PERSONAL DATA RETENTION AND DESTRUCTION POLICY

PURPOSE AND SCOPE OF THE POLICY

The Personal Data Retention and Destruction Policy (the "Policy") has been prepared by Marmara Cam Sanayi Ve Ticaret Anonim Şirketi (the "Company") to establish the procedures and principles regarding the retention and destruction activities carried out by the Company.

The Personal Data Retention and Destruction Policy (the "Policy") has been prepared by Marmara Cam Sanayi Ve Ticaret Anonim Şirketi (the "Company") to inform you about the processes of deletion, destruction, and anonymization of your personal data after processing such data in accordance with Law No. 6698 on the Protection of Personal Data (the "Law") and related legislation, including the Regulation on the Deletion, Destruction or Anonymization of Personal Data, and after the reasons for processing the data cease to exist or the maximum retention periods prescribed by law expire, and to fulfill the obligations as the data controller.

The Company prioritizes the processing of personal data of its employees, job applicants, service providers, visitors, customers or potential customers of products or services, supplier employees, supplier representatives, and other third parties, in compliance with the Constitution of the Republic of Turkey, international agreements, Law No. 6698 on the Protection of Personal Data, and other relevant legislation, ensuring that the rights of the relevant persons are effectively exercised, in line with the principles set forth by the Law and its mission, vision, and fundamental values.

The processes and procedures related to the retention and destruction of personal data are carried out by the Company in accordance with this Policy.

DEFINITIONS

The terms used in this Policy shall have the following meanings:

- **Recipient Group:** The category of real or legal persons to whom personal data is transferred by the data controller.
- **Explicit Consent:** Consent given freely and explicitly based on information on a specific matter.
- **Anonymization:** The process of rendering personal data in such a way that it cannot be associated with an identified or identifiable natural person, even when combined with other data.
- **Employee:** Company personnel.
- **Electronic Environment:** Environments where personal data can be created, read, modified, or written through electronic devices.
- **Non-Electronic Environment:** All written, printed, visual, and other environments outside electronic environments.
- **Service Provider:** Real or legal persons providing services within the scope of a contract with the Personal Data Protection Authority.
- **Data Subject:** The natural person whose personal data is processed.

- **Relevant User:** Individuals within the data controller's organization who process personal data, excluding those responsible for technical storage, protection, and backup, or those authorized and instructed by the data controller.
- **Destruction:** The deletion, destruction, or anonymization of personal data.
- **Law:** Law No. 6698 on the Protection of Personal Data.
- **Record Environment:** Any environment where personal data is processed wholly or partially by automated means or manually as part of any data recording system.
- **Personal Data:** Any information relating to an identified or identifiable natural person.
- **Personal Data Processing Inventory:** An inventory created by data controllers detailing their personal data processing activities in relation to business processes; including purposes, legal reasons, data categories, recipient groups, maximum retention periods, transfer to foreign countries, and data security measures.
- **Processing of Personal Data:** Any operation performed on personal data such as collection, recording, storage, retention, modification, rearrangement, disclosure, transfer, acquisition, classification, or prevention of use, either by automated or manual means.
- **Board:** Personal Data Protection Board.
- **Authority:** Personal Data Protection Authority.
- **Special Categories of Personal Data:** Data relating to a person's race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, clothing and appearance, membership in associations, foundations or unions, health, sexual life, criminal convictions and security measures, biometric and genetic data.
- **Periodic Destruction:** Deletion, destruction, or anonymization performed periodically by the data controller when the conditions for processing personal data are no longer met.
- **Policy:** The Policy on the Processing, Retention, and Destruction of Personal Data.
- **Data Processor:** A real or legal person processing personal data on behalf of the data controller under authorization.
- **Data Recording System:** A system in which personal data is structured and processed according to specific criteria.
- **Data Controller:** The real or legal person who determines the purposes and means of processing personal data and responsible for establishing and managing the data recording system.
- **Data Controllers Registry Information System (VERBIS):** An online information system created and managed by the Presidency for data controllers to apply to the Registry and perform related transactions.
- **Regulation:** The Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated October 28, 2017.

RESPONSIBILITIES AND TASK DISTRIBUTION

In cases where personal data is processed on behalf of the Company by another real or legal person, the Company as the data controller and the data processors are jointly liable before administrative authorities and relevant persons for taking data security measures according to the law. Accordingly, data processors are responsible at a minimum for implementing the measures taken by the Company and complying with the destruction periods and methods stated herein. As the data controller, the Company periodically audits the compliance of data processors with the Personal Data Protection legislation, administrative decisions, and judicial

rulings to ensure that the trust provided to the Company and the sharing of personal data with business partners, suppliers, and contractors is maintained in the same manner.

The Company acts in accordance with the following principles regarding the retention and destruction of personal data:

- The deletion, destruction, and anonymization of personal data are conducted fully in compliance with the Law, related legislation, Board decisions, and this Policy.
- All operations regarding the deletion, destruction, and anonymization of personal data are recorded by the Company and such records are kept for the periods specified in Article 8, excluding other legal obligations.
- Unless otherwise decided by the Board, the Company selects the appropriate method among deletion, destruction, or anonymization to erase personal data ex officio. However, upon request of the relevant person, the appropriate method will be selected with justification.
- When all conditions for the processing of personal data as set out in Articles 5 and 6 of the Law cease to exist, personal data shall be deleted, destroyed, or anonymized by the Company ex officio or upon the request of the relevant person. In this regard, if the relevant person applies to the Company:
    - Requests are answered within a maximum of 30 (thirty) days.
    - If the data subject's personal data has been transferred to third parties, the third parties are notified, and necessary actions are taken with them.

All departments and employees of the Company actively support the responsible units in properly implementing the technical and administrative measures taken under this Policy, training and increasing the awareness of unit employees, monitoring and continuous auditing, preventing unlawful processing and access to personal data, and ensuring lawful storage of personal data by taking technical and administrative measures to ensure data security in all environments where personal data is processed.

The titles, departments, and job descriptions of those responsible for retention and destruction processes are listed in Table 1.

TITLE	DEPARTMENT	DUTY
COMPANY DIRECTOR / CHAIRMAN OF THE BOARD	COMPANY	Responsible for employees acting in accordance with the Policy.
GENERAL MANAGER	MARMARA CAM INDUSTRY AND TRADE INC. MANAGEMENT	Responsible for all departments, units, and employees acting in accordance with the Policy within the Company.
HUMAN RESOURCES MANAGER	HUMAN RESOURCES DEPARTMENT	Responsible for preparing, developing, implementing, publishing in relevant environments, updating the Policy, and providing necessary technical solutions for its implementation.

Table 1: Task distribution for retention and destruction processes

RECORDING ENVIRONMENTS

The general environments used for storing personal data are listed below. However, some data may be stored in different environments due to their special nature or legal obligations. The Company acts as the data controller and processes and protects personal data in compliance with the Law, the Personal Data Processing and Protection Policy, and this Personal Data Retention and Destruction Policy.

Non-electronic environments:
Paper, manual data recording systems (participant forms, survey forms, visitor logs, authorized dealer forms, human resources forms and petitions, etc.), written, printed, visual environments, department cabinets, archive areas.

Electronic environments:
Personal computers, servers, information security devices (firewalls, intrusion detection and prevention systems, log files, antivirus software, etc.), mobile devices, software, fixed or portable disks, optical disks, and other digital environments within the Company.

Cloud environments:
Internet-based systems used by the Company but not physically located within it, employing cryptographic methods.

Table 2: Environments where personal data is recorded

EXPLANATIONS REGARDING RETENTION AND DESTRUCTION

The Company stores and destroys personal data of employees, job applicants, service providers, visitors, customers or potential customers, supplier employees, supplier representatives, and other third parties in compliance with the Law.

Detailed explanations regarding retention and destruction are given below.

5.1. EXPLANATIONS REGARDING PERSONAL DATA RETENTION

Article 3 of the Law defines the concept of personal data processing; Article 4 states that processed personal data should be relevant, limited, and proportionate to the purposes for which they are processed, and must be retained only for the time required by relevant legislation or the processing purpose. Articles 5 and 6 list the conditions for processing personal data.

Accordingly, personal data processed within the scope of the Company's activities are retained for the periods prescribed by relevant legislation or suitable to the processing purposes.

5.1.1. Legal Reasons Requiring Retention

Personal data processed within the Company's activities are retained for periods prescribed by relevant legislation, including but not limited to:

- Law No. 6698 on the Protection of Personal Data
- Turkish Code of Obligations No. 6098
- Social Insurance and General Health Insurance Law No. 5510
- Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications
- Occupational Health and Safety Law No. 6331
- Labor Law No. 4857
- Regulation on Health and Safety Measures to be Taken in Workplaces and Annexes
- Turkish Commercial Code No. 6102

Retention periods prescribed by these laws and secondary regulations in force are observed.

5.1.2. Processing Purposes Requiring Retention

The Company retains personal data processed within its activities for the following purposes:

- Conducting human resources processes,
- Planning and fulfilling employee rights and benefits,
- Ensuring the Company's commercial operations,
- Maintaining corporate communication,
- Ensuring company security,
- Contacting real/legal persons with whom the Company has a business relationship,
- Managing customer relations,
- Performing statistical studies,
- Executing tasks and transactions arising from signed contracts and protocols,
- Fulfilling legal obligations required or mandated by legislation,
- Contacting real/legal persons involved in business relations with the Company,
- Resolving requests and complaints of data subjects within the scope of the Personal Data Protection Law,
- Ensuring technical measures are taken under the Law (data backup, deletion/destruction recording, access log records, etc.),
- Evidence preservation for potential future legal disputes.

Personal data is securely retained in physical or electronic environments within the limits set by the Law and other relevant legislation.

5.2. REASONS REQUIRING DESTRUCTION

Personal data shall be deleted, destroyed, or anonymized by the Company ex officio or upon the data subject’s request in the following cases:

- Amendment or repeal of the relevant legislation that constitutes the legal basis for processing,
- Elimination of the purpose that requires the processing or storage of the data,
- Withdrawal of explicit consent by the data subject when processing is based solely on explicit consent,
- Acceptance by the Personal Data Protection Board or a judicial decision regarding the data subject's application for deletion or destruction of personal data under Article 11 of the Law,
- When the Company rejects the data subject's request for deletion, destruction, or anonymization of their personal data, finds its response insufficient, or fails to respond within the legally prescribed period; the data subject files a complaint with the Personal Data Protection Board and the request is deemed appropriate by the Board,
- Expiration of the maximum legal retention period without any justifiable reason to retain the personal data longer.

ENSURING THE SECURITY OF PERSONAL DATA

To ensure the secure storage of personal data, prevent unlawful processing and access, and ensure lawful destruction, the Company takes necessary technical and administrative measures in accordance with Article 12 and the fourth paragraph of Article 6 of the Law, as well as the sufficient measures announced by the Board for special categories of personal data.

6.1 ADMINISTRATIVE MEASURES TAKEN

The Company applies the following administrative measures according to the nature of the data and the storage environment:

- Confidentiality obligations and secrecy clauses are included in employment contracts.
- Disciplinary procedures for employees who violate security policies and procedures are established.
- Framework agreements or confidentiality undertakings are signed with data recipients to ensure data protection and security.
- Personal Data Inventory is prepared and regularly updated.
- Information obligations towards data subjects are fulfilled.
- Procedures to ensure the security of special categories of personal data are defined and implemented.
- Data minimization principles are applied.
- Additional security measures are applied to paper-based personal data, and documents are sent as confidential.
- Unauthorized acquisition of personal data is reported promptly to the data subject and the Board.
- Awareness and training programs on information security, personal data, and privacy are conducted for all employees with access to personal data.
- Legal and technical consultancy is obtained to follow developments and take necessary actions regarding information security and data protection.

- Physical security measures are implemented for data storage areas to protect against external risks (fire, flood, etc.).
- Periodic and random internal audits are conducted.

6.2 TECHNICAL MEASURES TAKEN

The Company takes the following technical measures based on the nature of data and storage environment:

- Penetration tests are conducted to identify risks and vulnerabilities in IT systems and necessary precautions are taken.
- Continuous monitoring of risks and threats affecting system continuity is done through real-time information security event management.
- Access control and authorization to IT systems are managed via access-right matrices and security policies through corporate active directory.
- Physical security of IT equipment, software, and data is ensured.
- Environmental and hardware security measures include access control systems, 24/7 monitoring, secure LAN switches, fire suppression, and climate control systems.
- Software security measures include firewalls, intrusion prevention, network access control, and malware protection.
- Risks of unlawful processing of personal data are identified and mitigated through appropriate technical controls.
- Access procedures and reporting for personal data access are established and monitored.
- Access logs to storage areas of personal data are recorded to control unauthorized access attempts.
- Deleted personal data are made inaccessible and unusable by authorized users.
- Systems and infrastructure are in place to notify relevant persons and the Board of unlawful data acquisition.
- Security patches are applied and information systems are kept up to date.
- Strong passwords are used in electronic environments processing personal data.
- Secure logging systems are used for record-keeping.
- Backup programs ensure secure storage of personal data.
- Access to personal data in electronic or non-electronic environments is limited based on access principles.
- The Company website uses secure protocols (HTTPS) with SHA 256 Bit RSA encryption.
- A separate policy exists for special categories of personal data security.
- Employees handling special categories receive training, sign confidentiality agreements, and their access rights are defined.
- Special category personal data stored and processed electronically is protected using cryptographic methods; keys are securely stored, logs maintained, and security updates and tests are regularly conducted.
- Physical security measures prevent unauthorized entry to physical storage of special category data.
- Special category data transferred by email is encrypted using corporate email or KEP accounts; transfers via portable media are encrypted with keys stored separately;

server-to-server transfers use VPN or sFTP; paper documents are sent with confidentiality and protected against theft or loss.

PERSONAL DATA DESTRUCTION TECHNIQUES

At the end of legally prescribed retention periods or when data is no longer needed for its purpose, the Company destroys personal data ex officio or upon request using the following methods compliant with relevant legislation.

7.1 DELETION OF PERSONAL DATA

DATA STORAGE MEDIUM	DESCRIPTION
Personal Data on Servers	Access rights are revoked by system administrators and data deleted once retention period ends.
Personal Data in Electronic Environments	Data is made inaccessible and unusable for all except database administrators after retention period.
Personal Data in Physical Environments	Access restricted except to archive manager; documents are irreversibly crossed out, painted over, or erased.
Personal Data on Portable Media	Data is encrypted and stored securely with access only to system administrator after retention period.
Cloud Solutions (e.g., Office 365)	Deletion commands are executed ensuring no recovery rights remain for deleted data.

7.2 DESTRUCTION OF PERSONAL DATA

DATA STORAGE MEDIUM	DESCRIPTION
Personal Data in Physical Environments	Paper documents are shredded irreversibly after retention period.
Personal Data on Optical/Magnetic Media	Media is physically destroyed by melting, burning, or pulverizing; magnetic media is exposed to strong magnetic fields to render data unreadable.

7.3 ANONYMIZATION OF PERSONAL DATA

Anonymization ensures personal data cannot be linked to an identified or identifiable natural person, even when combined with other data.

Techniques used may include:

- **Removal of Identifiers:** Deleting direct identifiers from personal data.
- **Masking:** Concealing parts of data (e.g., with asterisks).
- **Regional Hiding:** Deleting distinguishing information from aggregated data.
- **Generalization:** Aggregating data and removing identifiers to create statistical data.
- **Data Derivation:** Transforming data into more general content.
- **Noise Addition:** Adding controlled distortion to numerical data to prevent identification.

Under Article 28 of the Law, anonymized data may be processed for research, planning, and statistical purposes without requiring explicit consent.

The Company may decide ex officio to delete, destroy, or anonymize data and freely choose appropriate methods, including when requested by data subjects.

RETENTION AND DESTRUCTION PERIODS

Retention periods per data item are maintained in the Personal Data Processing Inventory, VERBIS registry, and this Policy. Destruction methods depend on data nature and importance.

Data retention is regularly reviewed for compliance with Law's principles. Data violating principles is deleted, destroyed, or anonymized.

Exceptions under Articles 5 and 6 of the Law are identified, and reasonable retention periods determined. After expiry, data is deleted, destroyed, or anonymized.

8.1 REQUESTS FOR DELETION OR DESTRUCTION OF PERSONAL DATA AND TIMEFRAMES

Upon a written request from the data subject using the Company's preferred form or other Board-approved methods:

- If conditions for data processing have ceased, the Company deletes, destroys, or anonymizes the data within 30 days, informing the data subject.
- If conditions have not fully ceased, the request may be rejected with written justification within 30 days.

8.2 PERIODIC DESTRUCTION

Data is destroyed every six months (June and December) according to legal retention periods and this Policy.

All deletion, destruction, and anonymization actions are logged and retained for at least three years, except where other legal obligations apply.

8.3 PROCEDURES FOR DATA PAST RETENTION PERIOD

- Paper-based data destruction is done by designated personnel with managerial knowledge and documented.
- Electronic data destruction is performed by IT department or relevant personnel under managerial supervision.
- Employees are responsible for timely destruction of personal data on assigned devices in accordance with inventory and HR instructions.
- IT provides technical tools for recording destruction actions.

RETENTION AND DESTRUCTION TIMEFRAMES BY DATA TYPE

Data Type	Retention Period	Destruction Timing
Employee Records	10 years after employment ends	First periodic destruction after period
Applicant Data	2 years	First periodic destruction after period
Emails and Internal Communications	10 years	First periodic destruction after period
Former Employee Records	10 years after leaving	First periodic destruction after period
Legal Records	10 years	First periodic destruction after period
Occupational Health and Safety Data	10 years	First periodic destruction after period
Camera Records	3 months	Automatically deleted
Log Records	10 years	First periodic destruction after period
Accounting and Financial Records	10 years	First periodic destruction after period
Customer/Insured Records	10 years after last relation	First periodic destruction after period
Official Correspondence	Indefinite	First periodic destruction after period
Contracts	10 years after contract ends	First periodic destruction after period
Internal Complaints and Documents	10 years	First periodic destruction after period
Tax Records	10 years	First periodic destruction after period
Visitor Records	2 years	First periodic destruction after period

Data Type	Retention Period	Destruction Timing
Intern Records	10 years after internship ends	First periodic destruction after period
Collective Bargaining and Union Records	Until first periodic destruction	First periodic destruction after period
Other Legally Collected Data	As per relevant legislation	First periodic destruction after period
Employee Location Records	1 year	First periodic destruction after period
Employee GSM Usage Records	2 years	First periodic destruction after period
Employee Training Records (Safety etc.)	10-15 years	First periodic destruction after period

---

POLICY PUBLICATION AND STORAGE

The Policy is published both as a signed hard copy and electronically, and also on the Company's website. Upon request, data subjects can access it. The signed paper version is stored by the Accounting department in the KVKK file.

The Policy becomes effective as of its publication date on https://www.marmaracam.com.tr.

POLICY UPDATES AND REVOCATION

The Company reserves the right to update the Policy due to changes in law, Board decisions, or technological and sector developments.

Changes are immediately incorporated and explained at the Policy's end.

If revoked, signed copies are canceled by the Board and stored for at least 5 years by Human Resources.

Marmara Cam Sanayi ve Ticaret Anonim Şirketi
Address: Ergene 1 OSB Sanayi Bölgesi Vakıflar OSB Sanayi Cad. No: 4 /1 Ergene / TEKİRDAĞ
Phone: +90 282 675 10 20
Email: info@marmaracam.com.tr