PERSONAL DATA RETENTION AND DESTRUCTION POLICY

1. Purpose

The purpose of the Mantagas Denizcilik Personal Data Retention and Destruction Policy ("Policy") is to set forth the procedures and principles regarding the deletion, destruction, or anonymization of personal data processed by **Mantagas Denizcilik ve Ticaret Limited Şirketi** ("Mantagas Denizcilik" or "Company") after the expiration of the processing period determined by applicable laws and regulations, or if no such period is stipulated, according to commercial practices, or when the purpose for processing such data no longer exists.

This Policy also includes the "technical and administrative measures taken to securely store personal data and to prevent unlawful processing and access" as stipulated in Article 6 of the Regulation on the Deletion, Destruction, or Anonymization of Personal Data, published in the Official Gazette No. 30224 on 28.10.2017. Furthermore, this Policy has been aligned with the Guidelines on the Deletion, Destruction, or Anonymization of Personal Data published by the Personal Data Protection Board. In addition, this Policy has been linked to the provisions of Article 9/f.4 and Article 5 of the Regulation on the Data Controllers Registry, published in the Official Gazette No. 30286 on 30.12.2017.

2. Scope

This Policy covers the deletion, destruction, or anonymization of all personal data processed by Mantagas Denizcilik in its capacity as a "Data Controller" under Article 7 of the Personal Data Protection Law No. 6698 dated 24.03.2016, either fully or partially by automatic means, or by non-automatic means as part of any data recording system, in electronic and/or paper environments, when the conditions for processing have ceased.

3. Definitions

For the purposes of this Policy:

Recipient Group:	Refers to the category of natural or legal persons to whom personal data is transferred by Mantagas Denizcilik.

Data Subject:	Refers to the natural persons whose personal data is processed by Mantagas Denizcilik.
Relevant User:	Refers to individuals within the Mantagas Denizcilik organization or those processing personal data as authorized and instructed by Mantagas Denizcilik.
Destruction:	Refers to the deletion, destruction, or anonymization of personal data.
Law (or KVKK):	Refers to the Personal Data Protection Law No. 6698, dated 24.03.2016.
Recording Environment:	Refers to any environment where personal data processed through automatic or non-automatic means is stored as part of any data recording system.
Personal Data Processing Inventory (or Inventory):	Refers to the inventory that identifies the personal data processing activities carried out by Mantagas Denizcilik, the purposes of processing personal data, the categories of data processed, the recipient groups, the groups of data subjects, and the maximum retention periods for the processed personal data, as well as the measures taken within the institution for data security and the personal data anticipated to be transferred to foreign countries.
Periodic Destruction:	Refers to the recurring deletion, destruction, or anonymization of personal data to be carried out at intervals specified in this Policy when the conditions for processing personal data stipulated in the Law have completely ceased.
Registry (VERBİS):	Refers to the data controllers' registry maintained by the Personal Data Protection Authority.
Data Recording System:	Refers to the recording system in which personal data is processed in a structured manner according to specific criteria.
Data Owner:	Refers to the person responsible for processing personal data or the section manager responsible for managing the data processing processes.
Data Controller:	Mantagas Denizcilik ve Ticaret Limited Şirketi
Web:	Refers to websites owned by Mantagas Denizcilik

Obfuscation:	Refers to the process of crossing out, painting over, or blurring personal data so that it can no longer be associated with an identifiable or potentially identifiable natural person.

In cases where definitions not covered by this Policy are needed, the definitions in the Law and Regulations can be referenced.

4. Implementation of the Policy and Relevant Legislation

Relevant legal regulations in force regarding the retention and destruction of personal data will be primarily enforced. In the event of a discrepancy between the legislation in force and the Policy, our Company acknowledges that the legislation in force will be applied.

This Policy has been created by concretizing the rules set out by the relevant legislation within the scope of Mantagas Denizcilik's practices.

5. Retention Periods for Personal Data Processed by Our Company

5.1. Retention Periods for Personal Data

Our Company retains personal data for the duration stipulated by the relevant laws and regulations. If the relevant legislation does not specify a retention period, personal data is processed for the duration necessary to provide the services offered by our Company while operating in a regulated sector, based on the requests of relevant institutions and commercial practices. After this period, the data is deleted, destroyed, or anonymized. Detailed information on this matter is provided in Section 10 of this Policy. If the purpose of processing personal data has ended and the retention periods determined by the relevant legislation and the Company have also expired, the personal data may only be retained to serve as evidence in possible legal disputes or to assert or establish a related right or defense. In determining these retention periods, the statute of limitations for asserting the aforementioned right and examples of previous similar requests made to our Company after the statute of limitations has passed are taken into consideration. In this case, the retained personal data will not be accessed for any other purpose and will only be accessed if necessary for the related legal dispute. After the expiration of the aforementioned period, the personal data will be deleted, destroyed, or anonymized.

If personal data processed by our Company has been transferred to third parties, those third parties are also required to delete, destroy, or anonymize the relevant personal data once the purpose of processing has ended. Our Company takes the necessary precautions to ensure this, and provisions regarding these precautions are included in contracts. Within the scope of the precautions taken, the relevant third parties are notified, and a commitment is obtained that the operation has been completed.

5.2. Data Storage Environments

Our Company stores all personal data processed within the scope of the Law in the following environments, either fully or partially through automatic means or by non-automatic means as part of any data recording system, in the following environments:

Electronic Environments:

- Company-owned servers and network systems, applications developed by the Company or obtained as a service, and cloud systems
- Servers (Databases, Emails, e-folders belonging to Business Units)
- Company-owned mobile devices (mobile phones, computers)
- Camera recording area
- Internet sites with infrastructure created by contracted firms

Non-Electronic Environments:

- Paper, Manual data recording systems (visitor logbook), locked cabinets, archive room

6. Actions to be Taken When Conditions for Processing Personal Data Cease

If the purpose for processing personal data ceases, explicit consent is withdrawn, or all conditions for processing personal data as specified in Articles 5 and 6 of the Law have ceased, or when none of the exceptions mentioned in the aforementioned articles apply, the personal data for which the conditions for processing have ceased will be deleted, destroyed (erased), or anonymized by the relevant business unit, taking into account business needs, and in accordance with Articles 7, 8, 9, or 10 of the Regulation, with an explanation of the method used. However, if there is a finalized court order, the method of destruction imposed by the court must be applied.

All users who process or store personal data, and all Company units responsible for data, will review their data recording environments to check whether the conditions for processing have ceased at least once every four months. Upon a data subject's request or notification from the Board or a court, the relevant users and units will conduct this review regardless of the periodic audit cycle.

As a result of the periodic reviews or at any time when it is determined that the conditions for processing data have ceased, the relevant user or data subject will decide to delete, destroy (erase), or anonymize the relevant personal data in the recording environment under their control in accordance with this Policy. In cases of doubt, the relevant data subject will seek the opinion of the relevant business unit before proceeding. If a decision needs to be made regarding the destruction of personal data with shared ownership stored in Central Information Systems, the opinion of the Personal Data Protection Committee will be sought, and the relevant business unit will decide whether to retain, delete, destroy (erase), or anonymize the personal data in accordance with this Policy.

All actions related to the deletion, destruction (erasure), or anonymization of personal data are recorded, and these records are retained for at least three years, excluding other legal obligations.

In accordance with Article 7.4 of the Regulation, the methods applied for the deletion, destruction (erasure), or anonymization of personal data will be published and explained after the Policy enters into force.

The deletion, destruction, or anonymization of personal data will be carried out in compliance with the general principles in Article 4 of the Law and the technical and administrative measures to be taken under Article 12, as well as the relevant legislative provisions, Board decisions, and court rulings.

A data subject, in accordance with Article 13 of the Law, may request the deletion, destruction, or anonymization of their personal data by applying to the Company. The relevant business unit will examine whether all conditions for processing the personal data have ceased. If all processing conditions have ceased, the relevant personal data will be deleted, destroyed, or anonymized. In such cases, as specified in the Data Destruction Procedure, the request will be resolved within a maximum of thirty days from the application date, and the individual will be informed through the KVKK contact

person appointed by the KVKK Officer. If all conditions for processing the personal data have ceased and the personal data in question has been transferred to third parties, the relevant business unit will immediately notify the third party to which the data was transferred and ensure that the necessary actions are taken in accordance with the Regulation.

In cases where all conditions for processing personal data have not ceased, the Company may reject requests for the deletion or destruction (erasure) of personal data made by data subjects, explaining the reason for the rejection in accordance with Article 13(3) of the Law. The rejection response will be communicated to the data subject in writing or electronically within 30 (thirty) days at the latest.

Requests for the deletion or destruction (erasure) of personal data will only be evaluated if the identity of the relevant person has been verified. For requests made through channels other than those specified, data subjects will be directed to channels where their identity can be verified or authenticated.

7. Enforcement of the Policy, Violation Cases, and Sanctions

This Policy will be announced to all employees and personal data subjects through the Company's website and will come into effect. From the date of its enforcement, it will be binding for all business units, consultants, customers, insurance companies, external service providers, and anyone else processing personal data within the Company.

The responsibility for monitoring whether employees comply with the requirements of the Policy lies with the supervisors of the respective employees. If a violation of the Policy is identified, the matter will immediately be reported to a superior by the responsible supervisor. If the violation is significant, the superior will promptly inform the KVK Committee.After an evaluation by the Human Resources department, appropriate administrative actions will be taken against employees who violate the Policy.

To fulfill the requirements of the Policy, the Company will take all necessary security measures within the scope of the Personal Data Protection Law (KVKK).

8. Individuals Involved in Personal Data Retention and Destruction Processes and Their Responsibilities

Within the Company, all employees, customers, insurance companies, consultants, external service providers, and anyone else who stores and processes personal data on behalf of the Company are responsible for fulfilling the requirements specified in the Law, Regulations, and the Policy regarding the destruction of data.

Each business unit is responsible for storing and protecting the data generated in their own business processes. However, if the generated data is stored solely in information systems outside the control and authority of the business unit, the relevant data will be stored by the units responsible for information systems.

Periodic destructions that could affect business processes, compromise data integrity, lead to data loss, or result in outcomes that are contrary to legal regulations will be carried out by the relevant information systems departments, taking into account the type of personal data, the systems in which it is located, and the data owner business unit.

8.1. Personal Data Protection Committee

A Personal Data Protection Committee will be established within the Company. The Personal Data Protection Committee is authorized and responsible for ensuring that the data of relevant individuals is stored and processed in accordance with the law, the Personal Data Protection and Processing Policy, and the Personal Data Retention and Destruction Policy, as well as for overseeing and conducting the necessary processes.

The Personal Data Protection Committee will consist of at least three people, including a manager, an administrative expert, and a technical expert. The titles and job descriptions of the Company employees who serve on the Personal Data Committee are as follows:

Title	Job Description
Personal Data Protection Committee Manager	Responsible for directing all planning, analysis, research, and risk assessment activities in

	projects carried out in compliance with the Law; managing the processes that need to be carried out in accordance with the Law, the Personal Data Protection and Processing Policy, and the Personal Data Retention and Destruction Policy; and making decisions on requests from relevant individuals.
KVK Specialist (Contact Person) (Technical and Administrative)	Responsible for examining and reporting the requests of relevant individuals to the Personal Data Committee Manager for evaluation; implementing the actions related to the requests evaluated and decided upon by the Personal Data Committee Manager in accordance with their decision; overseeing the retention and destruction processes and reporting these audits to the Personal Data Committee Manager; and executing the retention and destruction processes.

9. Conditions for the Retention, Deletion, Destruction, and Anonymization of Personal Data

9.1. Legal Clarification Regarding the Obligation to Retain, Delete, Destroy, and Anonymize Personal Data

As regulated in Article 138 of the Turkish Penal Code and Article 7 of the KVKK, despite the personal data having been processed in accordance with the relevant legal provisions, if the reasons requiring their processing no longer exist, the personal data will be deleted, destroyed, or anonymized upon the Company's decision or at the request of the personal data subject. In this context, our Company fulfills its obligation using the methods explained in this section.

If such a request is made by the personal data subject, an examination is conducted in accordance with the relevant Company policy, and the most appropriate method among deletion, destruction, or anonymization is chosen, the operation is carried out, and the personal data subject is informed.

9.2. Techniques for Deletion, Destruction, and Anonymization of Personal Data

The deletion, destruction, and anonymization of personal data are carried out in accordance with the Regulation and the techniques outlined in the relevant guidelines published by the Personal Data Protection Board.

9.2.1. Techniques for Deletion and Destruction of Personal Data

Our Company may delete or destroy personal data upon its own decision or at the request of the personal data subject, even though the personal data was processed in accordance with the relevant legal provisions if the reasons requiring its processing no longer exist. The most used deletion or destruction techniques by our Company are listed below:

(i) Physical Destruction

Personal data can also be processed through non-automatic means as part of any data recording system. During the deletion or destruction of such data, a system of physically destroying the personal data in a way that it cannot be reused is applied.

(ii) Secure Deletion from Software

When deleting or destroying data that is processed through fully or partially automated means and stored in digital environments, methods are used to securely delete the data from the relevant software so that it cannot be recovered.

(iii) Secure Deletion by an Expert

In some cases, the Company may engage an expert to delete personal data on its behalf. In this case, personal data is securely deleted or destroyed by an expert in such a way that it cannot be recovered.

9.2.2. Techniques for Anonymization of Personal Data

Anonymization of personal data means rendering the personal data incapable of being associated with an identified or identifiable natural person, even when combined with other data.

When the reasons requiring the processing of personal data, which has been processed in accordance with the law, cease to exist, our Company can anonymize the personal data. In accordance with Article 28 of the KVKK, anonymized personal data can be processed for purposes such as research, planning, and statistics. Such processing falls outside the scope of the KVKK, and the explicit consent of the personal data subject will not be sought. The most commonly used anonymization techniques by our Company are listed below:

(i) Masking

Data masking involves removing the key identifying information from the data set, thereby anonymizing the personal data.

(ii) Aggregation

The data aggregation method involves grouping multiple data sets, making it impossible to link the personal data to any individual.

(iii) Data Derivation

The data derivation method involves creating a more general content from the content of the personal data, making it impossible to link the personal data to any individual.

(iv) Data Shuffling

Data shuffling involves rearranging the values within the personal data set, breaking the connection between the values and the individuals.

9.3. Technical and Administrative Measures for Secure Retention of Personal Data, Prevention of Unlawful Processing, and Prevent Unauthorized Access

1.	Data classification software has been installed on all employee computers.
2.	A data classification system has been established to prevent the data leakage via email, USB, printer, etc., and to prevent data from being exported outside the company.
3.	Confidentiality agreements are signed. Information security agreements are signed with cooperating/service-providing firms, and audits on information security and lawful data processing are planned at regular intervals based on our audit rights.
4.	Efforts are being made to develop systems that record consents, transfer details, etc., regarding the processing of personal data.

5.	Common access permissions within the Company being regularly reviewed.
6.	Network and application security are ensured.
7.	Closed system network is used for transferring personal data over the network.
8.	Encryption and secure key management systems are applied.
9.	IT systems for procurement, development, and maintenance include security measures.
10.	The security of personal data stored in the cloud is ensured.
11.	Disciplinary measures related to data security are included in employee policies.
12.	Employees receive regular training and awareness on data security.
13.	Access logs are maintained regularly.
14.	Corporate policies on access, information security, usage, storage, and destruction have been prepared and implemented.
15.	The permissions of employees who have changed roles or left the Company are revoked.
16.	Up-to-date antivirus systems are used.
17.	Firewalls are used to protect company systems.
18.	Contracts signed with third parties include data security provisions.
19.	Policies and procedures related to personal data security are defined.
20.	Personal data security issues are reported promptly.
21.	The monitoring of personal data security is conducted.
22.	Necessary security measures are taken to control access to physical environments containing personal data.
23.	The security of physical environments containing personal data is protected against external risks such as fire, flooding, etc.
24.	The security of personal data in physical environments is ensured.
25.	Personal data is minimized as much as possible.
26.	Personal data is backed up, and the security of the backed-up data is also ensured.
27.	User account management and authorization control system is implemented and monitored.
28.	Internal periodic and/or random internal audits are conducted and commissioned.

29.	Log records are kept in a manner that prevents user interference.
30.	Existing risks and threats have been identified.
31.	Special categories of personal data sent via email are sent with encryption using using a corporate email account or KEP (Registered Electronic Mail).
32.	Secure encryption/cryptographic keys are used for special categories of personal data, and these keys are managed by different units.
33.	Intrusion detection and prevention systems are used.
34.	Cybersecurity measures are taken and their application is continuously monitored.
35.	Encryption is implemented.
36.	Special categories of personal data transferred on portable media, CDs, or DVDs are encrypted.
37.	Service providers processing personal data are audited regularly for data security.
38.	Efforts are made to raise awareness among service providers about data security.
39.	Data loss prevention software is used.
40.	Locked archive rooms are created to prevent unauthorized third-party access to physical documents containing personal data.
41.	Physical documents in the archive are classified accordingly.
42.	Based on the principle of proportionality, the collection of documents for contracts and applications is limited.

9.4. Technical and Administrative Measures for the Lawful Destruction of Personal Data

	Measures:
1.	Personal data within the scope of the policy is identified across all systems.
2.	The data controllers are informed of the data to be deleted, and decisions are made accordingly.
3.	In line with the decisions made, destruction measures outlined in this policy are applied to the identified data.

10. Personal Data Retention and Destruction Periods

10.1. Table Showing Retention and Destruction Periods of Personal Data

The retention and destruction periods of personal data are shown in the table below, categorized and indicating the maximum periods.

Data Subject	Data Category	Data Retention Period
Employee	Employment records and personal data submitted to the Social Security Institution regarding service duration and salary notifications	Maintained for the duration of the employment contract and 15 (fifteen) years from the beginning of the calendar year following the termination of the employment contract.
Employee	Data in the Workplace Personal Health File	Maintained for the duration of the employment contract and 15 (fifteen) years following its termination..
Business Partner/Solution Partner/Consultant	Identity information, contact information, financial information, voice recordings from phone calls, data of employees of the Business Partner/ Solution Partner/ Consultant for the purpose of executing the commercial relationship between the Company and the Business Partner/ Solution Partner/ Consultant	Maintained for the duration of the business/commercial relationship and for 10 (ten) years after its termination in accordance with Article 146 of the Turkish Code of Obligations and Article 82 of the Turkish Commercial Code.
Visitor	Name, surname, T.C. (ID) number, vehicle plate, and camera recordings taken when entering the physical premises of the Company	Maintained for 1 year.
Website Visitor	Name, surname, email address, browsing activity of the Website Visitor	Maintained for 2 (two) years.

Data Subject	Data Category	Data Retention Period
Job Applicant	Information in the resume and job application form of the candidate	Maintained for as long as the CV remains relevant and up-to-date, up to a maximum of 2 (two) years.
Customer	Name, surname, T.C. (ID) number, contact details, payment information, browsing activity, call recordings, product/service preferences, transaction history, and special day information	Maintained for 10 (ten) years from the date of delivery of each product/service purchased by the Customer in accordance with Article 146 of the Turkish Code of Obligations and Article 82 of the Turkish Commercial Code.
Customer	Camera footage	Maintained for 3 (three) months.
Potential Customer	Identity, contact, and financial information collected during contract negotiations for establishing a business relationship	Maintained for 10 (ten) years.
Company's Partner Institutions/Companies (Supplier, Contract Manufacturer, Dealer/Franchisee)	Identity information, contact, financial information, voice recordings from phone calls, and and data of employees of the partner institutions/companies during the execution of the commercial relationship with the Company	Maintained for the duration of the business/commercial relationship and for 10 (ten) years after termination as per the Turkish Code of Obligations (Article 146) and the Turkish Commercial Code (Article 82).

(a) If all conditions for processing personal data no longer exist:

(i) The data subject's request is resolved within maximum of thirty days, and the data subject is informed.

(ii) If the personal data subject to the request has been transferred to third parties, the Company notifies the third party of this situation and ensures that necessary actions are taken by the third party.

(b) If not all conditions for processing personal data have ceased, the request of the relevant person may be rejected by providing a reason under Article 13(3) of the Law, and the rejection response will be notified to the relevan person in writing or electronically within thirty days at the latest.

10.2. Information on Periodic Destruction Periods

Periodic destruction will be carried out every six (6) months, starting from the date the Regulation came into effect, and logs of the actions taken will be retained for three (3) years.

11. Roles and Responsibilities

All organs and departments of the Company are responsible for ensuring compliance with the Personal Data Retention and Destruction Policy and cooperating with the Personal Data Protection Commission.

The Legal Department serves as a source of advice, consultant, and guide in the execution of processes.

12. Review

In case of a conflict between the legislation in force regarding the protection and processing of personal data and the Personal Data Retention and Disposal Policy, the Company acknowledges that the legislation in force will prevail. The Personal Data Retention and Disposal Policy is published on the Company's website www.mantagas.com and is accessible to personal data owners. Any changes made to the Personal Data Retention and Destruction Policy in parallel with amendments and innovations in the relevant legislation will be made accessible to personal data subjects in a manner that they can easily access.