M.A.C. YARN FABRIC TEKS. SAN. A.Ş. A.S.

PERSONAL DATA RETENTION AND DESTRUCTION POLICY

JANUARY-2019
Version 01

Table of contents

1. ENTRANCE 2
   1.1. Purpose 2
   1.2. Scope 2
2. DEFINITIONS AND ABBREVIATIONS 2
3. DISTRIBUTION OF RESPONSIBILITIES AND DUTIES 4
4. RECORDING MEDIA 4
5. EXPLANATIONS REGARDING STORAGE AND DISPOSAL 4
   5.1. Disclosures Regarding Retention 5
   5.2. Legal Reasons Requiring Retention 5
   5.3. Processing Purposes Requiring Storage 5
   5.4. Reasons Requiring Destruction 6
6. TECHNICAL AND ADMINISTRATIVE MEASURES 7
   6.1. Technical and Administrative Measures 7
7. PERSONAL DATA DESTRUCTION TECHNIQUES 8
   7.1. Methods of Deletion of Personal Data 8
   7.2. Methods of Destruction of Personal Data 9
   7.3. Methods of Anonymization of Personal Data 9
8. STORAGE AND DISPOSAL PERIODS 9
9. PERIODIC DISPOSAL TIMES 10
10. PUBLICATION OF THE POLICY 10
11. STORAGE AND DISPOSAL PERIODS 10

PERSONAL DATA RETENTION AND DESTRUCTION POLICY

1. ENTRANCE

1.1. Purpose

Personal Data Retention and Destruction Policy ("Policy"), **M.A.C. İPİK FABRIC TEKS. SAN. A.Ş. A.S.** ("Company") has been prepared in order to determine the procedures and principles regarding the works and transactions related to the storage and disposal activities carried out. Company; In line with the mission, vision and basic principles determined in the Strategic Plan; The Company has prioritized the processing of personal data belonging to employees, employee candidates, service providers, visitors and other third parties in accordance with the Constitution of the Republic of Turkey, international conventions, the Law on the Protection of Personal Data No. 6698 ("Law") and other relevant legislation, and ensuring that the relevant persons use their rights effectively.

The works and transactions related to the storage and destruction of personal data are carried out in accordance with the Policy prepared by the Company in this direction.

1.2. Scope

Personal data belonging to Company employees, employee candidates, service providers, visitors and other third parties are within the scope of this Policy, and this Policy is applied to all recording environments where personal data owned or managed by the Company are processed and activities for personal data processing.

In addition, unless otherwise stated in this Policy, the documents referred to in the Policy include both printed and electronic copies.

2. DEFINITIONS AND ABBREVIATIONS

Explicit Consent	Consent on a specific subject, based on information and expressed with free will,
Recipient Group	The category of natural or legal person to whom personal data is transferred by the data controller
Constitution	The Constitution of the Republic of Turkey,
Anonymization	Making personal data incapable of being associated with an identified or identifiable natural person in any way, even by matching it with other data.
Electronic Media	Environments where personal data can be created, read, modified and written by electronic devices.
Non-Electronic Media	All other media other than electronic media such as written, printed, visual, etc.
Service Provider	A natural or legal person who provides services within the framework of a specific contract with the company
Relevant Person / Personal Data Owner	The natural person whose personal data is processed.
Related User	Persons who process personal data within the organization of the data controller or in line with the authorization and instruction received from the data controller, except for the person or unit responsible for the technical storage, protection and backup of the data,

Annihilation	Deletion, destruction or anonymization of personal data,
Law	Law No. 6698 on the Protection of Personal Data.
Recording Media	Any environment containing personal data that is fully or partially automated or processed by non-automatic means, provided that it is a part of any data recording system,
Personal data	Any information relating to an identified or identifiable natural person (e.g. name-surname, TCKN, e-mail, address, date of birth, credit card number, bank account number - *Therefore, the processing of information about legal entities is not within the scope* of the Law),
Personal Data Processing Inventory	Personal data processing activities carried out by data controllers depending on their business processes; The inventory that they create by associating the purposes and legal reason for processing personal data with the data category, the transferred recipient group and the data subject group, and the maximum retention period required for the purposes for which personal data is processed, the personal data envisaged to be transferred to foreign countries and the measures taken regarding data security.
Processing of Personal Data	Obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic or non-automatic means, provided that it is a part of any data recording system,
Board	Personal Data Protection Board,
Sensitive Personal Data	Data related to race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, dress, membership to associations, foundations or unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data,
Periodic Destruction	In the event that all of the conditions for processing personal data in the Law disappear, the deletion, destruction or anonymization process to be carried out ex officio at repeated intervals specified in this Policy,
Politics	Personal Data Retention and Destruction Policy
Data Processor	A natural or legal person who processes personal data on behalf of the data controller based on the authorization granted by the data controller.
Data Recording System	A recording system in which personal data is structured and processed according to certain criteria.
Data Controller	The person who determines the purposes and means of processing personal data and manages the place where the data is kept systematically (data recording system)
VERBIS	Data Controllers Registry

Regulation	Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated October 28, 2017

3. DISTRIBUTION OF RESPONSIBILITIES AND DUTIES

All units and employees of the company are required to ensure data security in all environments where personal data is processed in order to ensure the proper implementation of the technical and administrative measures taken by the responsible units within the scope of the Policy, to increase the training and awareness of the unit employees, to monitor and continuously supervise personal data, to prevent unlawful access to personal data and to ensure that personal data is stored in accordance with the law. It actively supports the responsible units in taking technical and administrative measures. The distribution and destruction processes of the titles, units and job descriptions of those involved in the storage and destruction processes of personal data are as follows;

APPELLATION	UNIT	TASK
IT Support	Data processing	It is responsible for providing the technical solutions needed in the implementation of the Policy.
Accounting Specialist	Accounting	It is responsible for the preparation, development, execution, publication and updating of the Policy in the relevant environments and for the Employees to act in accordance with the Policy.
Marketing Associate	**Marketing**	He is responsible for the execution of the Policy in accordance with his duties.
R&D and Purchasing Manager	**Purchase**	He is responsible for the execution of the Policy in accordance with his duties.

4. RECORDING MEDIA

Electronic Media	Physical Environments
Servers (Domain, backup, email, database, file share, etc.) Software (human resources, accounting and production software, portal,) Information security devices (firewall, intrusion detection and blocking, antivirus, etc.) Personal computers (Desktop, laptop) Mobile devices (phone, etc.) Removable memories (USB, Memory Card, etc.) Printer, scanner, copier	Paper Manual data recording systems Written, printed, visual media

5. EXPLANATIONS REGARDING STORAGE AND DISPOSAL

By the company; Personal data belonging to employees, employee candidates, visitors and employees of third parties, institutions or organizations with whom they are in contact as service providers are stored and destroyed in accordance with the Law.

In this context, detailed explanations regarding storage and disposal are given below, respectively.

5.1. Disclosures Regarding Retention

In Article 3 of the Law, the concept of processing personal data is defined, in Article 4, it is stated that the processed personal data should be connected, limited and measured for the purpose for which they are processed and should be kept for the period stipulated in the relevant legislation or required for the purpose for which they are processed, and in Articles 5 and 6, the processing conditions of personal data are listed.

Accordingly, within the framework of our Company's activities, personal data is stored for a period of time stipulated in the relevant legislation or in accordance with our processing purposes.

5.2. Legal Reasons Requiring Retention

Personal data processed in our company within the framework of its activities are kept for the period stipulated in the relevant legislation. In this context, personal data;

- 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 the Regulation of Publications Made on the Internet and Combating Crimes Committed Through These Publications,
- Occupational Health and Safety Law No. 6331,
- Law No. 4982 on the Right to Information,
- Labor Law No. 4857,
- Tax Procedure Law No. 213
- Regulation on Health and Safety Measures to be Taken in Workplace Buildings and Annexes

It is stored for the retention periods stipulated within the framework of other secondary regulations in force in accordance with these laws.

5.3. Processing Purposes Requiring Storage

It stores and uses personal data for the purposes of personal data processing in the relevant articles of the Personal Data Protection and Processing Policy and in accordance with the processing conditions of personal data in Articles 5 and 6 of the Law stated below, and if all of the said conditions are eliminated, it destroys personal data ex officio or upon the request of the personal data owner.

- Execution of Emergency Management Processes
- Execution of Information Security Processes
- Execution of Employee Candidate / Intern / Student Selection and Placement Processes
- Execution of Application Processes of Employee Candidates
- Execution of employee satisfaction and loyalty processes
- Fulfillment of Obligations Arising from Employment Contract and Legislation for Employees
- Execution of Benefits and Benefits Processes for Employees
- Execution of Audit / Ethics Activities
- Execution of Educational Activities

- Execution of Access Authorizations
- Execution of Activities in Accordance with the Legislation
- Execution of Finance and Accounting Affairs
- Ensuring Physical Space Security
- Execution of Assignment Processes
- Follow-up and Execution of Legal Affairs
- Conducting Internal Audit / Investigation / Intelligence Activities
- Execution of Communication Activities
- Planning Human Resources Processes
- Execution / Supervision of Business Activities
- Execution of Occupational Health / Safety Activities
- Receiving and Evaluating Suggestions for the Improvement of Business Processes
- Execution of Business Continuity Activities
- Execution of Logistics Activities
- Execution of Goods / Services Procurement Processes
- Execution of Goods / Services After-Sales Support Services
- Execution of Goods / Services Sales Processes
- Execution of goods / services production and operation processes
- Execution of Customer Relationship Management Processes
- Carrying out activities for customer satisfaction
- Organization and Event Management
- Execution of Performance Evaluation Processes
- Execution of Advertising / Campaign / Promotion Processes
- Execution of Risk Management Processes
- Execution of storage and archive activities
- Carrying out social responsibility and civil society activities
- Execution of Contract Processes
- Execution of Strategic Planning Activities
- Follow-up of Requests / Complaints
- Ensuring the security of movable property and resources
- Execution of Supply Chain Management Processes
- Execution of Wage Policy
- Execution of Marketing Processes of Products / Services
- Ensuring the Security of Data Controller Operations
- Foreign Personnel Work and Residence Permit Procedures
- Execution of Investment Processes
- Execution of Talent / Career Development Activities
- Providing information to authorized persons, institutions and organizations
- Execution of Management Activities
- Creation and follow-up of visitor records

5.4. Reasons Requiring Destruction

Personal data;

- Amendment or abolition of the provisions of the relevant legislation that form the basis for its processing,
- The disappearance of the purpose that requires its processing or storage,

- In cases where the processing of personal data takes place only on the basis of explicit consent, the person concerned withdraws his explicit consent,
- Pursuant to Article 11 of the Law, the application made by the person concerned regarding the deletion and destruction of personal data within the framework of their rights is accepted by the Authority,
- In cases where the Company rejects the application made to it by the person concerned with the request for the deletion, destruction or anonymization of their personal data, finds the answer insufficient or does not respond within the period stipulated in the Law; To make a complaint to the Board and this request is approved by the Board,
- The maximum period requiring the storage of personal data has expired and there are no conditions that justify storing personal data for a longer period of time,

in such cases, it is deleted, destroyed or ex officio deleted, destroyed or anonymized by the Company upon the request of the person concerned.

6. TECHNICAL AND ADMINISTRATIVE MEASURES

In order to store personal data securely, to prevent unlawful processing and access, and to destroy personal data in accordance with the law, technical and administrative measures are taken by the Company within the framework of adequate measures determined and announced by the Board for sensitive personal data in accordance with Article 12 of the Law and the fourth paragraph of Article 6 of the Law. You can find detailed information in our "Policy on the Processing and Protection of Sensitive Personal Data".

6.1. Technical and Administrative Measures

- Network security and application security are ensured.
- Closed system network is used for personal data transfers via the network.
- Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
- There are disciplinary regulations with data security provisions for employees.
- Training and awareness activities are carried out at regular intervals on data security for employees.
- An authorization matrix has been created for employees.
- Access logs are kept regularly.
- Corporate policies on access, information security, use, storage and destruction have been prepared and implemented.
- When necessary, data masking measures are applied.
- Confidentiality commitments are made.
- Employees who have a job change or leave their job are removed from their authority in this area.
- Up-to-date anti-virus systems are used.
- Firewalls are used.
- The signed contracts contain data security provisions.
- Extra security measures are taken for personal data transferred via paper and the relevant documents are sent in confidential document format.
- Personal data security policies and procedures have been determined.
- Personal data security issues are reported quickly.
- Personal data security is monitored.
- Necessary security measures are taken regarding entry and exit to physical environments containing personal data.

- The security of physical environments containing personal data against external risks (fire, flood, etc.) is ensured.
- The security of environments containing personal data is ensured.
- Personal data is reduced as much as possible.
- Personal data is backed up and the security of the backed-up personal data is also ensured.
- User account management and authorization control system are implemented and these are also followed.
- Periodic and/or random audits are carried out and carried out in-house.
- Log records are kept in such a way that there is no user intervention.
- Existing risks and threats have been identified.
- Protocols and procedures for the security of sensitive personal data have been determined and implemented.
- Intrusion detection and prevention systems are used.
- Penetration test is applied.
- Cyber security measures have been taken and their implementation is constantly monitored.
- Encryption is done.
- Sensitive persons data transferred in portable memory, CD, DVD media are encrypted and transferred.
- Data loss prevention software is used.

7. PERSONAL DATA DESTRUCTION TECHNIQUES

All transactions carried out within the scope of destruction are recorded by our Company and such records are kept for at least three years**, excluding other legal obligations** . Unless otherwise decided by the Board, our company chooses the appropriate method of deleting, destroying or anonymizing personal data ex officio according to technological possibilities and implementation costs. explains the reasoning.

7.1. Methods of Deletion of Personal Data

Deletion of personal data is the process of making personal data inaccessible and unusable for the relevant users in any way. Our company takes all necessary technical and administrative measures according to technological possibilities and implementation costs in order to ensure that the deleted personal data is inaccessible and non-reusable for the relevant users.

In this context, our Company applies the following methods for the deletion of personal data:

Data Recording Media	Explanation
Personal Data Contained on the Servers	For those who require storage of personal data on the servers for those whose time has expired, the system administrator removes the access authorization of the relevant users and deletes them.
Personal Data in Electronic Environment	Personal data in the electronic environment, which requires storage of expired, are made inaccessible and unusable in any way for other employees (relevant users) except for the database administrator.
Personal Data in the Physical Environment	For those whose personal data kept in the physical environment has expired, it is made inaccessible and unusable in any way for other employees, except for the unit manager responsible for the document archive. In addition, blackening is applied by scratching/painting/erasing in such a way that it cannot be read.

7.2. Methods of Destruction of Personal Data

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and unusable by anyone in any way. Our company takes all necessary technical and administrative measures according to the technological possibilities and implementation costs related to the destruction of personal data.

In this context, our Company applies the following methods for the destruction of personal data:

Data Recording Media	Explanation
Personal Data in the Physical Environment	Those whose personal data in the paper environment have expired are irreversibly destroyed by spraying and pressing methods or clipping machines
Personal Data on Optical / Magnetic Media	Physical destruction of personal data in optical media and magnetic media, such as melting, burning or pulverizing, is applied. In addition, the magnetic media is passed through a special device and exposed to a high value magnetic field, making the data on it unreadable.
Personal Data Contained on Portable Media	Personal data kept in flash-based storage media that require storage is irretrievably destroyed.

7.3. Methods of Anonymization of Personal Data

Anonymization of personal data is the rendering of personal data that cannot be associated with an identified or identifiable natural person in any way, even if it is matched with other data. In order for personal data to be anonymized; Personal data must be made incapable of being associated with an identified or identifiable natural person, even through the use of appropriate techniques in terms of the recording medium and the relevant field of activity, such as recycling by our Company, the recipient or recipient groups, and matching the data with other data. Our company takes all necessary technical and administrative measures according to the technological possibilities and implementation costs related to the anonymization of personal data.

In this context, our Company does not apply the process of anonymizing personal data electronically. Physically, the blackout method is used.

8. STORAGE AND DISPOSAL PERIODS

Our company retains and destroys personal data only for the period specified in the relevant legislation that it is obliged to comply with or for the purpose for which they are processed. In this context, our Company **stores and destroys personal data for the maximum periods specified in the** Annex-1 Storage and Destruction Periods Table below:

- In the event that the personal data owner applies to our Company and requests the destruction of his/her personal data, our Company:
- If all the conditions for processing personal data have disappeared:

- finalizes the request of the personal data owner *within thirty days at the latest* and informs the personal data owner, and

- If the personal data subject to the request has been transferred to third parties, it notifies the third party of this situation; It ensures that the necessary actions are taken before the third party.

- If all of the conditions for processing personal data have not been eliminated, the request of the personal data owner may be rejected by explaining the reason in accordance with the third paragraph of Article 13 of the Law, and the personal data owner shall be notified of the rejection in writing or electronically within thirty days at the latest.

9. PERIODIC DISPOSAL TIMES

Pursuant to Article 11 of the Regulation, the Company has determined the periodic destruction period **as 6 months**. Accordingly, **periodic destruction is carried out** in our Company every year in MARCH and SEPTEMBER.

10. PUBLICATION OF THE POLICY

This Policy has entered into force on the date of its publication. The policy has been published in JANUARY-2019 and is registered in the VERBIS system.

The policy may be updated from time to time in order to adapt to changing conditions and legislation. The Current Policy [www.mactextile.com.tr] will enter into force on the date of its publication.

11. STORAGE AND DISPOSAL PERIODS

Process	**Retention Period**	**Disposal Time**
Making Incentive Applications	Legal relationship + 10 years	In the first periodic destruction period following the end of the storage period
Execution of communication activities	Legal relationship + 10 years	In the first periodic destruction period following the end of the storage period
Storage of contracts established within the scope of administrative affairs and management activities	Legal relationship + 10 years	In the first periodic destruction period following the end of the storage period
Conducting social compliance audits, conducting audits of third-party companies by the company, conducting technical audits	5 years	In the first periodic destruction period following the end of the storage period
Data processing		
Defining user names for accounting, human resources and production programs	Legal Relationship+10 Years	In the first periodic destruction period following the end of the storage period
In order to ensure the security of the physical space, it is captured and stored with camera systems inside and outside the building and its annexes	2 months	In the first periodic destruction period following the end of the storage period
E-mail correspondence and contents	5 years	In the first periodic destruction period following the end of the storage period
Setting up the e-mail of the employees, determining the access authorities of the employees	As much as the legal relationship	In the first periodic destruction period following the end of the storage period

Follow-up of Access Records within the Scope of Law No. 5651	3 years	In the first periodic destruction period following the end of the storage period
Complaints received via the website contact form	1 year	In the first periodic destruction period following the end of the storage period
Administrative affairs		
Social media content	10 years	In the first periodic destruction period following the end of the storage period
Creating e-mail signatures of employees	As much as the legal relationship	In the first periodic destruction period following the end of the storage period
Obtaining travel insurance for employees	10 years	In the first periodic destruction period following the end of the storage period
Human Resources Activities		
Employee satisfaction surveys, request and suggestion boxes	2 years	In the first periodic destruction period following the end of the storage period
Employee payroll records	Legal Relationship+10 Years	In the first periodic destruction period following the end of the storage period
Job application forms	1 year / Legal Relationship+10 Years	In the first periodic destruction period following the end of the storage period
Personnel files	Legal Relationship+10 Years	In the first periodic destruction period following the end of the storage period
Occupational health and safety records, health files and training documents	Legal Relationship+15 Years	In the first periodic destruction period following the end of the storage period
Purchase		
Vehicle tracking	3 years	In the first periodic destruction period following the end of the storage period
Purchase offers	5 years	In the first periodic destruction period following the end of the storage period
Establishment of contracts	Legal Relationship+10 Years	In the first periodic destruction period following the end of the storage period
Current accounts, notary documents, e-invoice processes, payments, declarations, tax processes, logistics processes, audit activities carried out within the scope of accounting activities	10 years	In the first periodic destruction period following the end of the storage period
Contracts made within the scope of accounting activities, customer and supplier card cards, company establishment, general assembly activities	Legal Relationship+10 Years	In the first periodic destruction period following the end of the storage period
Creation of customer current records and customer cards within the scope of marketing activities	Legal Relationship+10 Years	In the first periodic destruction period following the end of the storage period

Receiving orders by e-mail within the scope of marketing activities	5 years	In the first periodic destruction period following the end of the storage period
Contracts for production and planning processes	Legal Relationship+10 Years	In the first periodic destruction period following the end of the storage period

Data	Retention Period	Disposal Time
Identity	**Legal Relationship + 15 Years**	In the first periodic destruction period following the end of the storage period
Communication	**Legal Relationship + 15 Years**	In the first periodic destruction period following the end of the storage period
Location	**3 years**	In the first periodic destruction period following the end of the storage period
Aslam	**Legal Relationship + 15 Years**	In the first periodic destruction period following the end of the storage period
Legal Action	**Legal Relationship + 10 Years**	In the first periodic destruction period following the end of the storage period
Customer Transaction	**Legal Relationship + 10 Years**	In the first periodic destruction period following the end of the storage period
Physical Space Security	**2 months**	In the first periodic destruction period following the end of the storage period
Transaction Security	**3 years**	In the first periodic destruction period following the end of the storage period
Risk Management	**Legal Relationship + 15 Years**	In the first periodic destruction period following the end of the storage period
Finance	**Legal Relationship + 10 Years**	In the first periodic destruction period following the end of the storage period
Professional Experience	**Legal Relationship + 15 Years**	In the first periodic destruction period following the end of the storage period
Audiovisual Recordings	**Legal Relationship + 15 Years**	In the first periodic destruction period following the end of the storage period
Health Information	**Legal Relationship + 15 Years**	In the first periodic destruction period following the end of the storage period
Criminal Conviction and Security Measures	**Legal Relationship + 10 Years**	In the first periodic destruction period following the end of the storage period
Biometric Data	**As Much as the Legal Relationship**	In the first periodic destruction period following the end of the storage period