored is logged, and inappropriate access or access attempts are instantly communicated to the relevant parties.

8) Procurement, Development and Maintenance of Information Technology Systems: Security requirements are taken into account when determining the needs related to the procurement, development or improvement of current systems by the company.

9) Backup of Personal Data: In cases where personal data is damaged, destroyed, stolen or lost for any reason, the Company ensures to operate as soon as possible by using the backed-up data. Backed-up personal data can only be accessed by the system administrator, and data set backups are kept outside the network.

Administrative Measures

- All activities carried out by our company have been analysed in detail for 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 by taking into account 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 checks are carried out in this context.
- Our company may receive services from external service providers from time to time in order to meet its information technology needs. In this case, the transaction is carried out by making sure that the external service providers processing the Data in question provide at least as much as the security measures provided by our Company. In this case, a written contract is signed by the Data Processor and this contract includes at least the following issues:
    - The Data Processor will only act in accordance with the instructions of the Data Controller and the purpose and scope of data processing specified in the contract and the KVKK and other legislation,
    - The Data Processor will act in accordance with the Personal Data Retention and Destruction Policy,
    - The Data Processor will be subject to an indefinite confidentiality obligation regarding the personal data it processes,
    - In case of any data breach, the Data Processor will be obliged to notify the Data Controller immediately,
    - Our Company will carry out or cause to carry out the necessary audits on the Data Processor's systems containing personal data, and it will be able to examine the reports resulting from the audit and the service provider company on site,
    - The Data Processor will take the necessary technical and administrative measures for the security of personal data; and
    - In addition, as long as the nature of the relationship between us and the Data Processor allows, the categories and types of personal data transferred to the Data Processor are also specified in a separate article.

- As emphasized by the Authority in its guidelines and publications, personal data is reduced as much as possible within the framework of the principle of data minimization and personal data, which is not necessary, outdated and does not serve a purpose, is not collected, and if it was collected in the period before the KVKK, they are destroyed in accordance with the Personal Data Retention and Destruction Policy.
- Personnel who are experts in technical issues are employed.

- Our company has determined provisions regarding confidentiality and data security in the Employment Contracts to be signed during the recruitment processes of its employees and the employees are asked to comply with these provisions. Employees are regularly informed and trained on the law on the protection of personal data and about the necessary measures to be taken in accordance with this law. In this context, the roles and responsibilities of the employees have been reviewed 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.
- Access authorizations are limited and authorizations are regularly reviewed.
- The technical measures taken are regularly reported to the authorized person and the issues that pose a risk are reviewed and the necessary technological solutions are worked to be produced.
- Software and hardware including virus protection systems and firewalls are installed.
- Backup programs are used to ensure that personal data is stored securely.
- Security systems are used for storage areas and the technical measures taken are periodically reported to the relevant person in accordance with internal controls and the issues that pose a risk are re-evaluated and necessary technological solutions are produced. Files/printouts stored in the physical environment are stored through the supplier companies and then they are destroyed in accordance with the determined procedures.
- The issue of Protection of Personal Data is also adopted by the senior management and a special Committee (KVK Committee) has been established and started to work on this issue. 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 are explained in detail.

HOW DO WE PROTECT YOUR SENSITIVE PERSONAL DATA?

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

Article 6 of the KVKK regulates data related to race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, disguise and dress, membership to associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data as sensitive personal data because they carry the risk of causing victimization or discrimination when they are processed unlawfully, and article in question has subjected the processing of this data to a more sensitive protection.

In accordance with Article 10 of the KVKK, our company enlightens the Relevant Persons during the acquisition of sensitive personal data. Sensitive personal data is processed by taking measures in accordance with the KVKK and by carrying out the necessary audits. As a rule, one of the conditions for processing sensitive personal data is to get the explicit consent of the data owner. Our company offers data owners the opportunity to express their explicit consent on a specific subject based on information and with their free will.

As a rule, our company obtains the explicit consent of the Relevant Persons in writing for the processing of sensitive personal data. However, pursuant to Article 6/3 of the KVKK, in the presence of any of the conditions specified in Article 5/2 of the KVKK, the explicit consent of the Relevant Persons is not sought. In addition, Article 6/3 of the KVKK regulates that personal data related to health and sexual life can be processed by persons or authorized institutions and organizations under the obligation of confidentiality for the purpose of protecting public health, preventive medicine, medical diagnosis, implementation of treatment and care services, planning and management of health services and

financing, without seeking the explicit consent of the person concerned. Regardless of the reason, the processing processes always take into account the general data processing principles and ensure compliance with them.

Our company takes special measures to ensure the security of sensitive personal data. In accordance with the principle of data minimization, sensitive personal data is not collected unless it is necessary for the relevant business process and they are processed only when necessary. In case of processing sensitive personal data, technical and administrative measures deemed necessary are taken to act in accordance with legal obligations and the measures determined by the KVK Board.

WHAT ARE YOUR RIGHTS REGARDING YOUR PERSONAL DATA?

Pursuant to Article 11 of the KVKK, as data owners you have the following rights regarding your personal data:

- To learn whether your personal data is processed by our Company,
- If your personal data has been processed, requesting information about it,
- To learn the purpose of processing your personal data and whether they are used in accordance with their purpose,
- To know the third parties to whom your personal data is transferred at home or abroad,
- To request the correction of your personal data in case that they are processed incomplete or incorrect and to demand the notification of the transaction made within this scope to third parties to whom your personal data has been transferred,
- Although it has been processed in accordance with the provisions of the KVKK and other relevant laws, to request the deletion or destruction of your personal data in the event that the reasons requiring its processing disappear, and to request the notification of the transaction made within this scope to the third parties to whom your personal data has been transferred,
- To object to the occurrence of a result against you by analysing the processed data exclusively through automated systems,
- To request compensation for the damage you have suffered in case you incur damage due to unlawful processing of your personal data.

In accordance with the Application Communiqué, you can submit these requests to our Company free of charge by the following method:

1) After filling out the form at www.mesa.com.tr address and signing it with wet signature, submitting the form in question in person to Mesa Mesken İnşaat A.Ş. Ihlamur Cad., No:2 Çayyolu, Çankaya/Ankara (we would like to remind you that your ID will need to be presented).
2) After filling out the form at the www.mesa.com.tr address and signing it with wet signature, submitting the form in question through a notary public to Mesa Mesken İnşaat A.Ş. Ihlamur Cad., No:2 Çayyolu, Çankaya/Ankara
3) After filling out the application form at the www.mesa.com.tr address and signing it with a "secure electronic signature" within the scope of the Electronic Signature Law No. 5070, submitting the form in question via registered e-mail with a secure electronic signature to the mesameskeninsas@hs01.kep.tr address.

4) Submission in writing by using your e-mail address previously notified to our Company and registered in our Company's system.

İn the application;

If Name and Surname is written in the application and if application is made in written, it is mandatory to specify T.R. Identity Number for citizens of the Republic of Turkey, nationality, passport number or identity number, if any, for foreigners, residential or workplace address for notification, e-mail address, telephone and fax number, if any, subject of the request. Information and documents related to the subject are also attached to the application.

It is not possible to make a request by third parties on behalf of personal data owners. In order for a person other than the personal data owner to make a request, there must be a wet-signed and notarized copy of the special power of attorney issued by the personal data owner on behalf of the person who will apply. In the application, which is made by you to use your rights stated above as well as use of your rights as a personal data owner and which contains your explanations regarding the right you request to use, the matter you are requesting must be clear and understandable, the matter you are requesting must be related to you personally, or if you are acting on behalf of someone else, you must be specifically authorized in this matter and your authority must be documented, the application must include identity and address information, and documents proving your identity must be attached to the application.

In this context, your applications will be finalized as soon as possible and within a maximum of 30 days. These applications are free of charge. However, if the transaction requires an additional cost, the fee in the tariff determined by the KVK Board may be charged.

In the event that the personal data owner submits his/her request to our Company in accordance with the stipulated procedure, our Company will conclude the relevant request free of charge as soon as possible and within thirty days at the latest, depending on the nature of the request. However, if the transaction requires an additional cost, the applicant will be charged the fee in the tariff determined by the KVK Board by our Company. Our company may request information from the relevant person in order to determine whether the applicant is the owner of personal data. In order to clarify the issues in the application of the personal data owner, our company may ask questions to the personal data owner about his/her application.

Pursuant to Article 14 of the KVKK, if your application is rejected by our Company or if you find our answer insufficient, or if we do not respond to the application in time; You can file a complaint with the KVK Board within thirty days from the date when you learned our company's response and in any case within sixty days from the date of application.

WHAT ARE THE SITUATIONS IN WHICH DATA OWNERS CANNOT ASSERT THEIR RIGHTS?

Pursuant to Article 28 of the KVKK, personal data owners cannot assert the above-mentioned rights of personal data owners in these matters, as the following situations are excluded from the scope of KVKK:

- Processing of personal data for purposes such as research, planning and statistics by anonymizing them with official statistics.

- Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that they don't violate national defence, national security, public security, public order, economic security, privacy of private life or personal rights or they don't constitute a crime.
- Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defence, national security, public security, public order or economic security.
- Processing of personal data by judicial authorities or enforcement authorities in relation to investigation, prosecution, trial or execution proceedings.

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

- In the case that the processing of personal data is necessary for the prevention of crime or for criminal investigation.
- In the case that the processing of personal data is made public by the personal data owner.
- In the case that the processing of personal data is necessary for the execution of supervisory or regulatory duties and disciplinary investigation or prosecution by authorized public institutions and organizations and professional organizations in the nature of public institutions, based on the authority granted by the law.
- In the case that the processing of personal data is necessary for the protection of the economic and financial interests of the State in relation to budget, tax and financial issues.

MISCELLANEOUS

As explained in detail above, your personal data can be stored and preserved and they can be classified in accordance with market research, financial and operational processes and marketing activities and they can be updated in different periods, and to the extent permitted by the legislation, within the framework of the law and within the scope of confidentiality principles, they can be transferred to third parties and/or suppliers and/or service providers and/or our foreign shareholders to whom we are affiliated because it is deemed necessary by the services to be provided and information can be transferred in accordance with the policies to which we are subject and doe to the reasons foreseen by other authorities, and they can be stored and processed by reporting and records and documents can be prepared as a basis for the transaction in electronic or paper media.

In case of inconsistency between the provisions of the KVKK and other relevant legislation and this Policy, the provisions of the KVKK and other relevant legislation will be applied first.

This Policy, which was prepared by our company, has 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 privacy statement due to legislative provisions that may change over time and changes in our company policies. We will post the most current version of the privacy statement on our website.

The User(s) irrevocably accept, declare and undertake that they have read this Personal Data Protection Policy before entering the website and that they will comply with all the issues stated herein, and that the

content on the website and all electronic media and computer records belonging to our Company will be considered as conclusive evidence in accordance with Article 193 of the Code of Civil Procedure.

APPENDIX-ABBREVIATIONS

ABBREVIATIONS	
Law no 5651	Law on Regulation of Publications Made on the Internet and Combating Crimes Committed Through These Publications, which came into force after being published in the Official Gazette No. 26530 dated 23 May 2007.
Constitution	Constitution of the Republic of Turkey No. 2709, dated 7 November 1982, published in the Official Gazette No. 17863, dated 9 November 1982
Communique regarding the application	Communiqué on the Procedures and Principles of Application to the Data Controller, which came into force after being published in the Official Gazette No. 30356 dated 10 March 2018.
Relevant Person/Relevant Persons or Data Owner	It refers to the real person, personal data of which is processed such as customers of Mesa Mesken and/or group companies with which Mesa Mesken is affiliated, corporate customers with whom it has commercial relations, business partners, shareholders, officials, candidate employees, interns, visitors, suppliers, employees of the institutions it cooperates with, third parties and other persons including but not limited to those listed here.
Regulation on Deletion, Destruction or Anonymization of Personal Data	Regulation on Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette No. 30224 dated 28 October 2017 and entered into force as of 1 January 2018.
KVKK	Personal Data Protection Law, which came into force after being published in the Official Gazette No. 29677 dated 7 April 2016.
KVK Board	Personal Data Protection Board
KVK Institution	Personal Data Protection Institution
m.	Article
For example	Example
Policy	Mesa Mesken Personal Data Protection and Privacy Policy
Company/Mesa Mesken	Mesa Mesken İnşaat A.Ş.
Turkish Penalty Code	Turkish Penal Code No. 5237 dated 26 September 2004, published in the Official Gazette No. 25611 dated 12 October 2004