Policy on Protection of Personal Data

Table of Contents

At Makyol, we attach importance to the privacy and security of your personal data. In this regard, we would like to inform you about how we process the personal data of our customers, suppliers, business partners, their employees and officials, and all other third parties, for what purposes we use such personal data, and how we protect the same in the course of our business relations.

All the terms and expressions used herein shall have the meanings attributed to them in the Personal Data Protection Law numbered 6698 **("PDPL")** and other relevant legislation. The term "you" used herein refers to you. The term personal data shall be construed to include sensitive personal data. The meanings of the terms and abbreviations used herein are presented in the ANNEX - Abbreviations section.

Please note that if you do not accept this Policy, you should not transmit your personal data to us. If you choose not to provide us with your personal data, in some cases we will not be able to provide you with our services, respond to your requests, or ensure the full functionality of our services.

Please note that it is your responsibility to ensure that any personal data you transmit to our company are accurate, complete and up to date as far as you aware. Furthermore, if you share any data regarding other people with us, it will be your responsibility to collect such data in accordance with local legal requirements. It will mean that you have obtained all the necessary permissions from such third persons to collect, process, use, and disclose their information, and our Company will not be held liable in this regard.

ABOUT MAKYOL

The service philosophy of Makyol, which focuses on customer satisfaction, differentiates Makyol from its competitors. At present, Makyol is a first-class contracting company that is preferred internationally as well as in the national market. Makyol successfully carries out joint venture projects with leading Turkish and foreign companies in the sector, both at home and abroad. Its managerial approaches, quality philosophy, strong values, understanding of social responsibility, commitment to ethical values, the importance it attaches to the environment, occupational health and safety, and the exemplary behaviors exhibited by it in these aspects sets the way for the sustainable growth of Makyol, which will continue to build what is right and good for humanity.

The terms "we", "Company", or "Makyol" used herein shall be used in the context of data processing activities performed as the Data Controller by Makyol İnşaat Sanayi Turizm ve Ticaret A.Ş., a company having its registered seat at "Etiler Mahallesi, Tepecik Caddesi, Melodi Sokak İ.T.Ü. Blokları E Blok, 34337 Beşiktaş/İstanbul", and registered to Istanbul Trade Registry with registration no. 141792 ("**Makyol**")

OUR PRINCIPLES REGARDING PROCESSING OF PERSONAL DATA

All personal data processed by our company are processed in accordance with the PDPL and other relevant legislation. The basic principles employed by while processing your personal data in accordance with Article 4 of the PDPL are explained below:

- **Processing in Compliance with the Law and the Rules of Good Faith**: Our company acts in accordance with the principles introduced by legal regulations and the general rule of trust and honesty in connection with the processing of personal data. In this context, our Company takes into account the proportionality requirements in the course of processing personal data, and does not use personal data other than for the intended purposes.

- **Keeping Personal Data Accurate and Updated When Required**: Our Company ensures that the personal data processed by it are accurate and up to date, taking into account the fundamental rights and legitimate interests of data subjects.

- **Processing Personal Data for Specific, Clear, and Legitimate Purposes**: Our company clearly and precisely determines the purposes of processing personal data that are legitimate and legal. Our company processes personal data to the extent that it is necessary in connection with products and services offered by our Company.

- **Being Connected, Limited, and Reasonable for the Purposes of Processing**: Our company processes personal data in a way that is convenient for the realization of the intended purposes, and avoids the processing of personal data that are not related to the realization of such purpose or that are not needed.

- **Preserving Personal Data for the Periods Set Out in the Relevant Legislation or Required for the Purposes of Processing**: Our company retains personal data only for the periods of time that are set out in the relevant legislation or that are required for the purposes 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 of time is specified, then our company observes such period of time; or if no such a period of time is set out, then personal data is kept for the period of time required for the purposes for which the personal data is processed. Personal data are deleted, destroyed or anonymized by our Company in the event of the expiration of the applicable period or the disappearance of the reasons for processing of the personal data.

CATEGORIES OF DATA SUBJECTS

The categories of data subjects, except for employees whose personal data are processed by our company (including interns, and employees of sub-employers), are indicated in the table below. A separate policy regarding the processing of personal data of our employees has been established and implemented at the company. Persons who fall outside of the following categories may also direct their requests to our Company in accordance with the PDPL. The demands of these persons will also be taken into consideration.

CATEGORY OF RELATED PERSON	DESCRIPTION
Customer	A real or legal person purchasing our products and services
Prospect Customer	A real or legal person who has made a request for, or has revealed an interest in, purchasing our products or benefiting from our services, or who might be considered to have such interest in accordance with the customs and the rules of honesty.
Visitor	A real person who enters the physical facilities (e.g. offices, construction sites, etc.) owned or organized by our Company or visits our websites for various purposes
Third Person	Any real persons (e.g. sureties, companions, family members, or relatives) who are associated with the persons specified above in order to ensure the security of commercial transactions carried out between our Company and such third persons or to protect their rights and to obtain benefits; or our all real persons whose personal data is to be processed by our Company for a specific purpose although it is not indicted in the policy (e.g. former employees)

Employee Candidate / Trainee Candidate	Any real person who has applied for a job to our Company in any way or who has revealed his/her CV and related information to our Company
Group Company Employee	Any employee or representative of any of the companies of Makyol Group, of which our company is a member, in Turkey or at abroad
Employees, Shareholders, and Officials of the Firms Cooperated by us.	Any real persons employed at the firms with which our company has all kinds of business relations (including but not limited to business partners, suppliers, etc.), including their shareholders and officials.

WHEN DO WE COLLECT YOUR PERSONAL DATA?

We collect your personal data mainly when:

- you buy or use our products or services
- you sell goods or provide services to us
- you fill out the information forms regarding Makyol projects
- you subscribe to our newsletters or choose to receive our marketing messages
- you contact us to submit complaints or feedbacks via e-mail or telephone
- you apply for a job at our company
- you attend our company's events, seminars, conferences and organizations
- you contact us for any purpose as a potential customer / supplier / business partner / sub-employer

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

WHAT PERSONAL DATA DO WE PROCESS ABOUT YOU?

The personal data we process about you varies according to the type of business relationship between us (eg customer, supplier, business partner, etc.) and the method used by you for communicating with us (eg telephone, e-mail, printed documents, etc.).

Basically, our personal data processing methods involve situations when you participate in our business events and surveys by phone or e-mail or interact with us in any other way. In this context, the personal data we process about you can be categorized as follows:

Data category	**Examples**
Identity Details	Details available on identity documents such as name, surname, title, date of birth
Contact Details	Email, phone number, address
Images and / or videos that can identify you	Photos and video images and audio data processed when you visit our Company for security reasons or when you attend events organized by our Company.
Financial data	Bank account details and billing details

Data category	Examples
Any other information you voluntarily decide to share with Makyol	Personal data you share based on your own initiative, feedbacks, opinions, requests and complaints, evaluations, comments submitted by you to us, our evaluations regarding these issues, uploaded files, fields of interest, and information submitted for our detailed examination before establishing a business relationship with you
Automatically collected electronic data	When you visit or use our website or applications, subscribe to our newsletters, or interact with us through other electronic channels, in addition to the information you directly transmit to us, we may also collect electronic data sent to us by your computer, mobile phone or other access device (e.g. device hardware model, IP address, operating system version and settings, time and duration of using our digital channels or products, your actual location that can be collected when you activate location-based products or features, links you click, motion sensor data, etc.)
Legal transactions and compliance	Your personal data and audit and inspection data processed within the scope of the determination and tracking of our legal receivables and rights, execution of our liabilities, and compliance with our legal obligations and our Company's policies
Corporate customer / supplier data	Data obtained as a result of operations carried out by our business units as part of our services, about data subjects such as customers / suppliers or employees or their authorized signatories.
Incident management and security data	Data collected about events that have the potential to affect our company, its employees, directors or shareholders such as license plate and vehicle details, transportation and travel details
Personal data collected from other sources	To the extent permitted by applicable laws and regulations, we may also collect your personal data through public databases, and the methods and platforms where our business partners collect personal data on our behalf. For example, before establishing a business relationship with you, we may conduct inquiries about you from public sources to ensure the technical, administrative and legal security of our business activities and transactions. In addition, it may be possible for you to transmit some personal data belonging to third parties to us (for example, personal data of any guarantors, companions, family members, etc.). In order for us to manage our technical and administrative risks, we may process your personal data by means of methods used in these fields in accordance with the generally accepted legal and commercial practices and rules of good faith.

PROCESSING PERSONAL DATA OF EMPLOYEE CANDIDATES

In addition to the above personal data categories, we collect personal data such as the school graduated, previous work experience, disability, and etc. about employee candidates to understand the experience and

qualifications of the candidate and evaluate his/her suitability for the vacant position, check the accuracy of the information submitted if necessary, and conduct inquiries about the candidate by contacting third persons whose contact details are provided by the candidate, communicate with the candidate about the job application process, recruit a suitable candidate for the vacant position, comply with legal regulations, and apply our Company's recruitment rules and human resources policies,

Personal data of employee candidates are processed via job application forms submitted via printed and electronic media, our company's electronic job application platform, applications sent to our company physically or by e-mail, employment and consultancy companies, face-to-face or electronic interviews, checks performed by our company about employee candidate, and recruitment tests conducted by human resources experts to assess the candidate's suitability during the recruitment process.

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

PROCESSING PERSONAL DATA OF OUR VISITORS AT OUR OFFICES / WORKSITES

Our company processes personal data for the purpose of ensuring the physical security of our Company, our employees and visitors during visitors' entrance to and exit from the company's buildings, and to inspect the workplace rules. In this context, names, surnames and Turkish ID numbers of our visitors are confirmed based on their IDs and recorded in a visitor logbook for the purpose of tracking entrances and exits of visitors.

The visitor is informed about the processing of personal data by means of a disclosure at the security entrance before his/her data is received. However, as our company has a legitimate interest in this context, the visitor's explicit consent is not obtained in accordance with the article 5/2 / f of the PDPL. These data are only physically kept in the visitor logbook and are not transferred to any other medium unless there is a suspicious situation that threatens the security of the Company. However, this information can be used in cases such as preventing crimes and ensuring the company's security.

In addition, for the purpose of providing security by our Company and for other purposes specified in the Policy, Internet access may be made available to our visitors who request such access during their stay at our company's offices. In this case, the logs of your internet access are kept in accordance with the Law No. 5651 and mandatory provisions of the legislation adopted thereunder, and these records are only processed upon request of authorized public entities and organizations or in order to fulfil our legal obligation during audits to be carried out within the Company.

Only a limited number of Makyol employees can access the logs obtained within this framework. The employees, who have access to the aforementioned logs, access these records only in response to requests of authorized public entities and organizations, or for use as part of audits, and share the same only with legally authorized persons.

PROCESSING PERSONAL DATA THROUGH CLOSED CIRCUIT CAMERA RECORDINGS

Security cameras are used to ensure the security of our company and our sites, and personal data are processed in this way. With surveillance activities conducted by means of security cameras, our company aims to increase the quality of the service provided, to ensure the safety of life and property of the physical premises of the company and the persons present within the company, to prevent abuse, and to protect the legitimate interests of data owners.

Personal data processing activities performed by our company using security cameras are carried out in accordance with the Constitution, the PDPL, the Law on Private Security Services No. 5188 and relevant legislation.

In accordance with Article 4 of the PDPL, our company processes personal data in a limited and reasonable manner in connection with the purposes for which they are processed. No monitoring activities are carried out in a way that may result in the intervention of the privacy of any person exceeding the security objectives. In this context, warning signs are placed in common areas where CCTV recordings are performed and data subjects are informed. However, since our Company has a legitimate interest in keeping CCTV recordings, no express consent is not obtained from data subjects. In addition, necessary technical and administrative measures are taken to ensure the security of personal data obtained as a result of CCTV monitoring in accordance with Article 12 of the PDPL.

In addition, a procedure has been drafted and implemented for the areas equipped with CCTV cameras, the coverage areas of the cameras, and the retention periods of camera records. Such procedure is taken into account before any CCTV cameras are installed and camera units are placed accordingly. No camera unit is allowed to be placed beyond the purpose of security and in any manner that would breach the privacy of individuals. Only a certain number of Company personnel have access to CCTV camera images, and these authorizations are regularly reviewed. Personnel who have access to these records sign a deed of commitment to protect personal data in accordance with the law.

Images are recorded through security cameras located at entrance doors, building exterior, cafeteria, visitor waiting room, employee camps and service areas of floor corridors to ensure building security, and the recording process is audited by the Administrative Affairs Department.

FOR WHICH PURPOSES DO WE USE YOUR PERSONAL DATA?

Our purposes for using your personal data vary depending on the type of business relationship established between us (e.g. customer, supplier, business partner, etc.). Basically, our purposes for processing your personal data are as follows. Personal data processing activities related to employee candidates are explained under the "Processing Personal Data of Employee Candidates" section above.

Our Purposes of Processing Personal Data	**Examples**
Evaluating potential suppliers / business partners	Conducting our inspection and conflict of interest process in accordance with our risk rules
Establishment and management of customer relations, execution and conclusion of contract process with our suppliers / business partners	The obtaining of preliminary information forms from customers for real estate sales, the taking of photos and videos during launches, the sharing of Makyol projects with public and private institutions and organizations, the execution and amendment of preliminary real estate sales contracts, the handling of down payment processes, the receipt of requests for apartment flats, the filling of the leaflets, the realization of apartment flat delivery and title deed transfer formalities, the establishment of subscriptions, the drafting of payment plans, the management of the processes with the banks related to the related loans, the management of processes regarding promissory notes, the transfer of preliminary real estate sales contracts, the performance of name change or termination

Our Purposes of Processing Personal Data	Examples
	processes, the realization of deals and transactions arising from the Law on Consumer Protection, the collection of contractually and commercially required documents, the appointment of environmental officers, the performance of licensing formalities, the following up of compliance with master agreements signed with administrations, providing legal opinions on contracts, conducting financial audits, conducting structural reports, analysis and project preparation processes and establishing contracts with suppliers in this context, conducting researches for domestic and international tenders and projects, performing pre-qualification preparations for participation in tenders, preparation of tender offers, participation in domestic and international tenders, sharing signature circulars with relevant institutions and organizations in order to participate in tenders, signing tender contracts, obtaining consultancy services for tenders, holding communication processes with tender partners, executing contracts with tender partners, making visits to private and official institutions abroad, archiving contracts physically and digitally, performing e-invoicing processes for invoices issued and approved on behalf of Makyol, generating system records of the companies which are to be paid, providing invoice management for foreign branches of Makyol, making payments on behalf of foreign branches, receiving and delivering checks and bills for payment and collection transactions, making findex inquiries for customers, performing financial adequacy checks during the process of determining tenants, concluding lease contracts, providing OT infrastructure services for Doria Hotel operated by Maktur, providing internet access for Doria Hotel guests, conducting pre-qualification inquiries for suppliers, conducting service organizations for suppliers, performing sales transactions for our company's services , submitting proposals, issuing invoices for supply of goods, performing invoicing processes for invoice refunds, price differences and return invoices, performing month-end reconciliation formalities, executing and performing contracts, providing security for post-contract legal formalities, developing services, evaluating new technologies and applications, determining and implementing our company's commercial and business strategies, managing operations (e.g. demand, proposal, evaluation, order, budgeting, contract) and financial operations, managing financial affairs, and offering alternatives to legal / natural persons which whom the company maintain commercial relations
Conducting direct marketing processes	Sending marketing notifications about our services via e-mail and telephone, conducting satisfaction surveys or evaluating and responding to your opinions, complaints and comments you have made through social media, online platforms or other media,

Our Purposes of Processing Personal Data	Examples
	informing our customers about company's innovations and campaigns, organizing marketing activities with participants at the events, and preparing greeting cards and letters for special occasions
Communication and support (upon your request)	Responding to requests for information about our services, providing support for requests received through our communication channels, and updating our records and databases
Compliance with legal obligations	Performing tax and insurance processes, fulfilling our legal obligations arising from the relevant legislation, especially including the Law No. 5651 and legislation adopted thereunder, the Law No. 6563 on the Regulation of Electronic Commerce and legislation adopted thereunder, the Law No. 6502 on Consumer Protection, the Turkish Penal Code No. 5237 and the Law No. 6698 on Protection of Personal Data, performing relevant processes before official institutions such as the Land Registry Directorates, performing relevant record keeping and disclosure obligations, compliance and audit, audit and inspection of official authorities, follow-up and conclusion of our legal rights and lawsuits, and mediation and arbitration processes on behalf of all companies and ordinary partnerships of Makyol Group, conducting necessary processes set out in laws and regulations to which we are subject such as data disclosure performed upon the request of official authorities, with regulatory and supervisory institutions as required or required by legal regulations, performing necessary or relevant formalities with regulating and auditing entities as specified in the PDPL.
Protecting and ensuring security of company's interests	Carrying out the necessary audit activities to protect the interests of the company, conducting conflict of interest controls, ensuring the legal and commercial security of the persons holding business relations with our company, keeping CCTV records for the protection of the company's equipment and assets, taking technical and administrative security measures, carrying out the necessary activities to improve the services we offer, implementing and supervising workplace rules, planning and executing social responsibility activities, protecting the commercial reputation and trust established by Makyol group companies, conducting audit activities for group companies, reporting, responding to, and taking all measures for, all incidents, accidents, complaints, losses, stealings, and etc. occurring inside the building, disclosing the rules to be followed for dangerous situations that may occur during maintenance and repair activities and measuring the professional competencies of subcontractors, ensuring the order of entrances to and exits from the company's employees and obtaining necessary

Our Purposes of Processing Personal Data	Examples
	information in terms of security, carrying out the necessary quality and standard audits, or fulfilling our reporting and other obligations as determined by laws and regulations, and evaluating the suitability of the acceptance of suppliers to the field
Planning and execution of the commercial activities of the company	Determining and implementing communication, market research and social responsibility activities carried out by our company, and carrying out purchasing transactions in line with the purpose of determining, planning and implementing the commercial policies of the company in the short, medium and long term.
Reporting and audits	Ensuring communication with Makyol group companies seated in Turkey, performing the required activities, and internal audit and reporting process
Protection of rights and interests	Making defenses against lawsuits, investigations and other legal claims brought against our company

HOW DO WE USE YOUR PERSONAL DATA FOR MARKETING?

As marketing activities are not considered within the scope of the exceptions set out in the clauses 5/2 and 6/3 of the PDPL, as a rule, we always obtain your consent to process your personal data for marketing purposes. Our company may send you regular promotional communications about its products, services, events, and promotions. Such promotional communications may be sent to you via different channels such as email, phone, SMS text messages, mail, or third party social networks.

In order to provide you with the best personalized experience, sometimes these communications may be tailored to your preferences (for example, based on the results we derive from your website visits, or based on links you click in our emails, as you tell us about them).

Based on your consent, we can perform marketing activities for the purpose of offering you opportunities about special products and services such as internet advertising, Targeting, Re-targeting, cross-selling, campaign, opportunity and product / service advertisements, using cookies for this purpose, making commercial offers considering your preferences and recent purchases, and tracking your usage habits according to previous records of your visits to http://www.makyolyasam.com.tr/ and http://www.makyolsantral.com/ applications, and presenting special products for you based on results of such tracking activities; processing data for the purpose of presenting special advertisements, campaigns, advantages and other benefits to you for sales and marketing activities and carrying out other marketing and CRM studies, processing data for the creation of new product and service models; sending of electronic commercial messages (such as campaigns, newsletters, customer satisfaction surveys, product and service advertisements); sending gifts and promotions; carrying out marketing activities in order to organize corporate communications and other events and invitations in this context and providing information in this regard.

When required by the applicable legislation, we will ask for your consent before starting the above activities. You will also be given the opportunity to withdraw (stop) your consent at any time. In particular, you can

always stop marketing-related notifications from being sent to you by following the unsubscribe instructions included in each e-mail and SMS message.

FOR WHAT LEGAL REASONS DO WE PROCESS YOUR PERSONAL DATA?

We process your personal data within the framework of the following legal reasons set out in Article 5 of the PDPL as well as in the Turkish Commercial Code No. 6102, Turkish Code of Obligations No. 6098, the Tax Procedure Law No. 213, and applicable legislation on electronic commerce:

Legal Reason	**Examples**
We process based on your consent in cases where we need to obtain your explicit consent in accordance with PDPL 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.
Any situation permitted by the applicable legislation	Specification of the name of the relevant person on the invoice pursuant to Article 230 of the Tax Procedure Law
In the event it is obligatory to protect the vital interests of any person	Disclosure to the doctor of the medical information of a board member who fainted at the board of directors
In the event we need to establish a contract with you, fulfil the contract, and fulfil our obligations under a contract	Obtaining the customer's bank account details within the scope of the contractual relationship with the Customer.
Fulfilling our legal obligations	Fulfilling our tax obligations, submitting any information requested by court
In the event that your personal data has been made public by you	Using personal data that you have made public by means of sending e-mails to us to communicate with you, through social media channels, for the purpose of making it public.
In the event that it is compulsory for us to process data for the establishment or protection of any right, to exercise our legal rights, or to defend against legal requests brought against us.	Keeping documents that are of proof / evidence nature, and using such documents when necessary
In cases required by our legitimate interests, provided that it does not harm your fundamental rights and freedoms.	Ensuring the security of our company’s communication networks and information, carrying out our corporate activities, detecting suspicious transactions and conducting researches in order to comply with our risk rules, benefiting from storage, hosting, maintenance, support services in order to provide IT services in terms of technical

Legal Reason	Examples
	and security, ensuring the efficiency of our company activities and benefiting from cloud technology in order to make use of technology

In cases where your Personal Data is processed with express consent, we would like to emphasize that if you withdraw your express consent, you will be removed from the commercial membership program where the processing is required based on the said explicit consent and you will not be able to benefit from the advantages you have benefited from as of the relevant date.

WHEN DO WE SHARE YOUR PERSONAL DATA?

Transfer of Personal Data in the Country

Our company is under the responsibility to act in accordance with the relevant regulations stipulated in the PDPL, especially the Article 8 of the PDPL, and the decisions taken by the Board regarding the transfer of personal data. As a rule, personal data and sensitive personal data of data subjects cannot be transferred by our Company to any other real or legal persons without the express consent of the data subjects.

In addition, data transfer is possible without the consent of the person concerned in the cases stipulated in Articles 5 and 6 of the PDPL. Unless otherwise regulated in the Law or other relevant legislation, our company may transfer personal data to any third parties seated in Turkey and other companies of Makyol Group Companies in accordance with the conditions stipulated in the PDPL and other relevant legislation and by taking the security measures specified in the legislation (or in the contract in the event such a contract is executed with the data subject)

Transfer of Personal Data Abroad

Our company may transfer personal data to third parties in Turkey, and personal data may also be transferred to abroad by being processed in Turkey or for processing and storage thereof outside Turkey, including the use of external resources and taking appropriate security measures in accordance with the requirements stipulated in the law and other regulations as given above. We transfer your personal data abroad by taking necessary technical and administrative measures through cloud computing technologies in order to carry out our corporate activities in the most efficient way and to benefit from the possibilities of technology. Your personal data is transferred abroad in accordance with the procedures and principles stipulated in Article 9 of PDPL, by ensuring the security of your data in order to carry out the activities and transactions related to our projects / tenders abroad.

In accordance with Article 9 of the PDPL, as a rule, we seek the explicit consent of the data subjects for the transfer of personal data abroad. However, personal data may be transferred abroad without the explicit consent of the data subject in accordance with the Article 9 of the PDPL, provided that one of the conditions regulated in Article 5/2 or Article 6/3 of the PDPL is satisfied, and in the foreign country where personal data is to be transferred

a) adequate protection is available,
b) no adequate protection is available, but and the data supervisors in Turkey and abroad delivers a written commitment for adequate protection, and the board’s permit is present in this regard.

In this regard, our Company requires that in exceptional cases where express consent is not sought regarding the transfer of personal data mentioned above, in addition to the conditions applicable for processing and transfer of personal data without consent, adequate protection is available in the country where the data will be transferred in accordance with the PDPL. The Personal Data Protection Board will determine whether sufficient protection is available or not. In the case of the absence of adequate protection, the data supervisors in Turkey and abroad must deliver a written commitment for adequate protection, and the board's permit must be present in this regard

Parties with which personal data is shared in the country and abroad

We do not share your personal data except in the special cases described herein. At Makyol, access to your personal data will be limited to those who need to know such personal data in line with the purposes defined in this Policy. In order to achieve the purposes of collecting your data (for detailed information about these purposes, please see the section "For what purposes do we use your personal data?"), we transfer your Personal Data to the following persons and entities:

1. *Companies of Makyol Group*: Since Companies of Makyol Group operate within an organic link, your data is shared with is available for access by Makyol Group Companies established in Turkey. This sharing is only made with employees who are authorized to fulfil the purposes of sharing in the relevant Makyol Group Companies. However, we would like to state that the sharing of data with Makyol Group Companies in general is carried out in a manner that does not include personal data within the scope of financial reporting on company activities such as corporate profitability and efficiency. In some special cases, instead of sharing anonymous data with Makyol Group Companies, we may prefer to share personal data (such as providing information technology infrastructure to Doria Hotel, sharing claim details for initiating an insurance claim file, and etc.) The Data Sharing Agreement regarding the transfer of your personal data to Makyol Group Companies has been signed and the necessary measures have been taken.

2. *Ordinary Partnerships of Makyol*: At Makyol, we sometimes carry out the projects / tenders in Turkey and abroad within through ordinary partnerships established with our business partners. In this context, we transfer personal data abroad for the purpose of conducting ordinary partnership functions, financing tender / project processes, employing people for projects / tenders, and coordinating and organizing project / tender processes.

2. *Service Providers*: This term defines the parties with which our company establishes business partnerships for purposes such as sales, promotion and marketing of services of our company, providing of after-sales support, and etc. while conducting its commercial activities. Like many businesses, we may work with reliable third parties such as information and communication technology providers, consultancy service providers, cargo companies, and travel agencies to carry out functions and services in the most efficient manner using the state of art technologies within the scope of some data processing activities, and in this context we can share data to carry out our activities. This sharing is limited to ensure that the purposes of the establishment and execution of the business partnership are fulfilled. In order to carry out the activities of our company in the most efficient way and to benefit from the technological advancements at the maximum level, we use cloud information technologies, and in this context we can process your personal data in Turkey and abroad through companies that provide cloud information services. The marketing services support company we share personal data with may be established abroad and accordingly data

sharing activities may be carried out with abroad in accordance with the provisions regarding data sharing abroad pursuant to Article 8 and Article 9 of the PDPL.

2. Public Bodies and Entities: When required by law or when we need to protect our rights, we may share your personal data with relevant public, judicial and administrative authorities (e.g. tax offices, SGK, SSI Inspectors, İŞKUR, law enforcement bodies, courts and enforcement offices, Land Registry Offices, Ministry of Environment and Urbanization, Consulates).

3. Persons Subject to Private Law: According to the provisions of the relevant legislation, persons subject to private law who are authorized to receive information and documentation from our Company can be shared with personal data for limited purposes covered by their legal authorities (eg Occupational Health and Safety Company, Audit Firms, BEDAŞ, İGDAŞ, İSKİ).

4. Professional consultants and other parties: In order to perform business activities of Makyol, we may share your personal data with other persons, including professional consultants such as the following, to support the execution of the procurement processes, conduct mediation and arbitration procedures, maintain our relations with our suppliers, and promote our projects:

    - Banks
    - Insurance companies
    - Auditors
    - Lawyers
    - Accountants
    - Credit Registration Office
    - Digital Agencies
    - Media Agencies
    - Marketing Consultants
    - Cargo Companies
    - Service firms
    - Insurance Companies
    - Site managements
    - Travel Agencies
    - Other external professional consultants

5. *Other parties involved in corporate transactions:* In addition, we may share your personal data with other parties involved in corporate transactions such as companies providing service and consulting services, customers, subcontractors, suppliers, and business partners in the country and at abroad for purposes of conducting contracts, contractual and commercial relations established for the execution of company's business and activities, ensuring the efficiency and security of our corporate processes, or in the process of the sale of a company or the sale of a certain part of a company to another company in order to fulfil the commitments made, or in the event that the name, assets or shares of Makyol become the subject of any other reorganization / restructuring, merger, joint venture or other sale or disposal processes (including those in connection with bankruptcy or similar transactions)

HOW LONG DO WE STORE YOUR PERSONAL DATA?

We only store 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 to keep your personal data at the end of the relevant periods, we destroy your personal data in accordance with the PDPL.

While determining the destruction periods of your personal data, we take into account the following criteria:

- The period accepted as a general practice in the sector where the data controller operates for purposes of processing of relevant data category,
- The period that requires the processing of personal data in the relevant data category, during which the legal relationship established with the relevant person will continue,
- The period during which the legitimate interest to be derived by the data controller will continue in accordance with the law and good faith, depending on the purpose of processing the relevant data category,
- The period during which the risks, costs and responsibilities to be generated by storing the relevant data category will continue legally depending on the purpose of processing,
- Whether the maximum period to be determined is suitable for keeping the relevant data category accurate and up-to-date when necessary,
- The period during which the data controller is obliged to keep the personal data falling into in the relevant data category in accordance with its legal obligations,
- The statute of limitations determined by the data controller for making a claim based on personal data falling into the relevant data category.

HOW DO WE DESTRUCT YOUR PERSONAL DATA?

Although personal data is processed in accordance with Article 138 of the Turkish Penal Code and Article 7 of the PDPL, in case the reasons requiring the processing thereof disappear, such personal data will be deleted, destroyed or anonymized at the discretion of our Company or upon a respective request of the data subject

In this context, the Personal Data Storage and Disposal Policy has been drafted. Our company reserves the right not to fulfil the request of a data subject in cases where it has the right and / or obligation to preserve personal data in accordance with the provisions of the relevant legislation. When personal data are processed by non-automatic means, provided that they are part of any data recording system, the physical destruction of personal data is performed in a way such personal data cannot be used later. When our company agrees with a person or entity for processing personal data on its behalf, the personal data shall be securely deleted by these persons or entities in a way that such personal data cannot be recovered any more. Our company may anonymize personal data when the reasons requiring the processing of personal data processed disappear in accordance with the law.

METHODS OF DESTRUCTING PERSONAL DATA

Deletion of Personal Data

Although personal data is processed in accordance with the provisions of the relevant law, in the event that the reasons requiring the processing thereof disappear, our Company may delete personal data at its own discretion or at the request of the data subject. Deletion of personal data is the process of making personal such data inaccessible and unavailable in any way for the relevant users. Our company takes all necessary technical and administrative measures to ensure that the deleted personal data are inaccessible and unavailable for the relevant users.

Destruction of Personal Data

Although personal data is processed in accordance with the provisions of the relevant law, in the event that the reasons requiring the processing thereof disappear, our Company may destroy personal data at its own discretion or at the request of the data subject. The destruction of personal data is the process of making personal data inaccessible, retrievable and reusable in any way. The data controller is obliged to take all necessary technical and administrative measures regarding the destruction of personal data.

Physical Destruction: Personal data may be processed in non-automatic ways, provided that they are a part of any data recording system. While such data is deleted / destroyed, the physical destruction of personal data in a way that cannot be used later is performed.

Secure Deletion from Software: While the data that is processed in fully or partially automatic ways and stored in digital media is deleted / destroyed, methods for deleting data from the relevant software in a way that cannot be recovered again are used.

Secure Deletion by a Professional: In some cases, a professional may hired to delete personal data on behalf of the company. In this case, the personal data are securely deleted / destroyed by the person skilled in this field so that such personal data cannot be recovered again.

Dimming: It means making personal data physically unreadable.

Making Personal Data Anonymous

Anonymization of personal data means making such personal data unrelated to a certain or identifiable natural person under any circumstances, even by matching with other data. Our company can anonymize personal data when the reasons requiring the processing of personal data that are legally processed disappear. In order for any personal data to be anonymized, the personal data must be rendered unrelated to any identified or identifiable natural person, even through the use of appropriate techniques in terms of recording medium and relevant field of activity, such as the return of 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.

In accordance with Article 28 of the PDPL, anonymized personal data can be processed for purposes such as research, planning and statistics. Such processing activities are outside the scope of the PDPL, and the explicit consent of the personal data subject will not be sought in this regard.

HOW DO WE PROTECT YOUR PERSONAL DATA?

Necessary administrative and technical measures are taken by our Company in line with the Personal Data Security Guide as published by the Personal Data Protection Authority, and relevant procedures are organized within the Company with disclosure and explicit consent texts drafted in order to protect your personal data and prevent any unlawful access thereto. Necessary inspections are carried out or outsourced to ensure the implementation of the provisions of the PDPL in accordance with Article 12/3 of the PDPL. These audit results are evaluated within the scope of the internal functioning of the Company and necessary actions are taken to improve the measures taken.

Your personal data mentioned above may be transferred to the physical archives and information systems of our Company and / or our suppliers, and they can be kept in both digital and physical environments. Technical and administrative measures taken to ensure the security of personal data are explained in detail below under two headings.

Technical Measures

We use generally accepted standard technologies and business security methods, including standard technology called Secure Socket Layer (SSL), for the protection of 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 applications 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, tampering, unauthorized disclosure or unauthorized access. In this context, we conclude agreements regarding data security with the service providers.

1) Ensuring Cyber Security: We use cyber security products to ensure personal data security, but the technical measures we take are not limited to such products. With measures such as firewalls and gateways, the first line of defense against attacks from environments such as the Internet is established. However, almost all software and hardware are subjected to some installation and configuration processes. Considering that some commonly used software, especially older versions, may have documented security vulnerabilities, unused software and services are removed from the devices. For this reason, deletion of unused software and services rather than keeping them up-to-date is preferred primarily because of its ease. With patch management and software updates, it is ensured that software and hardware work properly and that the security measures taken for the systems are checked regularly.

2) Access Restrictions: Access authorizations to systems containing personal data are restricted and regularly reviewed. In this context, employees are given access to the extent necessary for their job and duties, as well as their powers and responsibilities, and access to relevant systems is provided by using a username and password. While generating the said passwords and passwords, it is ensured that combinations consisting of uppercase letters, numbers and symbols are preferred instead of numbers or letter strings that are associated with personal information and are easy to guess. Accordingly, access authorization and control matrix is created.

3) Encryption: In addition to the use of strong passwords, limiting the number of password entry attempts to protect against common attacks such as the use of brute force algorithm (BFA), ensuring that passwords and passwords are changed at regular intervals, initiating the administrator account and admin authorization only when needed, deleting accounts and blocking the entries without losing time for employees who are dismissed from the data controller are among the methods that are used to restrict access

4) Anti Virus Software: In order to protect against malicious software, products such as antivirus and antispam are used that regularly scan the information system network and detect threats, and they are kept up to date and the required 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 with SSL or a more secure way.

5) Monitoring of Personal Data Security: Activities are performed such as checking which software and services are running in information networks, determining whether there are any intrusions or any other undesired events in information networks, logging activities of all users regularly (such as log records), reporting security problems as quickly as possible. Again, a formal reporting procedure is established for employees to report security weaknesses in systems and services or threats that use them. Evidence is collected and securely stored about unwanted events such as the crash of the information system, malicious software, decommissioning attacks, incomplete or incorrect data entries, violations that disrupt privacy and integrity, and abuse of the information system.

6) Ensuring the Security of Media Containing Personal Data: If personal data is stored on devices located in the campuses 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 (e.g. fire, flood, etc.) with appropriate methods and the entry / exit to these environments is controlled.

   If personal data is contained in electronic environment, access can be restricted between network components or components are separated in order to prevent security breaches of personal data. For example, if personal data is processed in this area by restricting it to a certain part of the network that is used only for this purpose, available resources may be reserved for the purpose of securing this limited area, not for the entire network.

   Measures at the same level are also taken for paper media, electronic media and devices that are located outside the Company campus and that contain personal data belonging to the Company. As a matter of fact, although personal data security violations are often caused by theft and loss of devices containing personal data (e.g. laptop, mobile phone, flash disk, etc.), personal data to be transferred by e-mail or mail are also sent carefully and by taking sufficient precautions. In case the employees access the information system network with their personal electronic devices, adequate security measures are taken for them as well.

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

   Documents available in paper environment 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 such documents is prevented.

   Our company informs the Personal Data Protection Board and data subjects as soon as possible if any personal data are obtained by third parties illegally in accordance with Article 12 of the PDPL. The Personal Data Protection Board may announce such situations on the website or by any other method if it deems necessary.

7) Storing Personal Data in the Cloud: In case of storing personal data in the cloud, the Company should evaluate whether the security measures taken by the cloud storage service provider are sufficient and appropriate. In this context, two-step authentication control is applied for knowing in detail what the personal data stored in the cloud is, and for backing up, ensuring synchronization and remote access to these personal data if required. During the storage and use of personal data in these systems, it is ensured that personal data are encrypted using cryptographic methods, are encrypted and disposed of in cloud environments, and where possible for personal data, in particular, separate encryption keys are used for each cloud solution service is provided. When the cloud computing service relationship ends, all copies of encryption keys that could be used to make personal data usable are destroyed. Access to data storage areas where personal data is stored are logged and inappropriate access or access attempts are instantly communicated to those concerned.

8) Procurement, Development and Maintenance of Information Technology Systems: Security requirements are taken into consideration while determining the needs of the company regarding the procurement, development or improvement of new systems.

9) Backing Up Personal Data: In cases where personal data is damaged, destroyed, stolen or lost for any reason, the Company ensures that the data is backed up as soon as possible. Backed up personal data can only be accessed by the system administrator, and data set backups are excluded from the network.

Administrative Measures

- All activities carried out by our company were analyzed in detail for all business units and as a result of this analysis, a process-based personal data processing inventory was 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 the PDPL have been prepared by considering the risks in this inventory)
- Personal data processing activities carried out by our company are audited using information security systems, technical systems and legal methods. Policies and procedures regarding personal data security are determined and regular controls are carried out in this regard.
- 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 activities are conducted by making sure that the said external service providers at least comply with the security measures provided by our Company. In this case, at least the following issues are included in the contract signed with the Data Processor:
    - The Data Processor acts only in accordance with the Data Controller's instructions in accordance with the purpose and scope of data processing as specified in the contract and in accordance with the PDPL and other legislation,
    - It acts in accordance with the Personal Data Storage and Destruction Policy,
    - The Data Processor is subject to an indefinite confidentiality obligation regarding the personal data processed,
    - In case of any data breach, the Data Processor is obliged to notify the Data Supervisor immediately about the breach
    - The fact that our Company will make or cause to be made the necessary audits on the systems of the Data Processor containing personal data, and may examine the reports resulting from the audits and perform on-site examinations of the service provider company,
    - It will take necessary technical and administrative measures for the security of personal data; and
    - In addition, to the extent permitted by the nature of the relationship between the Data Processor and us, the categories and types of personal data transferred to the Data Processor are also specified in a separate article.
- As the Authority emphasizes in its relevant guides and publications, personal data collected are reduced as much as possible, and any personal data that are unnecessary, or are outdated, or do not serve any purpose are not collected, and any such personal data collected at any time prior to the adoption of the PDPL is destroyed pursuant to the principle of data minimization.
- Personnel who are experts in technical matters are employed.
- Our company includes provisions regarding confidentiality and data security in employment agreements to be executed during the recruitment process of its employees, and asks employees to comply with these provisions. Employees are regularly informed and trained on the law on protection of personal data and taking necessary measures in accordance with this law. The roles and responsibilities of the employees were reviewed and their job descriptions were revised in this regard.
- Technical measures are taken in line with technological developments, and the measures taken are periodically checked, updated and renewed.
- Access authorizations are restricted and authorizations are regularly reviewed.

- The technical measures taken are regularly reported to the officials, and efforts are made to fiend the necessary technological solutions by reviewing issues that pose a risk.
- Software and hardware including antivirus systems and firewalls are installed.
- Backup programs are used to ensure the safe storage of personal data.
- Security systems are used for storage areas; technical measures taken are periodically reported to the relevant person as required by internal controls; and issues that pose a risk are re-evaluated and necessary technological solutions are found. Files / outputs stored in physical environment are stored by supplier companies worked with and then destroyed in accordance with applicable procedures.
- The issue of personal data protection is also assumed by the senior management, and a special Committee (Personal Data Protection Committee) has been established and started to work in this regard. A management policy regulating the operating rules of the Company's Personal Data Protection Committee has been put into effect within the Company with the duties of the Personal Data Protection Committee 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 adopted and put into effect.

Article 6 of the PDPL classifies any data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, dress, memberships to associations, foundations or unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data, as sensitive personal data since such data bear the risk of causing victimization or discrimination of individuals if they are processed unlawfully, and stipulates more strict protective measures for the processing of such sensitive personal data

Our company makes disclosures to the relevant persons during the acquisition of sensitive personal data in accordance with Article 10 of the PDPL. Sensitive personal data are processed by taking measures in accordance with the PDPL and by carrying out the necessary inspections. As a rule, one of the conditions for processing special personal data is the explicit consent of the data subject. Our company offers data subjects an opportunity to express their explicit consent on a specific subject, based on information and with free will.

As a rule, our company obtains the express consent of the relevant persons in writing for the processing of sensitive personal data. However, in the presence of any of the conditions specified in Article 5/2 of the PDPL, the explicit consent of the relevant persons is not required in accordance with Article 6/3 of the PDPL. In addition, Article 6/3 of PDPL stipulates that personal data on health and sexual life may be processed by individuals who are bound by an obligation to keep confidential information as such, or by any authorized bodies and entities without the explicit consent of the person concerned for the purpose of protecting the public health, delivering preventive medicine, medical diagnosis, treatment and healthcare services, and planning, managing, and financing healthcare services. Regardless of the reason, the general principles of data processing are always taken into consideration with respect to processing activities, and compliance with these principles is ensured.

Our company takes special measures to ensure the security of sensitive personal data. In accordance with the principle of data minimization, sensitive personal data are not collected unless necessary for the relevant business process, and such sensitive personal data are processed only when necessary. In case of processing sensitive personal data, necessary technical and administrative measures are taken to comply with

applicable legal obligations and to comply with the measures determined by the Personal Data Protection Board.

WHAT ARE YOUR RIGHTS REGARDING YOUR PERSONAL DATA?

In accordance with Article 11 of the PDPL, as a data subject you have the following rights:

- To know whether your personal data has been processed by our Company,
- To request information if your personal data has been processed,
- To know the purpose of processing your personal data and whether they have been used appropriately for their intended purposes,
- To know the third parties in the country or abroad to whom your personal data has been transferred,
- To request the correction of your personal data in case of any incomplete or incorrect processing, and to request the notification of such corrections to any third parties to whom your personal data has been transferred,
- To request the deletion or destruction of your personal data in the event that the reasons requiring the processing thereof have disappeared, despite the fact that it has been processed in accordance with the provisions of the PDPL and other relevant laws, and to request the notification of such deletion or destruction activities to any third parties to whom your personal data has been transferred,
- To object to the emergence of any results against you through analysis of the processed data exclusively through automated systems
- To request the compensation of any damages and losses you have suffered due to unlawful processing of your personal data.

In accordance with the Communiqué on Filing Applications, you may send these requests to our Company free of charge by the following method:

1) You may complete and wet sign a form available at www.makyol.com.tr, and deliver it personally at the following address: Makyol İnşaat Sanayi Turizm ve Ticaret A.Ş. Etiler Mahallesi, Tepecik Caddesi, Melodi Sokak İ.T.Ü. Blokları E Blok, 34337 Beşiktaş/İstanbul (we would like to remind you that your identity will need to be presented).

2) You may complete and wet sign a form available at www.makyol.com.tr, and send it to the following address via a notary public: Makyol İnşaat Sanayi Turizm ve Ticaret A.Ş. Etiler Mahallesi, Tepecik Caddesi, Melodi Sokak İ.T.Ü. Blokları E Blok, 34337 Beşiktaş/İstanbul

3) You may complete and sign a form available at www.makyol.com.tr with a secure electronic sign pursuant to the Electronic Signature Law No.5070, and email it to **makyol@hs03.kep.tr** from your registered email address

4) You may submit a writing letter from your e-mail address that has been previously notified to our company and registered in our Company's system.

The application must contain name and surname; signature if the application is submitted in writing ; Turkish ID number for the citizens of the Republic of Turkey; the nationality, passport number or identification number, if any, for foreigners; place of residence or workplace address for notification; e-mail address, telephone and fax numbers for notification; and subject of the request. Information and documentation related to the subject shall also be attached to the application.

It is not possible to make requests by third parties on behalf of personal data subjects. In order for a person other than the personal data subject to make a request, a wet signed and notarized copy of a special power of attorney issued by the personal data subject in the name of the person who will make the application must be available. In the application which is to be filed to use your rights mentioned above as a data subject and which contains your explanations regarding the right you are to use, the subject of your request must be clear and understandable; the subject matter must be related to your person; or if you are acting on behalf of someone else, you must be specially authorized in this regard based on certification of such authorization; the application must include your identity and address details; and documents that prove your identity must be attached to the application.

Any application filed will be finalized in the shortest possible period of time but not later than 30 days in any event. These applications may be filed free of charge. However, if the transaction requires an additional cost, the amounts set out in the tariff issued by the Personal Data Protection Board may be charged.

If the personal data subject submits his/her request to our Company in accordance with the prescribed procedure, our Company will finalize the request free of charge as soon as possible and within thirty days at the latest, depending on the nature of the request. However, in case the transaction requires an additional cost, the amount set out in the tariff issued by the Personal Data Protection Board will be collected from the applicant by our Company. Our company may request information from the person concerned in order to determine whether the applicant is the subject of the personal data in question. In order to clarify the matters included in the application of the personal data subject, our company may ask questions to the personal data subject about his/her application.

In case your application is rejected by our Company in accordance with Article 14 of PDPL, or you find our answers insufficient, or we do not respond to the application in time, you may file a complaint to the Personal Data Protection Board within thirty days from the date you receive the response of our company, and in any case within sixty days from the date of application.

WHAT ARE THE SITUATIONS WHERE DATA SUBJECTS CANNOT CLAIM THEIR RIGHTS?

Personal data subjects may not claim the above-mentioned rights of personal data subjects in the following situations since such situations are excluded from the scope of PDPL in accordance with Article 28 of the PDPL:

- Processing 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 do not violate national defense, national security, public security, public order, economic security, privacy of private life or personal rights or they do not constitute a crime.
- Processing of personal data in connection with preventive, protective and intelligence activities carried out by public bodies and entities authorized by law to ensure national defense, national security, public security, public order or economic security.
- Processing of personal data by judicial authorities or execution authorities in connection with investigation, prosecution, trial or execution proceedings.

In accordance with the article 28/2 of the PDPL, personal data subjects cannot assert their other rights in the cases listed below, except the right to claim compensation:

- Processing of personal data is necessary for the prevention of any crime or for a criminal investigation.
- Processing of personal data made public by the personal data subject.
- Processing of personal data is necessary for the execution of supervision or regulation duties and for disciplinary investigation or prosecution by the authorized public bodies and entities or by professional organizations having the status of a public entity, based on the authority granted by the law.
- Processing of personal data is necessary for the protection of the economic and financial interests of the State regarding budget, tax and financial issues.

MISCELLANEOUS

As explained in detail above, your personal data can be stored and preserved, classified in connection with market research, financial and operational processes and marketing activities, updated in different periods and, to the extent permitted by the legislation, transferred to any third parties and / or suppliers and / or service providers as required by the service and / or our foreign shareholders within the framework of laws and confidentiality principles, revealed and stored in accordance with the policies to which we are subject and for the reasons stipulated by other authorities, and processed by means of reports, and used to organize records and documents as a basis for electronic or paper processing.

In case of any inconsistencies between the provisions of PDPL and other relevant legislation on one part and this Policy on the other part, the provisions of the PDPL and other relevant legislation will govern.

This Policy drafted by our company entered into force pursuant to a decision taken by the Board of Directors of Makyol.

We would like to remind you that we may make updates in this Policy due to the legislative provisions that may change over time or due to any changes that may occur in our company's policies. We will post the most up-to-date version of the Policy on our website.

The Users hereby irrecoverably agree, declare and undertake that they have read this Personal Data Protection Policy before entering the website, that they will comply with all the requirements set out herein, and that the content available at the website and all electronic media and computer records of our Company will be deemed as definitive evidence in accordance with Article 193 of the Code of Civil Procedure

Effective Date: 1.1.2021

Version: 1.1.

ANNEX - ABBREVIATIONS

ABBREVIATIONS	
The Law No.5651	The Law on Regulating Publications on the Internet and Combating Crimes Committed Through These Publications, as published in the Official Gazette No. 26530 dated May 23, 2007
Constitution	Constitution of the Republic of Turkey dated November 7, 1982 and Numbered 2709, published in the Official Gazette No. 17863 dated November 9, 1982
Application Communiqué	Communiqué on Application Procedures and Principles for Data Controllers, which entered into force after being published in the Official Gazette dated March 10, 2018 and numbered 30356
Relevant Person(s) or Data Subject	Any real persons whose personal data are processed, including but limited to customers of Makyol and / or Makyol's affiliates; their corporate customers, business partners, shareholders, officials, candidate employees, interns, visitors, and suppliers; employees of entities with which they maintain a cooperation; and any other third parties
Regulation on the Deletion, Destruction or Anonymization of Personal Data	Regulation on the Deletion, Destruction or Anonymization of Personal Data, published in the Official Gazette dated 28 October 2017 and numbered 30224, which became effective as of January 1, 2018
PDPL	Law on Protection of Personal Data, published in the Official Gazette dated April 7, 2016 and numbered 29677
PDP Board	Personal Data Protection Board
PDP Authority	Personal Data Protection Authority
Art.	Article
Ex.	Example
Policy	This Personal Data Protection and Privacy Policy of Makyol
Company/ Makyol	Makyol İnşaat Sanayi Turizm ve Ticaret A.Ş.
Turkish Penal Code	Turkish Penal Code numbered 5237 and dated September 26, 2004, published in the Official Gazette numbered 25611 and dated October 12, 2004