POLICY ON PROTECTION, STORAGE, TRANSFER AND DESTRUCTION OF PERSONAL DATA by MARMARA ULUSLARARASI İNŞAAT VE TİCARET ANONİM ŞİRKETİ

1. INTRODUCTION

Law No. 6698 on the Protection of Personal Data ("Law"), which entered into force after its publication in the Official Journal dated 07.04.2016, regulates the protection of fundamental rights and freedoms of individuals, especially the privacy of private life, while processing personal data, as well as the obligations of data controllers who collect and process data, and the procedures and principles they are bound by. "Policy on Protection, Storage, Transfer, and Destruction of Personal Data by Marmara Uluslararası İnşaat ve Ticaret Anonim Şirketi" has been established to implement the law and its implementing regulations, the resolutions adopted by the Personal Data Protection Authority, and to describe the duties and responsibilities of the public and Company employees.

2. PURPOSE and SCOPE

The Policy on Protection, Storage, Transfer, and Destruction of Personal Data by Marmara Uluslararası İnşaat ve Ticaret Anonim Şirketi has been prepared to be enforced for the Company, managers, employees, customers, and all persons who establish a relationship with the Company.

This Policy sets out the rules and principles in order to serve the rights to privacy and inviolability of private life of all natural persons who establish a relationship with the Company and the rights to protection of personal data protected by the Law. Any violation of the Policy implies that the Company has violated the Law as it acts as the registered Data Controller; therefore, violation of Policy on Protection, Storage, Transfer, and Destruction of Personal Data by Marmara Uluslararası İnşaat ve Ticaret Anonim Şirketi by employees shall be deemed to breach discipline.

3. DEFINITIONS

For all documents and activities in this Policy and Law on the Protection of Personal Data, the following definitions shall apply:

a. Explicit consent: freely given, specific and informed explicit,
b. Anonymizing: rendering personal data impossible to link with an identified or identifiable natural person, even though matching them with other data,
c. Data subject: the natural person, whose personal data is processed,
d. Personal data: all the information relating to an identified or identifiable natural person,
e. Processing personal data: any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means,
f. Authority: the Personal Data Protection Authority,
g. Company: Marmara Uluslararası İnşaat ve Ticaret Anonim Şirketi
h. Data processor: the natural or legal person who processes personal data on behalf of the controller upon his authorization,
i. Data controller: the natural or legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system.

4. GENERAL PRINCIPLES

Personal data may only be processed in compliance with the procedures and principles set forth in Law. The following principles shall be complied with within the processing of personal data: lawfulness and conformity with rules of *bona fides*; accuracy and being up to date, where necessary; being processed for specific, explicit and legitimate purposes; being relevant with, limited to and proportionate to the purposes for which they are processed; being retained for the period of time stipulated by relevant legislation or the purpose for which they are processed.

5. COLLECTION OF AND PROCESSING PERSONAL DATA

The Company collects the personal data detailed below and also in the Personal Data Inventory for establishing a business relationship with the personnel it employs, preparing the personnel and medical files, executing employment contracts, securing workplace and customer safety, concluding contracts for purchase, sale, service procurement and similar contracts with the companies with whom the Company enters into business relations or maintains business relations, executing contracts, fulfilling legal, financial and commercial obligations thereof, and analysing commercial risks, carrying out procurement operations as well as legal and administrative operations and fulfilling the legal obligations set forth in the provisions of the legislation to which the Company is subject, primarily Labor Law No. 4857, Occupational Health and Safety Law No. 6331, Social Insurance and General Health Insurance Law No. 5510, Turkish Commercial Code No. 6102, and Tax Legislation.

a. Our Company collects and processes all kinds of special and general data of our employees digitally and physically under Labor Law No. 4857 and the provisions of the applicable legislation for the purposes specified above and also, in the Corporate Personal Data Inventory.
b. The Company collects and processes data on the identity and contact details as well as data on payment and invoicing instruments of the counterparty legal merchant representatives for the performance of the relevant contracts under the agreements that have been concluded or to be concluded with the companies with which the Company will enter into business relations or with which it maintains business relations.
c. The surveillance cameras in the group hotels keep running in order to maintain the security of the hotels. Additionally, the identity data and contact details of the guests who stay at the group hotels and who intend to benefit from the hotels are processed and stored.
d. The identity data and contact details and signature circulars of the authorized persons and employees of legal entities with which the Company maintains a business relationship are collected and processed in order to carry out the financial and accounting operations of the Company.
e. The grounds, processes, procedures, and all other technical details of the processing of personal data by the Company are specified in the Corporate Personal Data Inventory.

6. EXPLICIT CONSENT FOR PROCESSING PERSONAL DATA

Personal data shall not be processed without the explicit consent of the data subject. The explicit consent must be in writing or provable and must be obtained after the data subject has been informed of the collection, use, transfer, and destruction. The company may process the personal data, without seeking the explicit consent of the data subject, only in cases where one of the following conditions is met:

a. it is clearly provided for by the laws.
b. it is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid,
c. processing of personal data belonging to the parties of a contract is necessary provided that it is directly related to the conclusion or fulfilment of that contract,
d. it is mandatory for the data controller to be able to fulfil his legal obligations.
e. the data is made available to the public by the data subject himself,
f. data processing is mandatory for the establishment, exercise or protection of any right,
g. it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

7. OBLIGATIONS OF THE DATA CONTROLLER

While collecting personal data, the Company, as data controller, or the person authorised by it is obliged to inform the data subjects about the following:

a. the identity of the controller and of his representative, if any,
b. the purpose of data processing;
c. to whom and for what purposes the processed data may be transferred,
d. the method and legal grounds for of collection of

personal data.

The Company, as data controller, are obliged to take all necessary technical and administrative measures to provide a sufficient level of security in order to:

a. prevent unlawful processing of personal data,

b. prevent unlawful access to personal data,
c. ensure the retention of personal data.

8. RIGHTS OF THE DATA SUBJECT

Each person has the right to apply to the controller and

a. to learn whether his personal data are processed or not,
b. to request information if his personal data are processed,
c. to learn the purpose of his data processing and whether this data is used for intended purposes,
d. to know the third parties to whom his personal data is transferred at home or abroad,
e. to request the rectification of the incomplete or inaccurate data, if any,
f. to request the erasure or destruction of his personal data of a special nature, if any,
g. To request notification of the operations carried out to third parties to whom your personal data has been transferred,
h. to object to the processing, exclusively by automatic means, of his personal data, which leads to an unfavourable consequence for the data subject,
i. to request compensation for the damage arising from the unlawful processing of his personal data.

You can send your request for exercising your rights to us by sending it to our mail, fax, or registered e-mail address indicated below with a secure electronic signature, or by filling out the Application Form on our website, or in accordance with the method if the Personal Data Protection Board defines a different method in writing and with a wet signature along with the certificates that prove your identity.
For your requests on Marmara Uluslararası İnşaat ve Ticaret Anonim Şirketi, please find our contact details below:

Address : Türkmen Mah. Gazi Beğendi Bulvarı No.21 Kuşadası/Aydın
Phone : 0256 618 15 30
E-Mail : info@korumar.com.tr

9. TRANSFER OF PERSONAL DATA

Your personal data may be transferred to business partners, shareholders, holdings to which our Company is affiliated, subsidiaries, companies from which our Company procures services as a supplement or extension of its activities, suppliers, subcontractors, banks, ministries, municipalities, support service providers, contracted companies, institutions that cooperate in accordance with the provisions of the legislation, public authorities and bodies, and law enforcement agencies for the purposes set out above and under the applicable legal provisions and the requirements and purposes of processing personal data set out in Articles 8 and 9 of the LPPD.

Personal data shall never be transferred abroad without the explicit consent of the data subject. However, the transfer of personal data abroad, regardless of the explicit consent of the data subject, requires one of the conditions set out in Article 6 above, as well as the following conditions pursuant to Article the LPPD:

a. If sufficient protection is available in the foreign country,
b. Where no sufficient protection is available, if the data controllers in Türkiye and in the respective foreign country undertake to provide sufficient protection in writing and if the data controller holds the clearance of the Authority.

The countries where sufficient protection is available for transfer abroad shall be designated and announced by the Authority. The personal data may be transferred abroad, without prejudice to the provisions of international conventions, in cases where the interests of Türkiye or the data subject would be seriously harmed, but only with the approval of the Authority after consulting the relevant public institution or organization. The provisions set forth in other laws on the transfer of personal data abroad are reserved.

10. MEASURES TAKEN FOR THE PROTECTION OF PERSONAL DATA

Personal data shall be stored in existing and secure physical or electronic mediums available within the Company. Only the persons authorized by the Company shall be allowed access to the data.
Concordantly,

a. The network and application are secured; key management is applied; security measures are taken for procurement, development, and maintenance of information technology systems; access logs are kept regularly; data masking measures are implemented; up-to-date anti-virus systems and firewalls are used; user account management and authorization control systems are implemented; log records are kept regularly; intrusion detection and prevention systems are used; penetration tests are run; cyber security measures are taken; data is encrypted and data loss prevention software is used.
b. Necessary security measures are taken for entry and exit to physical mediums containing personal data; physical mediums containing personal data are secured against any external risks (fire, flood, etc.); mediums containing personal data are secured.
c. Disciplinary regulations involving data security for employees are in force; training and awareness-raising efforts on data security are organized for employees at regular intervals. The authorisations of employees who have changed their duties or left their jobs are revoked.
d. The signed contracts contain data security provisions and include commitments on confidentiality. The personal data are backed up, backed up personal data are also secured, and the personal data security issues are reported quickly.
e. The Company employees shall destruct the personal data for which the purpose and duration of use have lapsed in accordance with their training on the law and the instructions issued by the Company management.

11. PRINCIPLES FOR THE DESTRUCTION OF PERSONAL DATA

a. All kinds of destruction methods can be followed when destruction of personal data; any data in any digital form may either be destructed by permanently erasing the files or by corrupting the data in the digital medium in a way that makes it unreadable. The physical files are primarily preferred to be destructed by incineration.
b. If the grounds for processing personal data have ceased to exist and unless there exists consent for storage, the personal data should be either destructed or anonymized.
c. Despite the prior explicit consent, personal data must be destructed or anonymized upon the request of the data subject.
d. The data must be destructed to make it inaccessible and irreversible.
e. The data controller shall be obliged to carry out the necessary audits or have them carried out in order to implement the provisions of this Law in its own institution or organization.
f. Data controllers and data processors shall neither disclose the personal data they have acquired to anyone else against the provisions of this Law nor use them for purposes other than processing. This obligation shall survive their resignation from office.
g. In the event that the processed personal data is obtained by others through illegal means, the data controller shall notify the data subject and the Authority as soon as possible. If necessary, the Authority may announce the breach on its website or by any other method it deems appropriate.

12. DESTRUCTION PERIODS

The personal data shall be stored for the periods indicated in the table below under the applicable Legislation and the principles set forth in this Policy and shall be anonymized or destructed after the deadline. Since data from the same data category may be processed due to different procedures, the following table has been created by taking into account the longest retention period:

Data Category	Retention Time	Destruction Period
Identity Data (name, surname, date of birth, place of birth, marital status, serial number of identity card, Turkish ID No, signature, etc.)	30 years	Within 180 days after the end of the retention period
Contact Details (work address, home address, personal e-mail, corporate e-mail, contact address, registered electronic mail address (REM), work phone, home phone, cell phone)	30 years	Within 180 days after the end of the retention period
Personnel Data (payroll data, disciplinary proceedings, employment records, property declaration data, CV, performance evaluation reports, leaves, etc.)	10 years following the dissolution of the relationship	Within 180 days after the end of the retention period
Data on Legal Proceedings (information in correspondence with judicial authorities, information in the case file)	10 years	Within 180 days after the end of the retention period
Data on Customer Proceedings (invoice, bill, cheque details, order details, requests)	5 years	Within 180 days after the end of the retention period
Security Data of Physical Space (camera footage)	45 days	Within 180 days after the end of the retention period
Process Security Data (ip addresses, website login and logout details, password and passcodes)	2 years	Within 180 days after the end of the retention period
Finance Data (balance sheets, financial performances, credit and risk profiles, assets, salaries, insurance premiums, bank account details)	10 years	Within 180 days after the end of the retention period
Professional Experience Data (diploma credentials, courses attended, vocational trainings, certificates, transcripts)	10 years following the dissolution of the relationship	Within 180 days after the end of the retention period
Marketing Data (Advertising, surveys, cookie registrations)	3 years	Within 180 days after the end of the retention period
Audiovisual Recording Data (photo)	10 years following the dissolution of the relationship	Within 180 days after the end of the retention period

Philosophical Belief, Religion, Sect and Other Belief Data	10 years following the dissolution of the relationship	Within 180 days after the end of the retention period
Association Membership Data	10 years following the dissolution of the relationship	Within 180 days after the end of the retention period
Foundation Membership Data	10 years following the dissolution of the relationship	Within 180 days after the end of the retention period
Medical Data (disability details, blood groups, personal medical data, information on devices and prostheses in use, medical records, periodic medical examination form for employment)	15 years following the dissolution of the relationship	Within 180 days after the end of the retention period
Criminal Conviction and Security Measure Data (criminal records)	10 years following the dissolution of the relationship	Within 180 days after the end of the retention period
Biometric Data (fingerprint)	Within the periodic destruction time following the dissolution of the relationship	Within 180 days after the end of the retention period