KÖSEMEN MAKİNA PARÇA İMALİ SAN. VE TİC. LTD. ŞTİ.	PERSONAL DATA PROTECTION LAW	Version	1.1
		First Publication Date	01.09.2020
	DELETION, DESTRUCTION OR ANONYMIZATION OF PERSONAL DATA	Last Updated Date	01.09.2020

POLICY ON DELETION, DESTRUCTION OR ANONYMIZATION OF PERSONAL DATA

1. ENTRANCE

1.1. Purpose

Explaining the procedures and principles determined by data controllers for determining the maximum period required for the purpose for which personal data is processed and for erasing, destroying and anonymizing personal data.

1.2. Base

This Policy has been prepared based on the first paragraph of the 5th article of the Regulation on the Deletion, Destruction or Anonymization of Personal Data prepared in accordance with the Law No. 6698.

1.3. Scope

Personal data of company personnel, job candidates, visitors, service providers and other third parties are within the scope of this Policy, and this Policy is applied to all recording environments where personal data owned by the company is processed and to activities related to the processing of personal data.

1.4. Definitions

a) Recipient group: The category of natural or legal persons to whom personal data is transferred by the data controller,Explicit Consent: Consent based on information and expressed with free will, related to a specific subject.
b) Relevant user: Persons who process personal data within the data controller organization or in accordance with the authority and instructions received from the data controller, excluding the person or unit responsible for the technical storage, protection and backup of data,
c) Destruction: Deletion, destruction or anonymization of personal data,
d) Law: The Law on the Protection of Personal Data No. 6698 dated 24/3/2016,
e) Recording medium: Any medium containing personal data processed by fully or partially automatic means or non-automatic means provided that it is part of any data recording system,
f) Personal Data: Any information related to an identified or identifiable natural person.
g) Personal data processing inventory: Personal data processing activities carried out by data controllers in connection with their business processes; the inventory they create

by associating with the personal data processing purposes and legal reason, data category, transferred recipient group and data subject person group and explaining the maximum retention period required for the purposes for which personal data is processed, personal data planned to be transferred to foreign countries and the measures taken regarding data security,

h) Processing of Personal Data: All kinds of operations performed on data such as obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data, which are fully or partially automatic or non-automatic provided that they are part of any data recording system.
i) Board: Personal Data Protection Board,
j) Special Personal Data: Data regarding the race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and attire, association, foundation or union membership, health, sexual life, criminal conviction and security measures of individuals, and biometric and genetic data.
k) Periodic destruction: The process of deleting, destroying or anonymizing personal data specified in the storage and destruction policy and carried out ex officio at recurring intervals in the event that all the processing conditions of personal data specified in the Law are eliminated,
l) Policy: Personal Data Storage and Destruction Policy
m) Data Processor: A natural or legal person who processes personal data on behalf of the data controller based on the authority granted by the data controller.
n) Data Recording System: A recording system in which personal data is structured and processed according to certain criteria.
o) Data Controller: A natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.
p) Data Controllers Registry Information System (VERBIS): An information system created and managed by the Presidency, accessible over the internet, to be used by data controllers in applying to the Registry and other relevant transactions related to the Registry.
q) Regulation: Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated 28 October 2017.

2. RECORDING MEDIA

Kişisel veriler aşağıdaki belirtildiği şekilde hukuka uygun olarak güvenli bir şekilde saklanır.

2.1.Electronic Media

a) Personal Computers
b) Mobile Devices
c) Software (VERBIS, Accounting Programs)
d) Information security devices (firewall, attack detection and prevention, log file, antivirus, etc.)

2.2. Elektronik Olmayan Ortam

a) Paper
b) Manual Record Keeping Media (Visitor Book, Job Application Forms, Personnel Files, etc.)
c) Written, printed visual media

3. RESPONSIBILITIES AND DUTY DISTRIBUTIONS

All units and employees of the company will support the responsible units for the implementation of administrative and technical measures to be taken to ensure data security within the scope of the Policy. The distribution of titles, units and job descriptions of those responsible for the storage and destruction of personal data is given in the table below.

Title	Unit	Duty
Company Partners/Data Controllers	Board of Directors/Administrative Bodies	Ensuring that employees act in accordance with the policy
Purchasing, Accounting, Finance and Operations, Human Resources, Production Employees	Other Units	Ensuring that the policy is prepared, developed, updated and carried out in accordance with their duties..

4. STORAGE AND DESTRUCTION

Personal data processed within the framework of company activities are stored as stipulated in the relevant legislation or for a period appropriate to the processing purposes.

4.1 Legal Reasons Requiring Storage

a) Law No. 6698 on the Protection of Personal Data,
b) Law No. 5510 on Social Insurance and General Health Insurance,
c) Law No. 5651 on the Regulation of Publications Made on the Internet and Combating Crimes Committed Through Such Publications,
d) Law No. 6331 on Occupational Health and Safety,
e) Labor Law No. 4857,
f) Other secondary regulations in force pursuant to these laws

4.1.1 Processing Purposes Requiring Storage

a) To carry out human resources, accounting and finance processes.
b) To ensure communication.
c) To ensure company security,
d) To be able to conduct statistical studies.
e) To carry out work and transactions as a result of signed contracts and protocols.

f) Within the scope of VERBIS; to determine the preferences and needs of employees, data controllers, contact persons, data controller representatives and data processors, to organize and update the services provided accordingly.
g) To ensure that legal obligations are fulfilled as required by legal regulations.
h) To establish contact with real and legal persons who have a business relationship with the Company.
i) To make legal reports.
j) To fulfill the burden of proof as evidence in legal disputes that may arise in the future.

4.2. Reasons Requiring Destruction

Personal data;

a) The relevant legislative provisions constituting the basis for processing are changed or abolished,
b) The purpose requiring processing or storage is eliminated,
c) In cases where the processing of personal data is carried out only based on the explicit consent condition, the relevant person withdraws his/her explicit consent,
d) The company accepts the application made by the relevant person for the deletion and destruction of his/her personal data within the framework of his/her rights in accordance with Article 11 of the Law,
e) In cases where the company rejects the application made by the relevant person requesting the deletion, destruction or anonymization of his/her personal data, finds the response insufficient or does not respond within the period stipulated in the Law; a complaint is filed with the Board and this request is approved by the Board,
f) In cases where the maximum period requiring the storage of personal data has passed and there are no conditions that justify storing personal data for a longer period, the company deletes, destroys or anonymizes the data upon the request of the relevant person, or deletes, destroys or anonymizes the data ex officio.

5.ADMINISTRATIVE AND TECHNICAL MEASURES

5.1. Administrative Measures

The administrative measures taken by the Company regarding the personal data it processes are listed below:

a) Training is provided on preventing unlawful processing of personal data, preventing unlawful access to personal data, ensuring the preservation of personal data, and communication techniques to improve the qualifications of employees.
b) Confidentiality agreements, disclosure texts and explicit consent statements are made to employees regarding the activities carried out by the company.
c) There are disciplinary regulations that include data security provisions for employees.
d) Employees are provided with training and awareness activities on data security at certain intervals.

e) A matrix of authority has been created for employees. Corporate policies on access, information security, use, storage and destruction have been prepared and implemented..
f) Confidentiality commitments are made.
g) The security of physical environments containing personal data is ensured against external risks (fire, flood, etc.).
h) The security of environments containing personal data is ensured.
i) The data contact person has been assigned and his/her responsibilities have been determined.
j) The Personal Data Processing Inventory has been prepared.
k) The Company fulfills the obligation to inform the relevant persons before starting to process personal data.
l) Personal data is reduced as much as possible.
m) Periodic and/or random audits are carried out and carried out in-house.
n) Protocols and procedures for special personal data security have been determined and implemented.
o) Audits are carried out at certain intervals regarding data security of data processing service providers.
p) Awareness of data processing service providers is ensured regarding data security.
q) Data loss prevention software is used.

5.2. Technical Measures

a) Network security and application security are provided.
b) A closed system network is used for personal data transfers via the network.
c) Key management is implemented.
d) Security measures are taken within the scope of information technology systems procurement, development and maintenance.
e) Access logs are kept regularly.
f) Authorizations of employees who change their duties or leave their jobs are revoked in this area.
g) Up-to-date anti-virus systems are used.
h) Firewalls are used.
i) Personal data is backed up and the security of backed up personal data is also ensured.
j) User account management and authorization control systems are implemented and these are monitored.
k) Log records are kept in a way that prevents user intervention.
l) If personal data of a special nature is to be sent via e-mail, it is definitely sent encrypted and using a KEP or corporate mail account.
m) Secure encryption / cryptographic keys are used for personal data of a special nature and are managed by different units.
n) Intrusion detection and prevention systems are used.

o) Cyber security measures have been taken and their implementation is constantly monitored..

6. PERSONAL DATA DESTRUCTION TECHNIQUES

6.1 Deletion of Personal Data

Personal data is deleted using the methods specified in the table below.

Data Recording Environment	Description
Personal Data in Electronic Environment	Personal data in electronic media, whose storage period has expired, are rendered inaccessible and non-reusable by any means for employees (relevant users), except for the database administrator.
Personal Data in the Physical Environment	For personal data kept in a physical environment, those for which the period requiring storage has expired are rendered inaccessible and/or non-reusable by anyone, including the unit manager responsible for the document archive.

6.2. Destruction of Personal Data

Personal data is destroyed using the methods specified in the table below.

Data Recording Environment	Description
Personal Data in Physical Environment	Personal data in paper form, whose storage period has expired, are destroyed irreversibly.
Personal Data in Electronic Environment	Personal data in electronic media, whose storage period has expired, are rendered inaccessible and non-reusable by any means for employees (relevant users), except for the database administrator.

6.3 Anonymization of Personal Data

Anonymization of personal data is the process of rendering personal data incapable of being associated with an identified or identifiable natural person, even when matched with other data. In order for personal data to be anonymized, it must be rendered incapable of being associated with an identified or identifiable natural person, even through the use of techniques appropriate for the recording medium and relevant field of activity, such as the return of personal data by the data controller or third parties and/or matching of data with other data.

7. STORAGE AND DESTRUCTION PROCESSES

Regarding personal data processed within the scope of the company's activities;

- ✓ The retention periods for all personal data within the scope of activities carried out in accordance with the processes are listed in the Personal Data Processing Inventory;
- ✓ Retention periods based on data categories are recorded in VERBIS;
  Process-based retention periods are included in the Personal Data Storage and Destruction Policy.

The company will update the storage periods in question if necessary. The company will automatically delete, destroy or anonymize personal data whose storage periods have expired.

Storage and Destruction Periods According to Processes

Period	Storage Period	Destruction Time
Execution of Human Resources Processes	10 years from the end of activity	During the first periodic destruction period following the end of the storage period
Finance and Operations, Execution of Accounting Processes	10 years from the end of activity	During the first periodic destruction period following the end of the storage period
Execution of Occupational Health and Safety processes	10 years from the end of activity	During the first periodic destruction period following the end of the storage period
Camera Records	Kayıttan itibaren 1 ay	During the first periodic destruction period following the end of the storage period
Criminal Cases	10 years from the end of activity	During the first periodic destruction period following the end of the storage period

8. PERIODIC DESTRUCTION PERIOD

In accordance with Article 11 of the Regulation, the Institution has determined the periodic destruction period as 6 months, so the periodic destruction process is carried out in the company in June and December every year.

9. STORAGE OF POLICY

The policy is kept by the company in the Personal Data Protection Law file as a hard copy with wet signature.

10. POLICY UPDATE PERIOD

The policy is reviewed as needed and necessary sections are updated.

11. ENFORCEMENT AND REPEAL OF THE POLICY

The policy is deemed to have entered into force after it has been signed in wet ink. If it is decided to be repealed, the old copies of the policy with wet ink signatures are cancelled (by stamping or writing cancellation) by the decision of the board of directors and/or the data controller and are kept by the company for at least 5 years.